TESIS DOCTORAL

LA SEGURIDAD CIBERNÉTICA Y LOS DERECHOS HUMANOS LOS LÍMITES DE LA RESTRICCIÓN DE DERECHOS HUMANOS PARA LA PROTECCIÓN DEL ESPACIO CIBERNÉTICO

Autora:
Alexandra Cerasela Pana

Tesis depositada en cumplimiento parcial de los requisitos para el grado de Doctor en
Estudios Avanzados en Derechos Humanos

Universidad Carlos III de Madrid

Director:

Prof. JOSÉ MANUEL RODRÍGUEZ URIBES, Ph.D.

Marzo 2021

A Nicu e Isa

mi Norte y mi Sur

AGRADECIMIENTOS

A mi estimado profesor José Manuel Rodríguez Uribes, por toda su transferencia de conocimiento y por su paciencia para orientarme y apoyarme en todo este largo y duro camino académico. Tengo suerte de haber conocido este gran hombre de cultura; a usted exteriorizo mi profundo agradecimiento. Ser su alumna ha sido un gran honor.

Al estimado profesor Carlos Lema Añón, director del programa de doctorado en Estudios Avanzados en Derechos Humanos, y a Dña. María Carmen Alcubilla Raboso, por brindarme siempre su tiempo, paciencia y quedar siempre pendiente a mis solicitudes e inquietudes.

A mi hermano Dorin y a su hermosa Janeth que me apoyaron en todos estos cinco años de estudio y esfuerzo, inspirándome en cada momento.

A mis padres y suegros, hermanos y cuñados, y a todos mis familiares que me aceptan tal como soy y me ayudan a seguir siempre adelante.

A mis primeros profesores españoles Luis Gutiérrez Sanjuán y Nicolas Rodríguez Castellano que me enseñaron la riqueza jurídica y cultural de España en mi experiencia Erasmus, un momento clave en mi camino académico.

A mis amigos españoles: Isabel, Juan, Seila, Mateo, José y Lisa por su amistad y apoyo en esta aventura académica.

A todos mis colaboradores y compañeros que han aportado buenas experiencias en mi vida, me han orientado en mis decisiones y me han ayudado a crecer profesionalmente.

A mi querido Nicu por caminar de mano más de 20 años, ayudándome a pasar todos los momentos difíciles de mi vida, por su paciencia y su amor infinito.

A mi hija Isa, por compartirme con esta tesis.

CONTENIDOS PUBLICADOS Y PRESENTADOS

- PANA, Alexandra Cerasela (2020). Aplicarea regulamentelor europene în domeniul securităţii cibernetice. Rolul Agenţiei Uniunii Europene pentru securitate cibernetică *(La aplicacion de los reglamentos europeos en el ambito de la seguridad cibernetila. El papel de la Agencia de Seguridad Cibernética de la Unión Europea*). Revista Pandectele Romane no. 3/2020, Editorial Wolters Kluwer România, pp. 71-88. Esta fuente está incluida en el capítulo III de esta tesis.

- PANA, Alexandra Cerasela (2019). Rolul factorului uman în asigurarea protecţiei datelor personale prelucrate în cadrul comunităţilor virtuale *(El papel del factor humano para garantizar la protección de los datos personales procesados dentro de las comunidades virtuales);* Revista Pandectele Române, nr. 6/2019, Wolters Kluwer România, pp. 79-91. Esta fuente está incluida en el capítulo II.

Contenido

RESUMEN PARA DOCTORADO INTERNACIONAL

Ciberespacio: la última frontera. Aquí es donde empieza la nueva misión de los juristas en buscar nuevas formas de ejercicio de los derechos humanos. Afortunadamente, no es una misión de ciencia ficción, sino un desafío real, actual y lleno de oportunidades. Consideramos que es el mejor momento para proponer esta tesis e iniciar un trabajo de investigación sobre la dinámica del derecho en la era de las nuevas tecnologías.

La tesis está fundamentada en la investigación de este nuevo espacio donde ha entrado el ser humano, titular de los derechos y libertades fundamentales. Como cualquier entorno nuevo, despierta la curiosidad, la necesidad de explorar, pero también la necesidad de estar seguro. El ser humano está programado genéticamente para proteger su vida, integridad y libertad en cualquier entorno, tanto físico como virtual.

La ciberseguridad es un tema nuevo, que empezó a fomentar los debates solo desde 1988. Estados, empresas privadas y especialistas se dieron cuenta rápidamente de la necesidad de regular este campo, incluso adaptando el derecho internacional a las nuevas realidades. Los conflictos, eventos frecuentes en la sociedad humana, han migrado rápidamente del espacio físico al espacio virtual, al igual que las armas. Los virus informáticos, las aplicaciones invasivas y el software de espionaje sustituyen a las armas y herramientas de guerra clásicas.

Las medidas de seguridad propuestas e implementadas por las autoridades estatales con responsabilidades en el ámbito de la seguridad nacional, así como por empresas privadas que desarrollan programas para combatir ciberataques, basados en medidas de ciber espionaje o hack-back[1], se adaptan a los nuevos desafíos tecnológicos, pero evitan solucionar problemas importantes para el individuo como el respeto a sus derechos fundamentales, cuyo reconocimiento y regulación le han costado años de lucha y fundamentación filosófico-legal.

En este contexto, cuando la vida del ciudadano se traslada, cada vez más al espacio virtual con todos sus elementos - banca por internet, telemedicina, información e investigación de fuentes digitales, comercio electrónico, citas virtuales, realidad virtual -

[1] El *hack-back* (devolver el hackeo) sería la acción de utilizar la fuerza cibernética para contener el ciberataque de un agresor en un contexto de legítima ciberdefensa. Tendría por tanto paralelismos con los mismos componentes que la legítima defensa personal en el terreno analógico, con la salvedad de que los defensores en este caso serían personas jurídicas y empresas. Montero, A. (2018) *Hack-back: ¿legítima ciberdefensa en empresas?,* Real Instituto Elcano.

se deben proponer medidas para proteger el ciberespacio que pueden ser diseñadas en correlación directa con las medidas de seguridad aplicadas en el entorno offline.

Si el entorno offline está claramente determinado, y hay actores con papeles muy claros (estados, territorios administrativos, instituciones con responsabilidades en el campo de la seguridad y protección de los ciudadanos, etc.), el espacio virtual sigue siendo una jungla, sin límites conocidos y con incipientes formas de órganos de control, que deberían proteger a los usuarios vulnerables para no ser víctimas de los manipuladores digitales.

En este momento, las Naciones Unidas a través de sus comisiones y grupos de expertos, ha asumido el papel de garante de los derechos humanos en el ciberespacio, interpretando las disposiciones de los tratados internacionales y elaborando recomendaciones, para ciber conflictos y alianzas entre Estados y grandes empresas con control tecnológico sobre Internet, tanto en términos de contenido como de conexiones informáticas.

A nivel de la Unión Europea, el papel de las instituciones comunitarias, bien definido en el proceso de desarrollo y aplicación de las normas jurídicas, permite diseñar un marco jurídico coherente para la política de ciberseguridad, asegurando un sistema de protección eficaz basado en la cooperación entre los Estados miembros, al mismo tiempo con una protección efectiva de los derechos individuales en el entorno virtual. La tradición democrática de los estados europeos contribuye a la identificación de soluciones viables con respecto a la libertad del ciberespacio y la importancia del individuo en la sociedad.

El surgimiento y el fortalecimiento del papel de ENISA en la política europea de ciberseguridad, ofrece la ventaja de estandarizar, centralizar y explotar de manera coherente los datos comunicados por los Estados miembros con el fin de desarrollar normativas bien fundamentadas.

Asimismo, esta tesis estudia algunas categorías de derechos fundamentales para descubrir la forma en que se ven influenciados por la nueva realidad de la vida cotidiana. El entorno en el que se ha estudiado y conceptualizado estos derechos a lo largo de la historia, hasta la confirmación en diversos instrumentos de derecho internacional, ha cambiado profundamente. Las amenazas comienzan a ser diversas, y para los juristas no especializados en informática, es un gran reto identificar las brechas en los mecanismos informáticos que garanticen y protejan los derechos fundamentales cuando el individuo actúa en el entorno online. Es posible que la generación de *juristas nativos digitales* se

haga cargo del trabajo de los juristas *adaptados digitalmente* y sea capaz de construir un sistema legal aplicable a este nuevo entorno de vida del individuo. Esto será posible solo dentro de 10 años, cuando la nueva generación creada en la era de las nuevas tecnologías, posea la capacidad de analizar y proponer soluciones legales.

La investigación se centra en el derecho a la privacidad y los elementos que lo componen, siendo considerado como uno de los derechos fundamentales más vulnerables en el entorno online. Los derechos derivados, como el derecho al nombre, la identidad, el honor, la dignidad y la integridad física se están transformando y adquiriendo nuevos valores en la era de las nuevas tecnologías. Algunos de estos derechos se transforman, se trasladan al ciberespacio, se adhieren al ser virtual y se convierten en derechos digitales, propios del nuevo entorno social. En el contenido de la tesis se desarrolló un capítulo dedicado a esta nueva categoría de derechos en el que se intenta establecer sus contenidos y las formas de manifestación.

Con respecto a los mecanismos necesarios para garantizar el ejercicio de los derechos y libertades fundamentales, el trabajo analiza los distintos niveles de protección: desde el nivel supranacional (internacional), hasta el regional y nacional, específico de cada Estado. Los mecanismos institucionales y jurisdiccionales están organizados en gran medida de acuerdo con las mismas reglas, guiándose por las regulaciones internacionales sobre derechos humanos, en particular, continuando con las regulaciones a nivel regional y estatal. En el nuevo contexto tecnológico, es necesario revisar dichos mecanismos para que mantengan la misma eficiencia deseada en el momento de su creación.

Un punto importante de la investigación consiste en el análisis de las restricciones aplicadas a los derechos humanos bajo el imperio de la Ley. Sin referirse a las injerencias ilegales, sino analizamos la injerencia permitida por la ley, especialmente en nombre de la seguridad colectiva.

Seguidamente, se muestran los debates y análisis destinados a establecer el punto de equilibrio entre la importancia de un derecho fundamental u otro. Tanto el derecho a la vida privada como el derecho a la seguridad se consideran fundamentales, pero no absolutos. Desde esta perspectiva, se deben establecer límites claros para que la protección de uno no afecte la integridad del otro. Los Estados a veces imponen medidas excesivamente restrictivas del derecho a la privacidad en nombre de la seguridad nacional, y el ciberespacio es el entorno adecuado para tales prácticas. Cualquier práctica de este tipo, situada a uno de los dos extremos, ya sea muy invasiva en la esfera personal o ineficaz desde una perspectiva de seguridad, debe ser reevaluada y relacionada con los

derechos humanos, tanto desde una perspectiva individual como colectiva. Por ejemplo, el derecho a la vida privada o el derecho a la seguridad del ser humano puede, dentro de límites razonables, restringir el derecho de otra persona a expresarse o manifestar ciertas necesidades mentales en el espacio digital.

Teniendo en cuenta los objetivos propuestos al principio, aplicando los métodos de investigación correspondientes y analizando la literatura, el marco normativo vigente y la jurisprudencia en derechos humanos, esta tesis identifica y enfatiza la interacción entre los derechos humanos fundamentales y los efectos sociales de las nuevas tecnologías, incluyendo las consecuencias sobre los derechos conexos.

En este contexto particularmente dinámico, el mayor desafío para la nueva generación de juristas será adaptar el marco legal actual, a las nuevas realidades del mundo digital. Dado que las normas de derecho que rigen nuestra vida cotidiana han evolucionado lentamente y durante un largo período de tiempo, la rápida evolución tecnológica y la migración del individuo al espacio virtual requieren una urgente adaptación del marco legal a las nuevas realidades para que la Ley pueda mantener su misión de guardián del bienestar público.

Además, esta nueva pandemia, origina y causa inciertos ampliamente cuestionado en el entorno online, ha provocado una restricción en masa de los derechos humanos similar a la última guerra mundial. Se ha restringido el derecho a la: libertad de circulación, manifestación, reunión, expresión, educación, trabajo e incluso el derecho a buscar la felicidad. Por la limitación de estos derechos la gente, por temor al enemigo invisible e incomprendido, aceptó sin oposición la mayor parte todas estas injerencias de las autoridades en su vida privada y en el conjunto de sus libertades fundamentales. Solo pequeños grupos de activistas continúan luchando por defender sus derechos fundamentales. No sabemos si este evento global llamado pandemia COVID 19 reescribirá la historia de los derechos fundamentales, pero es cierto que su impacto en el ámbito de las libertades individuales ha tenido un efecto muy fuerte e inquietante con respecto a otra transformación, incluida la revolución tecnológica.

En estas condiciones, nos queda una única opción o desafío: defender al individuo, con todos sus atributos, en una sociedad dinámica, caracterizada por transformaciones atípicas.

REZUMAT PENTRU MENȚIUNE DOCTORAT INTERNAȚIONAL

Spațiul cibernetic – ultima frontieră. Aici începe misiunea juriștilor în căutarea noilor forme de exercitare a drepturilor omului. Din fericire, nu este o misiune science-fiction, ci este o provocare reală, actuală și plină de oportunități. Consider că am ales cel mai bun moment pentru a propune această teza și a iniția o muncă de cercetare asupra dinamicii dreptului în era noilor tehnologii. Această eră este abia la început.

Lucrarea de față pornește de la cercetarea acestui nou spațiu în care a pătruns ființa umană deținătoare a drepturilor și libertăților fundamentale. Ca orice mediu nou, stârnește curiozitatea, nevoia de a explora dar și nevoia de a fi în siguranță. Ființa umană este programată genetic să își protejeze viața, integritatea și libertatea în orice mediu s-ar afla, atât fizic cât și virtual.

Securitatea spațiului cibernetic este o temă nouă, se discută despre acest subiect abia din anul 1988. Statele, companiile private și specialiștii au conștientizat rapid necesitatea reglementării acestui domeniu, inclusiv prin adaptarea dreptului internațional la noile realități. Conflictele, evenimente frecvente în societatea umană, au migrat rapid din spațiul fizic în spațiul virtual, la fel și armele. Virușii informatici, aplicațiile intruzive, softurile de spionaj iau locul clasicelor arme și unelte de război. Măsurile de securitate propuse și implementate de autoritățile statale cu atribuții în domeniul securității naționale, cât și de companiile private care dezvoltă programe de combatere a atacurilor cibernetice, bazate pe spionaj cibernetic sau măsuri de tipul *hack-back* se adaptează noilor provocări tehnologice, dar ocolesc teme importante pentru individ cum ar fi respectarea drepturilor sale fundamentale, a căror recunoaștere și reglementare au costat ani buni de luptă și fundamentare filosofico-juridică.

În contextul în care viața cetățeanului migrează din ce în ce mai mult către spațiul virtual, cu toate elementele ei – internet banking, telemedicină, informare și cercetare din surse digitale, comerț electronic, *virtual dating*, *virtual reality* – măsurile de protecție a spațiului cibernetic trebuie gândite în directă corelare cu măsurile de securitate aplicate în mediul off-line. Dacă mediul off-line este clar determinat și există actori cu roluri clare (state, teritorii administrative, instituții cu atribuții în domeniul securității și siguranței cetățeanului etc.), spațiul virtual este încă o junglă, fără limite cunoscute și cu organisme

de supraveghere în stadiu incipient de dezvoltare care ar trebui să poată proteja utilizatorii vulnerabili în cazul în care devin victime ale unor manipulatori digitali.

La acest moment Organizația Națiunilor Unite, prin comisiile și grupurile de experți, și-a asumat rolul de garant al drepturilor omului în spațiul cibernetic, interpretând prevederile tratatelor internaționale și elaborând recomandări pentru conflictele cibernetice și parteneriatul dintre state și marile companii care dețin controlul tehnologic asupra Internetului, atât din perspectiva conținutului cât și al conexiunilor informatice.

La nivelul Uniunii Europene, rolul instituțiilor comunitare, fiind bine definit în ceea ce privește elaborarea și implementarea normelor de drept, permite creionarea unui cadru legal coerent în ceea ce privește politica de securitate cibernetică, asigurarea unui sistem efectiv de protecție bazat pe cooperarea dintre statele membre, dar și protecția efectivă a drepturilor individuale în mediul online. Tradiția democratică a statelor europene contribuie la identificarea unor soluții viabile în ceea ce privește libertatea spațiului cibernetic și importanța individului în societate. Apariția și întărirea rolului ENISA în politica europeană de securitate cibernetică oferă avantajul uniformizării, centralizării și exploatării coerente a datelor raportate de statele membre în vederea elaborării unor reglementări corect fundamentate.

Teza studiază și categoriile de drepturi fundamentale din perspectiva modului în care acestea se văd influențate de noua realitate a vieții cotidiene. Mediul în care aceste drepturi au fost studiate și conceptualizate de-a lungul istoriei până la momentul proclamării lor în diverse instrumente de drept internațional, s-a schimbat profund. Amenințările încep să fie altele decât cele cunoscute, iar pentru juriști, eminamente atehnici, este o mare provocare identificarea breșelor din mecanismele de garantare și protecție a drepturilor fundamentale atunci când individul acționează în mediul online. Este posibil ca generația juriștilor *nativi digitali* să preia munca juriștilor *adaptați digitali* și să poată construi un sistem legal aplicabil acestui nou mediu de viață al individului, dar acest lucru va fi posibil abia peste 10 ani când noua generație, născută în epoca noilor tehnologii, va avea capacitatea de a analiza și propune soluții juridice.

Cercetarea s-a focalizat cu precădere asupra dreptului la viață privată și a elementelor care îl compun, considerat fiind ca unul dintre cele mai vulnerabile drepturi fundamentale în mediul on line. Drepturile derivate, precum dreptul la nume, la identitate, la onoare, la demnitate, la integritate fizică se transformă și capătă noi valențe în era noilor

tehnologii. O parte dintre aceste drepturi se transformă, migrează în spațiul cibernetic, se atașează ființei virtuale și devin drepturi digitale, specifice noului mediul de viață socială. În cuprinsul tezei a fost dezvoltat un capitol dedicat acestei noi categorii de drepturi în care se încearcă stabilirea conținutului și a formei de manifestare.

În ceea ce privește mecanismele de garantare a exercițiului drepturilor și libertăților fundamentale, lucrarea analizează diversele niveluri de protecție: de la nivelul suprastatal (internațional), la cel regional și cel național, specific fiecărui stat. Mecanismele instituționale și jurisdicționale se organizează în mare parte după aceleași reguli fiind ghidate de reglementările internaționale în materia drepturilor omului, cu precădere, continuând cu reglementările la nivel regional și statal. În noul context tehnologic, inclusiv aceste mecanisme necesită o revizuire astfel încât să își poată păstra eficiența dorită la momentul creării lor.

Un punct important al lucrării îl reprezintă analiza restrângerilor aplicate drepturilor omului sub imperiul legii. Așadar nu ne referim la ingerințele aflate în sfera ilegalului, ci la ingerințele permise de lege, în special în numele securității colective. Aici apar dezbaterile și analizele care vizează stabilirea punctului de echilibru între importanța unui drept fundamental sau al altuia. Atât dreptul la viață privată, cât și dreptul la securitate sunt considerate fundamentale, dar nu absolute. Din această perspectivă, trebuie stabilite limite clare astfel încât protejarea unuia să nu afecteze integritatea celuilalt. Uneori statele stabilesc măsuri restrictive exagerate asupra dreptului la viață privată în numele securității naționale, iar spațiul cibernetic este mediul propice pentru acest gen de practici. Orice practică de acest gen, aflată la una dintre cele două extreme, fie intrusivă în sfera personală, fie ineficientă din perspectiva securității, trebuie reevaluată și corelată cu drepturile omului, atât din perspectivă individuală cât și colectivă. De exemplu, dreptul la viață privată sau dreptul la securitate al ființei umane poate restrânge, în limite rezonabile, dreptul altei persoane de a se exprima sau de a-și manifesta anumite nevoi psihice în spațiul digital.

Ținând cont de obiectivele propuse, cu aplicarea metodelor de cercetare asumate și analizând literatura de specialitate, cadrul normativ în vigoare și jurisprudența referitoare la drepturile omului, această teză identifică și subliniază interacțiunea dintre drepturile fundamentale ale ființei umane și efectele sociale ale noilor tehnologii, inclusiv consecințele asupra drepturilor conexe.

În acest context deosebit de dinamic, cea mai mare provocare pentru noua generație de juriști va fi adaptarea cadrului legal în vigoare la noile realități ale lumii digitale. În condițiile în care normele de drept care ne guvernează viața de zi cu zi au avut o evoluție lentă și extinsă pe o perioadă lungă de timp, evoluția tehnologică rapidă și migrarea individului în spațiul virtual impun o adaptare urgentă a cadrului legal la noile realități astfel încât norma de drept să își poată păstra misiunea de gardian al binelui public.

Mai mult, această nouă pandemie, cu origini și cauze incerte, aprig dezbătute în mediul online, a determinat o restrângere în masă a drepturilor omului poate la fel de acerbă cu cea provocată de ultimul război mondial. Ne-au fost restrânse pe rând dreptul la libertatea de mișcare, dreptul la întruniri, dreptul la manifestări, dreptul la exprimare, dreptul la educație, dreptul la muncă și inclusiv dreptul la căutarea fericirii. Iar oamenii, de teama inamicului nevăzut și neînțeles, au acceptat în cea mai mare parte toate aceste ingerințe ale autorităților în viața lor privată și în cercul libertăților lor fundamentale. Grupuri mici de activiști continuă lupta de apărare a drepturilor lor fundamentale. Nu știm dacă acest eveniment global numit pandemie va rescrie istoria drepturilor fundamentale, dar cert este că impactul lui asupra sferei libertăților individuale a avut un efect mult mai abrupt și mai intrusiv decât orice altă transformare, inclusiv cea tehnologică.

În aceste condiții, ne rămâne o singură opțiune: aceea de a apăra individul, cu toate atributele sale, într-o societate dinamică, caracterizată de transformări atipice.

ABSTRACT FOR THE INTERNATIONAL DOCTORATE NOTE

Cyberspace - the last frontier. This is where the mission of the lawyers begins: to search new forms of human rights manifestation. Fortunately, it is not a science-fiction mission, but a real, current and full of opportunities challenge. We consider that this is the best-chosen moment to propose this paper and to initiate a research work on the dynamics of law under the era of new technologies. Because this era has just begun.

This thesis aims to explore this new space where the human being, holder of fundamental rights and freedoms, has entered. Like any new environment, the digital world arouses curiosity, engages the human need to explore but also activates the need to be safe. The human being is genetically programmed to protect his life, integrity and freedom in any type of environment, no matter if is real or virtual.

Cybersecurity is a new topic; this topic has been brought in public debates only since 1988. States, private companies and specialists have quickly become aware of the need of regulation in this area, including by adapting international law to new realities.

Conflicts, as frequent events in human society, have rapidly migrated from physical to the virtual space. The weapons as well. Cyber viruses, spyware, worms, malware took the place of the classic weapons and tools of war. The proposed security measures were implemented by state authorities with responsibilities in the field of national security, as well as by private companies. The efforts made to develop programs to fight against cyber-attacks, based on cyber espionage or hack-back measures, must be adapted to ever new technological challenges, but not forgetting the important issues for the individual human being, such the respect for his fundamental rights, whose recognition and regulation have cost years of legal struggle and philosophical debates.

In this context, where the life of the citizen migrates more and more to the virtual space, with all its elements - internet banking, telemedicine, information and research from digital sources, electronic commerce, virtual dating, virtual reality – protective measures for cyberspace must designed in direct correlation with the security measures applied in the offline environment.

If the offline environment is clearly determined, populated with actors playing key roles (states, administrative territories, institutions with responsibilities in the field of

security and safety of citizens, etc.), the virtual space is still a jungle, with unknown limits and incipient supervisory bodies struggling to protect vulnerable users against digital criminals.

At this moment, the United Nations, through its commissions and expert groups, has taken on the role of human rights protector in cyberspace, interpreting the provisions of international treaties and developing recommendations for cyber conflicts and partnerships between states and large companies with technological control over the Internet, both in terms of digital content and computer connections.

In the European Union, the specific role of the public institutions in the legal area allows drafting a coherent legal framework for cybersecurity policy, ensuring an effective system of protection based on cooperation between Member States, also bringing an effective protection of individual rights in the online environment. Also, the democratic tradition of Member States contributes in finding viable solutions regarding the freedom of cyberspace respecting, in the same time, the social importance of the human being. The creation on ENISA, with its determined role in the European cybersecurity policy, offers the advantage of a coherent approach in standardizing, centralizing and exploiting the data reported by Member States in order to develop well-founded regulations.

The thesis also studies some categories of fundamental rights observing the new perspective of human liberty and privacy induced by technology and digitalization of reality. It is obvious that the initial environment where these rights have been studied and conceptualized has radically changed and their legal confirmation in the international law must be adapted to the new reality.

The new digital threats to human fundamental rights are different from the known ones, and for the lawyers, who are non-technical by nature, it is a great challenge to identify the gaps in the informatics mechanisms of protecting fundamental rights when the person acts in the online environment. Maybe the generation of digital native lawyers will take over the work of digitally adapted lawyers and will be able to build a legal system applicable to this new living environment of the individual, but this success will be possible only after the next 10 years, when the new generation, born in the age of new technologies, will have the ability to analyze and propose legal solutions.

The research focused mainly on the right to privacy and its legal components, being considered as one of the most vulnerable fundamental rights in the online environment. Connected human rights, such as the right to a name and to a nationality, identity, honor, dignity, physical integrity, are transforming and gaining new values in the era of technology. Some of these rights are reinvented and relocated into cyberspace, where they attach to the virtual human being and become digital rights, specific to the digital social environment. In the thesis there we dedicated a chapter to this new category of human liberties, aiming to establish the content and the limits of these new digital rights.

Regarding the mechanisms for guaranteeing the exercise of fundamental rights and freedoms, the paper analyzes the various levels of protection: from the supranational (international) level, to the regional and national level, specific to each state.

The institutional and jurisdictional mechanisms are largely organized according to the same rules, being guided by international human rights framework, at a global level, and particularly regulated by regional or local specific legal regulations. In the new technological context, these mechanisms need to be revised so that they can maintain their desired efficiency as the moment of their creation.

Another important point of this paper is the analysis of the restrictions applied to human rights under the rule of law. So, we are not referring to any illegal interference, but we analyze the limitations allowed by law, especially in the name of collective security. This is the point where debates and analyzes converge in finding the perfect balance between the importance of one fundamental right to another. Both right to privacy and right to security are considered fundamental, but not absolute. From this perspective, clear boundaries must be set so that the exercise of one right does not affect the integrity of the other. Sometimes states impose overly restrictive measures on the right to privacy in the name of national security, and cyberspace is the perfect environment for such practices.

Any practice situated at one of the two extremes, either intrusive in the personal sphere or inefficient from a security perspective, must be re-evaluated and correlated with the human rights, both from an individual and a collective perspective. For example, the right to privacy or the right to security of one person may interfere, in reasonable limits,

with the right of another person to express himself or herself or to manifest certain psychical needs in the digital space.

Fallowing the proposed objectives, applying the specific research methods and analyzing the legal literature, the regulatory framework and the jurisprudence on human rights, this thesis identifies and emphasizes the interaction between fundamental human rights and the social effects of the new technologies, including the consequences on related rights.

In this particularly dynamic context, the biggest challenge for the new generation of lawyers will be to adapt the current legal framework to the new realities of the digital world. Given that the rules of law governing our daily lives have a long and slow evolution, this rapid technological revolution and the migration of the individual into virtual space urge for a quick adjustment of the legal framework to new realities so that the rule of law to be able to keep its mission of guardian of the public welfare.

Moreover, this new pandemic, with uncertain origins and causes, hotly debated in the online environment, has led to a more severe human rights restriction than the last world war. We have been restricted in our right to freedom of movement, right to public meeting, right to manifestation, right to expression, right to education, right to work and even our right to pursue happiness. Under the fear of the unseen and unknown enemy, people accepted the most part all these interferences from the authorities in their private lives and in their circle of fundamental freedoms.

Small groups of activists continue the fight to defend their fundamental rights. We do not know whether this global event called the pandemic will rewrite the history of fundamental rights, but it is certain that its impact on the individual freedoms has already determined a huge and more intrusive impact than any other transformation, including technological.

Under these conditions, we have only one challenge: to defend the human individual in this dynamic society, with all its attributes, characterized by atypical transformations.

INTRODUCCIÓN

Actualmente, la sociedad cambia y se moviliza de la calle a las redes sociales y las plataformas. El mundo cambia y el mundo material se convierte cada vez más en mundo virtual. La sociedad moderna evoluciona, cambia, y se traslada a las redes sociales y plataformas virtuales, conllevando a que nuestros sentimientos se manifiesten en frases cortas y emoticones. La comunicación se comprime en palabras cortas o cortadas, las cartas se transforman en e-mails de máximo dos frases, y el tiempo ya no es suficiente para ninguno de nuestros planes.

En toda esta tormenta de transformaciones, ¿qué vamos a hacer con nuestras reglas de convivencia y con nuestro sistema legal?, todos los principios y las reglas de nuestra sociedad tienen que trasladarse en la nueva sociedad cibernética. Es el momento cuando el Derecho, como ciencia social, está enfrentando un gran desafío: el de adaptarse al espacio abierto creado en Internet o caer en desuso.

El www (World Wide Web) se está organizando y pasa desde el simple usuario a las comunidades virtuales, lo que implica la importación de las reglas sociales en el mundo virtual. Siendo también, el momento idóneo para reformar y mejorar los sistemas sociales y jurídicos.

En la sociedad clásica estamos acostumbrados a ser protegidos por varias autoridades que vigilan que nuestros derechos fundamentales estén garantizados: la libertad, la integridad física, la propiedad, la seguridad etc. ¿Pero en la sociedad virtual, quien vigila nuestros derechos y garantiza su respeto ante cualquier violación?

Al mismo tiempo, es importante conocer el coste de la protección del ser humano en el espacio cibernético. La presente tesis trata de identificar los derechos fundamentales más vulnerables en el nuevo entorno online y a las autoridades responsables para protegerlos.

Al mismo tiempo, se analizará el precio justo de la seguridad cibernética, de una forma analógica con la seguridad individual que gozamos todos los días en nuestras sociedades clásicas[2]. Como ya sabemos, a veces el precio de la seguridad es la limitación de otros derechos fundamentales del ser humano, como el derecho a la vida privada (vigilancia, intervención de conversaciones privadas, etc.), el derecho de la libertad (detención de posibles de infractores), el derecho a la libre expresión (censura de los

[2] Hurtaud, S. (2014) *Cyber security. Time for a new paradigm*. Information & Technology Risk. Editorial Deloitte, pp. 90-95

materiales o medios con contenidos ilícitos o inmorales), el derecho a la libertad de movimiento o a moverse libremente (prohibición de inmigración ilegal) y otros derechos de la persona que interfieren con las reglas sociales cuando se ejercen más allá de los límites establecidos.

Al principio las redes de Internet nacieron libres, como un espacio donde el internauta puede manifestarse de cualquier manera según sus propios límites. Una situación similar al jardín de Edén. Pero, con el tiempo, la cantidad de usuarios virtuales ha aumentado y el entorno digital se transformó en un laberinto y en una verdadera Torre Babel, donde cada usuario habla su idioma y expresa variedad de pensamientos, según sus intereses. Es el crecimiento de internet, su uso masivo y la aparición de cada vez más conflictos cuando hizo pensar que era necesario regularlo[3]. Se pensó en la necesidad de crear reglamentos y organismos de control para su uso correcto.

Después de la aparición de los organismos de reglamentación y vigilancia en Internet, todos los problemas relacionados con la intervención de tales organismos en la vida privada de la ciudadanía aparecieron. Había que fijar un marco legal claro que estableciera la frontera clara entre la necesidad de controlar el espaciador virtual de internet y la protección de los derechos y las libertades de los internautas. Para las organizaciones de Derechos Humanos hay un peligro de restricción de derechos humanos en las redes digitales. Los activistas de los derechos humanos han trasladado su lucha en el entorno digital: "mantener el Internet libre y abierto" es el eslogan de todas sus manifestaciones virtuales. Pero ninguno de estos activistas propone las soluciones para la seguridad cibernética del ser humano (el usuario virtual) que también es uno de nuestros derechos fundamentales muy relacionado con el derecho a la vida. El derecho a la seguridad garantiza el pleno cumplimiento de los demás derechos fundamentales del ser humano y el libre ejercicio de estos derechos en los límites establecidos por los derechos de los demás.

Pues el derecho a la seguridad cibernética del usuario permite que este individuo se manifieste libre y protegido en el entorno online, sin tener miedo de que sus datos personales puedan ser robados, que sus derechos de propiedad intelectual no van a ser vulnerados, que su intimidad no será violada por otros usuarios, que sus conversaciones no serán publicadas sin su consentimiento. Para garantizar su derecho a la seguridad cibernética algunos organismos tienen que "vigilar" el entorno virtual.

---

[3] Kurbalija, J y Gelbstein, E. (2005) *Gobernanza de Internet: Asuntos, Actores y Brechas*, Editorial DiploFoundation y la Sociedad para el Conocimiento Mundial, p. 82,

Igual que en la sociedad clásica, a veces, los estados y las autoridades responsables para "vigilar" el respecto de las normas sociales y la seguridad del individuo pasan un poco más de los límites e intervienen en la vida privada de las personas "un poco más de lo que se debe". Por estas razones la sociedad internacional estableció reglas y límites de la intervención de las autoridades en la vida de los protegidos. Al mismo tiempo, organizaciones y organismos internacionales y estatales están analizando y sacando a la luz los casos de abuso por parte de los estados o las autoridades.

El mundo virtual abrió oportunidades tanto para las personas como para Estados y organismo privados. El ciber espionaje internacional, patrocinado por los Estados, ha dado luz a nuevas nociones como *"guerra cibernética"* y a una nueva industria de armas cibernéticas[4]. Las nuevas historias están siendo utilizadas en algunas partes del mundo para animar a los ciudadanos a renunciar a las libertades civiles para una mayor sensación de seguridad[5]. En los EE. UU., por ejemplo, el espionaje cibernético practicado por los hackers chinos es un argumento clave que se utiliza para apoyar la controvertida ley "*Cyber Intelligence Sharing and Protection Act"* (CISPA) que permitiría a las autoridades acceder a grandes cantidades de datos de usuarios sin una orden judicial.

En otros lugares, las amenazas internas a la seguridad nacional que plantea el uso de las nuevas tecnologías han sido utilizadas para justificar extensas medidas de vigilancia[6]. Por ejemplo, en India, no es posible acceder a los teléfonos móviles o a conexiones de Internet, incluso en los cibercafés, sin identificación oficial, y se requiere a los proveedores de Internet y los cibercafés que mantengan registros detallados de la historia de la navegación de los usuarios.

Las narrativas de la fatalidad que invariablemente acompañan a dichas medidas se basan aún más en la fuerza del crecimiento real de la delincuencia cibernética - que ahora se dice que hay más de 150.000 virus y otros tipos de código malicioso en circulación, con un millón de personas que se convierten en víctimas de delitos cibernéticos cada día[7].

---

[4] Gómez, A. (2012) *El ciberespacio como escenario de conflicto. Identificación de las amenazas*, en El ciberespacio. Nuevo escenario de confrontación, Madrid, Ed. Ministerio de Defensa, pp. 167-204

[5] Pepitone, J. (2013) *Cybersecurity lobbying doubled in 2012*. CNN Money (New York). The Cybercrime Economy, Recuperado de: https://money.cnn.com/2013/04/08/technology/security/cybersecurity-lobbying/index.html#_blank.

[6] Glenny, M. (2011) *DarkMarket: Cyberthieves, Cybercops and You*. Editorial Knopf; Canadian First edition, p. 217.

[7] Deibert R. (2012) *The Growing Dark Side of Cyberspace (. . . and What To Do About It)*, Penn State Journal of Law & International Affairs, vol. I, Issue 2, p. 260.
Recuperado de: https://elibrary.law.psu.edu/jlia/vol1/iss2/3.

De esta manera el tema de la seguridad cibernética y la protección de los derechos de la ciudadanía en las redes preocupa cada vez y es un tema controversial. Sobre este problema se pronuncian cada vez más los Estados y los agentes políticos y sociales, también del ámbito internacional.

En realidad, existen amenazas reales y van en aumento. El acceso ilegal a los datos y a las computadoras, así como la interferencia de datos, se han convertido en problemas más comunes y complejos que afectan a un gran número de personas. Temas como: el fraude está adoptando nuevas formas en Internet, y a medida que más de nuestra infraestructura crítica se vuelve dependiente de Internet, las infracciones de seguridad pueden tener repercusiones significativas, incluyendo afectación de los derechos humanos cuando, por ejemplo, un ataque impide que las personas accedan a los servicios públicos o al ejercicio de su derecho a la expresión.

La obligación de los Estados es garantizar los derechos y libertades dentro de su territorio y cambien en este tema, no tan nuevo ya, del uso masivo de las redes y la criminalidad que le acompaña[8].

Sin embargo, las estrategias de seguridad cibernética deben ser diseñadas e implementadas de una manera que es convergente con el derecho internacional de los derechos humanos - con demasiada frecuencia esto no es el caso, como se ve en los regímenes de vigilancia descritos anteriormente. La aplicación de las normas de protección de derechos humanos a las políticas de Seguridad Cibernética se basará, en primer lugar, en la familiarización de todos los actores implicados con las normas de derechos humanos y la promoción de manera coherente[9].

En otros casos, se encontró incluso, Estados que están detrás de las amenazas como los ataques cibernéticos dirigidos hacia los defensores de los derechos humanos o la oposición política. Por tanto, es importante que la comunidad de derechos humanos empiece a comprometerse con estos discursos más de cerca, para anular las amenazas contra los mismos. Además, deben ofrecer propuestas de solución para que no se repitan y garanticen las reglas y normas de derechos humanos también en las redes digitales, garantizando la seguridad cibernética a la vez.

[8] Torrecuadrada, S. (2013) *Internet y el uso de la fuerza*, en Ciberseguridad global. Oportunidades y compromisos en el uso del ciberespacio, Granada, Ed. Universidad de Granada, pp. 91-118.
[9] Shackelford, S. J. (2009) *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*. Berkley Journal of International Law, Vol. 25, No. 3/2009, recuperado de: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1396375

La investigación realizada en la presente tesis busca identificar y analizar los puntos neurálgicos en el conjunto de los derechos fundamentales que se activan con la interacción del ser humano y el mundo virtual. El principal objetivo de esta tesis es de establecer los límites de las intrusiones legales sobre los derechos individuales por parte de las autoridades, usando las nuevas tecnologías y el Internet. Para encontrar respuestas a las preguntas que se formularán más adelante, se utilizó diversas fuentes de información como: los textos de los tratados internacionales y convenios regionales sobre los derechos humanos, los textos constitucionales de diferentes países, pero con acento especial sobre el marco jurídico de España y Rumania, la doctrina constitucional emanada de los órganos jurisdiccionales, y los pronunciamientos doctrinales.

Entre los métodos de investigación empleados para llegar a las conclusiones perseguidas mencionamos el método comparativo (se han comparado las normas que regulan los derechos fundamentales en distintos sistemas de derecho), el método histórico (presentando la evolución de los derechos en los últimos años), el método correlacional y el método deductivo para proponer soluciones adaptadas a los nuevos desafíos.

La tesis se desarrollará en ocho capítulos que tratan sobre los problemas y desafíos jurídicos mencionados en los párrafos anteriores. En líneas generales, la investigación se centra en buscar respuestas a tres grandes preguntas sobre el contenido de la noción de *seguridad cibernética*, la existencia de un estado de derecho en el entorno digital y la posibilidad de regular la conducta del usuario en el espacio virtual en armonía con los intereses de seguridad colectiva y el respeto de los derechos humanos.

¿Qué es la seguridad cibernética?

En la actualidad, el término *seguridad cibernética* goza de varias definiciones, ya que se utiliza para cubrir una amplia gama de preocupaciones: en diferentes contextos y por diferentes actores, el término se utiliza para referirse a la seguridad de la infraestructura nacional; la seguridad de la infraestructura de Internet; la seguridad de las aplicaciones y servicios; la seguridad de los usuarios (que van desde las empresas a los usuarios individuales); a la estabilidad del Estado y de las estructuras políticas[10].

[10] Robinson, N. (2014): *EU cyber-defence: a work in progress*. EU Institute for Security Studies, vol.10, pp 1-10, recuperado de: http://www.iss.europa.eu/uploads/media/Brief_10_Cyber_defence.pdf.

De acuerdo con la Comisión Europea, la ciberseguridad representa "*todas las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciber amenazas*"[11].

Citando a Kaspersky, una de las más importantes compañías internacionales dedicadas a la seguridad informática, con presencia en aproximadamente 195 países del mundo (su sede central en Rusia, mientras que el holding está registrado en Reino Unido):

> *"La ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil, y puede dividirse en algunas categorías comunes"*[12].

Esta terminología apunta a una de las principales preocupaciones acerca de este discurso en crecimiento: la terminología cubre una agenda que es inexacta, que mezcla preocupaciones legítimas e ilegítimas y fusiona diferentes tipos y niveles de riesgo. Esto evita que el escrutinio verdadero, objetiva e inevitablemente, conduzca a respuestas que son de amplio alcance y pueden ser fácilmente usadas de manera indebida o abusiva.

El uso de un lenguaje cargado y ambiguo puede determinar, de hecho, consecuencias de gran alcance, ya que muchos gobiernos están utilizando vagas amenazas internas y externas como argumentos para justificar cada vez mayores inversiones en armas cibernéticas y sistemas de vigilancia masiva y cada vez mayor control gubernamental sobre el Internet y sobre sus ciudadanos[13].

La sensación de alarma o peligro inminente, incorporada en las narrativas de seguridad cibernética, representa una forma de manipulación de la mente humana para aceptar la limitación de sus derechos en nombre de la seguridad. No obstante, en 2020 el peligro de contaminación con el coronavirus COVID 19 ha determinado una histeria global, aunque los datos sobre el virus, la manera de transmisión y sus efectos son controversiales. Los estados y los individuos se han alarmado de una manera tan fuerte

---

[11] Artículo 2 (1) del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) no 526/2013 (en adelante Reglamento sobre la Ciberseguridad)

[12] Eugene Kaspersky – cofundador y Director General de Kaspersky, el proveedor privado de soluciones de ciberseguridad y protección de endpoints más grande del mundo. Mas información en: https://latam.kaspersky.com/about/team.

[13] Farwell, J.P. y Rohozinski, R. (2011) *Stuxnet and the Future of Cyber War*, Revista Survival, Global Politics and Strategy , vol. 53, issue 1, pp. 23-40.

que los derechos fundamentales pasaron a segundo plano, siendo limitados, restringidos con el acepto general de las mases. Aunque todavía estamos viviendo este experimento, nuestros derechos están siendo limitados, con la justificación de preservar otro derecho fundamental que es el derecho a la salud y a la seguridad. La amenaza de un peligro inminente, invisible, no detectable parece ser motivo suficiente para que la ciudadanía renuncie a derechos fundamentales.

La histeria social originada por la idea de un ataque inminente físico, cibernético, médico, puede crear la opinión de que todas las respuestas son válidas y legítimas, de manera acrítica. Por ejemplo, como se manifestó anteriormente, en muchos países, tanto democráticos y no democráticos, las amenazas a la seguridad nacional han sido utilizadas para justificar los mecanismos de vigilancia amplios, con más y más datos de los ciudadanos recogidos y de fácil acceso por las autoridades estatales.

Otras medidas nefastas de "seguridad" incluyen el desarrollo de los llamados "interruptores de Internet" (la noción de cierre de Internet con el fin de protegerlo), que restringe el uso de la encriptación, la implementación de mecanismos de filtrado y bloqueo y la introducción de políticas de nombres reales[14]. Estas medidas que representan una amenaza para las libertades civiles, sin embargo, tienden a carecer de supervisión judicial.

¿Cómo se protegen los derechos humanos en el entorno online y cuáles son las perspectivas sobre el futuro democrático del Internet?

"*Los mismos derechos que tienen las personas fuera de la línea también deben ser protegidos en línea*"[15] - esta simple declaración, aprobada por una resolución del Consejo de Derechos Humanos de la ONU el 2 de junio de 2012, confirma lo que parecía evidente para los activistas de derechos humanos desde hace muchos años. Aunque otros derechos humanos (como el derecho de reunión y asociación pacíficas, el derecho a un recurso efectivo y la presunción de inocencia) también son pertinentes, dos derechos humanos en particular formarán los elementos básicos de los enfoques de la seguridad cibernética que respetan los derechos. Uno de estos es el derecho a la vida privada, o el derecho de mantener los datos y la comunicación fuera de los ojos del gobierno, las empresas u otros ciudadanos. El derecho a la vida privada es un componente necesario en

[14] Perlroth, N. (2013) *Researchers Find 25 Countries Using Surveillance Software*, The New York Time Journal. Recuperado de: https://bits.blogs.nytimes.com/2013/03/13/researchers-find-25-countries-using-surveillance-software/.
[15] Consejo de Derechos Humanos (2012) *Promoción, protección y disfrute de los derechos humanos en Internet* (A/HRC/20/L.13), New York, United Nations General Assembly, 29 June 2012.

el desarrollo de una política de seguridad centrada en el ciudadano. Sin embargo, no es suficiente, ya que no cumple todos los requisitos para estar uno seguro en línea de la manera que hemos definido anteriormente. Por ejemplo, el derecho a la vida privada no ofrece salvaguardias suficientes contra los controles de contenido instituidos por los gobiernos en el nombre de las políticas de seguridad en los puntos donde los cables de Internet entran en un país.

En la evaluación de las políticas de seguridad cibernética se debe otorgar la misma importancia al disfrute sustantivo por parte de todos los ciudadanos del derecho a la libertad de expresión. La libertad de expresión se ve interferida cuando una acción impide que alguien busque, reciba o imparte otra expresión que no sea la legítimamente limitada, y acciones que desalienta o inhibe esa expresión.

Ambos derechos pueden ser restringidos bajo ciertas circunstancias y solo si tal restricción está prevista por la ley. Sin embargo, las interferencias con la libertad de expresión solo serán legítimas si siguen la prueba acumulativa tripartita que está prevista por la ley, es decir legalidad, proporcionalidad y necesidad.

Asimismo, las interferencias con el derecho a la vida privada requieren que "*debe existir una ley que defina claramente las condiciones por las cuales el derecho de los individuos a la privacidad puede ser restringido en circunstancias excepcionales y las medidas que invaden este derecho deben tomarse sobre la base de una decisión específica por una autoridad estatal expresamente facultada por la ley para hacerlo, generalmente el poder judicial, con el fin de proteger los derechos de los demás, por ejemplo para obtener pruebas que impidan la comisión de un delito y deben respetar el principio de proporcionalidad*"[16].

Según el Relator Especial existen algunas situaciones cuando es posible y recomendable restringir el derecho a la libre expresión:

> *"En este sentido, entre los tipos legítimos de información que pueden restringirse cabe mencionar la pornografía infantil (para proteger los derechos del niño), la incitación verbal al odio (para proteger los derechos de las comunidades afectadas), la difamación (para proteger los derechos y la reputación de los demás contra ataques injustificados), la incitación directa y pública a cometer actos de genocidio (para proteger los derechos de los demás)*

[16] Frank La Rue (2011) *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión*, New York, Asamblea General de las naciones Unidas, 16 de Mayo 2011. Recuperado de: https://www.acnur.org/fileadmin/Documentos/BDL/2015/10048.pdf.

y el fomento del odio nacional, racial o religioso que constituya incitación a la discriminación, hostilidad o violencia (para proteger los derechos de los demás, como el derecho a la vida)"[17].

Estos términos y pruebas han sido desarrollados y elaborados a través de la jurisprudencia y normas de derecho indicativo[18] *"soft law"*. Cualquier medida de seguridad que no se adhiera a estos criterios estrictos, aunque posiblemente incremente la seguridad de la red afecta la seguridad sustantiva del pueblo. Es muy importante que existan claros límites legales internacionales sobre las acciones que pueden tomar legalmente en el dominio cibernético. Leyes y prácticas que interfieren con los derechos humanos en línea sólo son legítimas en la medida en la que caen dentro de los estrechos límites permitidos por la ley internacional de derechos humanos. Por tanto, es necesario volver a examinar la agenda de seguridad cibernética a la luz de las normas y valores de los derechos humanos.

Sin embargo, la vigilancia tiene que ser necesaria y proporcionada a la amenaza[19]. Con frecuencia, estas condiciones quedan sin cumplirse. En lugar de apoyarse unos a otros, la seguridad informática y la vigilancia están en frecuente desacuerdo. Si a desarrollar políticas de seguridad informática que apoyan fundamentalmente los derechos humanos, es esencial que esto se reconozca y se contabilice el estado de derecho que existe en el mundo físico, offline, debe trasladarse con todos sus elementos y principios al entorno online.

Las políticas de seguridad informática no deberían limitarse a desempeñar un papel defensivo, sino un papel facilitador, poniendo efectivamente la autonomía y el bienestar de las personas en su centro. Con la finalidad de evaluar la eficacia de una medida de seguridad cibernética, es esencial tener en cuenta no sólo el impacto potencial de las diversas amenazas a la seguridad cibernética, sino también las soluciones propuestas. Si una medida, aplicada para proteger a las personas, afecta ella misma los derechos humanos, de tal manera y en tal medida que incluso limita la capacidad de las personas para acceder y utilizar el Internet, no puede ser considerada como una medida de seguridad razonable.

---

[17] Ibidem.

[18] El derecho indicativo (soft law) representa "un conjunto de instrumentos jurídicos de carácter no vinculante que, sin embargo, aspiran a influir en la legislación vinculante indicando un camino al que se aspira llegar. Es el antónimo de derecho imperativo" (hard law) – **RAE: Diccionario panhispánico del español jurídico.**

[19] Deibert, R. (2012) idem.

¿Es posible una Carta Cibernética de Derechos Humanos?

En los últimos años se ha producido una serie de intentos por definir exactamente cómo se aplican las normas internacionales de derechos humanos en el entorno online. Los "*Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones"*[20] es una propuesta de reglamentación elaborada por unos ONG para demonstrar que las normas y estándares internacionales de derechos humanos son aplicables en los casos de la vigilancia de las comunicaciones en el entorno electrónico.

El texto[21] reafirma el carácter fundamental del derecho a la intimidad y subraya la conexión esencial con la dignidad humana, demostrando que las actividades de vigilancia sobre las comunicaciones de las personas tanto en el entorno electrónico como también en el medio real constituye una injerencia con los derechos fundamentales. los principios declaran una vez más que solo la ley puede ser el único fundamento para la intervención de las autoridades en la vida privada de una persona. Para ser autorizada, toda restricción debe lograr un objetivo legítimo, ser idónea, necesaria y proporcional con la amenaza publica que se quiere neutralizar. Los fundamentos y las ideas de estos 13 principios se encuentran regulados en los instrumentos internacionales importantes de derechos humanos como la Declaración Universal de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, la Convención Americana sobre Derechos Humanos y Deberes del Hombre, la Declaración de los Derechos Humanos de ASEAN y la Carta Africana de Derechos Humanos y de los Pueblos.

Los activistas proponen la adopción de un convenio internacional cibernético dedicado a la protección de los derechos humanos, construido sobre una base de estos trece principios fundamentales, dedicados a garantizar una mayor transparencia y un control cívico. El principal objetivo de tal convenio seria la limitación de las injerencias en la vida privada de los individuos para garantizar el respecto de los principios de la democracia participativa.

[20] Los principios, que son el fruto de un trabajo común de los representantes de la sociedad civil y expertos, fueron elaborados y publicados por las organizaciones Access, Artículo 19, Asociación Civil por la Igualdad y la Justicia, Asociación por los Derechos Civiles, Association for Progressive Communications, Bits of Freedom, Center for Internet & Society India, Comisión Colombiana de Juristas, Electronic Frontier Foundation, European Digital Rights, Fundación Karisma, Open Net Korea, Open Rights Group, Privacy International, y Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, entre otros..

[21] El texto integral de los principios es disponible en https://necessaryandproportionate.org/principles/.

El primer principio, el de *la legalidad*, que representa un elemento común para todas las democracias y los estados de derecho, prohíbe cualquier acción contra el derecho de la vida privada de los ciudadanos si no está autorizada por una ley fundamental y no goza de un procedimiento claro, regulado en normas jurídicas con carácter público:

> *"Cualquier limitación al derecho a la privacidad debe ser prescrita por ley. El Estado no debe adoptar o implementar una medida que interfiera con los derechos a la privacidad en ausencia de una ley públicamente disponible, que cumpla con un nivel de claridad y precisión suficientes para asegurar que las personas la conozcan por adelantado y puedan prever su aplicación. Dado el ritmo de los cambios tecnológicos, las leyes que limitan el derecho a la privacidad deben ser objeto de revisión periódica por medio de un proceso legislativo o reglamentario de carácter participativo"*[22].

El principio del *objetivo legítimo* no permite a las autoridades estatales autorizar las actividades de vigilancia sobre los ciudadanos si la investigación no es absolutamente necesaria para proteger los valores de una sociedad democrática. Si el objectivo se puede lograr de otra manera, no se pueden justificar las injerencias en la vida privada. de toda forma, todas estas medidas intrusivas en la vida privada del individuo no deben ser motivadas por razones étnicas, sexuales, religiosas, políticas u otro tipo de discriminación.

> "*Las leyes sólo deberían permitir la vigilancia de las comunicaciones por parte de autoridades estatales específicas para alcanzar un objetivo legítimo que corresponda a un interés jurídico preponderante e importante y que sea necesario en una sociedad democrática. Cualquier medida no debe aplicarse de manera que discrimine con base en raza, color, sexo, idioma, religión, opinión política o de otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición."*[23]

En tercer lugar, la vigilancia de las comunicaciones debe ser absolutamente *necesaria* y puede ser autorizada en base de una ley estatal que la permite de modo exprés. Al mismo tiempo, cuando se elige este modo de investigación se debe analizar si es la única forma de lograr el objectivo legitimo o si existen otras modalidades de defender los valores sociales en peligro. Siempre se debe elegir el método de acción que menos vulnera los derechos fundamentales:

---

[22] Ibidem.
[23] Ibidem.

"Las leyes que permiten la vigilancia de las comunicaciones por el Estado deben limitar dicha vigilancia a lo que es estricta y evidentemente necesario para alcanzar un objetivo legítimo. La vigilancia de las comunicaciones sólo debe llevarse a cabo cuando es el único medio para alcanzar un objetivo legítimo, o bien cuando habiendo varios medios sea el menos propenso a vulnerar los derechos humanos. La carga de establecer esta justificación, tanto en los procesos judiciales como en los legislativos, recae en el Estado"[24].

Según el principio de *la idoneidad,* las medidas de vigilancia se evalúan desde un punto de vista legal y también desde una perspectiva técnica. Para cumplir con este requisito, las medidas deben representar la única manera para cumplir el objectivo legítimo de la intervención, es decir defender derechos o libertades de otros seres humanos.

El principio de *la proporcionalidad* reafirma la necesidad de que la vigilancia de las comunicaciones debe ser autorizada por un juez imparcial y competente únicamente cuando se pruebe:

"En concreto, esto requiere que, si un Estado busca acceder o usar información protegida obtenida a través de vigilancia de las comunicaciones en el marco de una investigación penal, debe establecer ante una autoridad judicial competente, independiente e imparcial que:

1. existe un alto grado de probabilidad de que un grave delito ha sido cometido o será cometido;

2. la evidencia sobre tal delito sería obtenida al acceder a la información protegida que se busca;

3. otras técnicas de investigación que son menos invasivas y están disponibles ya han sido agotadas;

4. la información a la que se accede se limitará a la razonablemente relevante para el presunto delito y cualquier exceso en la información recopilada será destruido o devuelto sin demora, y

5. solo tendrá acceso a la información la autoridad especificada y se utilizará solo para el propósito para el cual se le dio autorización"[25].

El sexto principio se refiere a *la autoridad judicial competente* a tomar las decisiones efectivas sobre el inicio y la aplicación de las medidas de vigilancia. Para tener

[24] Ibidem.
[25] Ibidem.

legitimidad, la autoridad que autoriza las medidas debe ser independente de las autoridades encargadas a desarrollar efectivamente las medidas de vigilancia sobre las comunicaciones. Al mismo tiempo, esta autoridad debe ser reconocida como un organismo experto en el ámbito de la legalidad y puede tener la capacidad institucional para tomar decisiones judiciales relacionadas con actividades de vigilancia, tecnologías de vigilancia y procedimientos legales efectivos. La autoridad debe trabajar con expertos en materia de derechos humanos, de limitación de las libertades fundamentales y seguridad nacional.

Según el principio del *debido proceso,* ningún procedimiento legal no puede estar fuera del marco jurídico relativo al respeto de los derechos humanos y de la vigilancia sobre las comunicaciones de las personas. En este sentido, cualquier medida de restricción de la libertad humana debe ser autorizada por un juez o un tribunal independiente, después de un análisis riguroso de los motivos que justifican tal injerencia en la vida privada de una persona. La persona cuyos derechos se restringen puede pedir, dentro de un plazo razonable, una audiencia pública y justa ante una instancia judicial independiente e imparcial, legal constituida, para defender sus libertades fundamentales. Existe la posibilidad de denegar este derecho solo en caso de emergencia cuando corre un riesgo inminente de peligro para la vida humana. Cuando ocurre este tipo de situación es posible autorizar con efecto retroactivo las medidas de restricción, pero el mero riesgo de fuga o de destrucción de pruebas no representa un motivo legal y suficiente para la autorización.

Todas las personas que han sido objeto de vigilancia deben ser notificadas sobre las medidas que se han tomado, según *el principio de la información*. Solo si se puede demonstrar que existen riesgos para alcanzar el objectivo legítimo que justifica las medidas o corre un peligro para la vida de una persona, es posible eludir esta obligación de notificación:

> *"El retraso en la notificación solo se justifica en las siguientes circunstancias:*
>
> *1. La notificación pondría en serio peligro la finalidad para la que se autoriza la vigilancia, o existe un riesgo inminente de peligro para la vida humana; y*
>
> *2. La autorización para retrasar la notificación es otorgada por la autoridad judicial competente en el momento en que se concede la autorización para la vigilancia; y*
>
> *3. La persona afectada es notificada tan pronto como el riesgo desaparece o dentro de un período de tiempo razonable y factible, según lo que ocurra*

primero, y en todo caso en el momento en que la vigilancia de las comunicaciones se ha completado"[26].

La transparencia de las decisiones y de los procedimientos relativos a las medidas de vigilancia es un principio que requiere la publicación de los textos legales, reglamentaciones e instrucciones relativos al uso, alcance, desarrollo y estadísticas generales de los procedimientos de vigilancia.

El principio de *la supervisión pública* requiere la adopción de una legislación especial relativa a la vigilancia de las comunicaciones y también la organización y el desarrollo de instituciones y mecanismos de supervisión pública de este tipo de actividades.

A base del principio de *integridad de las comunicaciones y sistemas* ningún estado no tiene la permisión de obligar o de recomendar a los proveedores de infraestructuras de comunicaciones que ponga a su disposición o que permita a desarrollar actividades de vigilancia de las comunicaciones de los usuarios o control y recopilación de datos de los clientes.

En caso de conflicto positivo de leyes vigentes en estados diferentes, sería aplicable el principio de las garantías para *la cooperación internacional* que permite la aplicación de la ley que ofrece el mayor grado de protección para los derechos fundamentales.

Al mismo tiempo, los estados son obligados a adoptar leyes que ofrezcan g*arantías contra el acceso ilegítimo y que protegen el derecho a recurso efectivo,* es decir penalizar los actos de vigilancia ilegal de las personas por parte de organismos públicos o privados no autorizados por la ley o por un juez imparcial.

Hay una necesidad urgente de una correlación entre las políticas de seguridad cibernética y los derechos humanos. Los debates actuales sobre seguridad cibernética sufren una falta de claridad de definición que permite que todas las iniciativas en esta área sean determinadas por un sentimiento de crisis, no sea tan legítimo. En esta atmósfera, se hacen esfuerzos insuficientes para establecer la naturaleza exacta y la gravedad de cada amenaza e investigar el costo de las soluciones ofrecidas y así realmente contrarrestar el problema que pretenden abordar. Además, se oculta el papel a menudo problemático de los gobiernos y las empresas que contribuyen a la inseguridad.

[26] Ibidem.

Una razón importante por la cual se ha permitido que esto suceda es porque el enfoque adoptado para la seguridad es negativo: la seguridad se define como una ausencia del daño. Por el contrario, proponemos un enfoque positivo de la seguridad que sitúa en el centro a las personas y sus capacidades de actuar libres en el medio electrónico.

Lo que realmente proponemos es enseñar a los utilizadores como defenderse solos en el medio online, devolver a la gente su derecho y su capacidad de protegerse en línea, sin proponer políticas bastante protectoras y con efectos secundarios que destruyen los propios instintos de autoprotección del ser humano.

Centrándose en este enfoque, sería obligación que las medidas de ciberseguridad respeten y apoyen el derecho a la vida privada y el derecho a la libertad de expresión. Aunque otros derechos humanos son relevantes también, estos dos son derechos clave para facilitar la actuación audaz de las personas en el medio electrónico. Al evaluar las cuestiones contenciosas y sus resoluciones propuestas en contra de la medida en que respetan y apoyan estos derechos, se podría lograr avances importantes.

Por último, este enfoque se basa en que los gobiernos y las empresas aceptan ejercer la restricción mutua. Con el fin de institucionalizar el principio de moderación, se requiere un modelo distributivo de la gobernanza de Internet que reconozca y respete el papel de una amplia variedad de actores y, a través de un sistema de controles y equilibrios, garantice que ninguno de estos actores pueda controlar el medio electrónico sin la colaboración y el acuerdo de los demás. Tal enfoque sería más adecuado a las realidades del nuevo entorno que Internet ha provocado. Igualmente haría posible cambiar el énfasis en los enfoques centrados en el estado de la seguridad cibernética por aquellos centrados en las personas.

CAPÍTULO I. El concepto de Seguridad Cibernética

El mundo está de acuerdo con la idea que, el espacio virtual constituye una oportunidad para compartir información o aumentar el desarrollo económico. Este nuevo ámbito de interacción humana cambia profundamente la vida de nuestras sociedades, nuestros negocios e incluso nuestros estilos de vida. Mientras que el comercio, la energía, el transporte y la industria se están transformando al aprovechar las comunicaciones electrónicas, así como las capacidades cada vez más eficientes de recopilación y procesamiento de datos, algunos están trabajando hacia el advenimiento de una "humanidad creciente", conectada en profundidad y permanentemente, un mundo donde el Hombre y la Tecnología se fusionaría.

En España, la primera definición oficial del ciberespacio se mencionó en la Orden Ministerial 10/2013, de 19 de febrero, por la que se creó el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas, en la que aquél es descrito como el "*dominio global y dinámico compuesto por infraestructuras de tecnología de la información – incluyendo Internet –, redes de telecomunicaciones y sistemas de información*". En diciembre de 2013, la definición del orden ministerial se incluyó en la Estrategia de Ciberseguridad Nacional[27], el primer documento oficial que reconoce el papel del desarrollo de las Tecnologías de Información y Comunicación (TIC) en la aparición de un nuevo espacio de relación en el que la rapidez y facilidad de los intercambios de información y comunicaciones, sin barreras de distancia y tiempo.

La verdad es que la tecnología ha abierto un mundo nuevo de posibilidades. Nuevos productos y servicios aparecen a cada paso y momento acostumbrándonos con transformaciones diarias y gadgets inteligentes que pueden leer nuestros pensamientos. Con cada nuevo avance, con cada nueva compra, nuestra dependencia tecnológica crece y las herramientas tecnológicas se transforman en bienes esenciales para nuestro bien estar. Junto con estas transformaciones, crece también la importancia de la ciberseguridad[28]. Usar todas estas aplicaciones informáticas y todos los equipamientos tecnológicos de última generación nos obliga introducir cada día más datos personales en Internet, seguir más tiempo conectados, lo que nos expone y nos transforma en posibles víctimas de alguna forma de ciberdelincuencia o de ciberataque. Cada vez aparecen más

[27] Consejo de Seguridad Nacional (2019) Estrategia de Ciberseguridad Nacional, texto disponible en: http://www.lamoncloa.gob.es/documents/20131332estrategiadecibersegu ridadx.pdf.
[28] Ibidem.

casos de cibercriminalidad que justifican todas estas medidas tomadas por los estados y las autoridades[29]. El número y la tipología de los virus informáticos en circulación se aumenta cada hora, los tipos de códigos dañinos se desarrolla constantemente y un millón de personas se convierten en víctimas de los delitos cibernéticos todos los días[30].

En este contexto, la seguridad cibernética y las medidas que la respaldan se han convertido en un tema de actualidad que ocupa la agenda diaria de los gobiernos que intentan definirla y buscar soluciones prácticas para su desarrollo. Con base en el Artículo 2 del Reglamento sobre Ciberseguridad, la ciberseguridad representa "*todas las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciber amenazas*".

De hecho, hay amenazas genuinas. El acceso ilegal a computadoras personales, el robo de datos y la clonación de credenciales se han vuelto comunes y complejos. Los casos de fraude informático se están volviendo más comunes y se están convirtiendo día a día en delitos complejos que afectan a un gran número de personas[31]. El robo de la cartera que se practicaba antes en los lugares apiñados se ha transformado en robo digital de las credenciales de la cuenta de internet-banking o del correo electrónico.

Las organizaciones internacionales trabajan cada una en su campo de competencia para identificar soluciones prácticas, reglas de conducta o implementar mecanismos de cooperación, que deberían permitir a los Estados combatir el delito cibernético, garantizar una cierta resistencia y evitar los efectos en cascada de una confrontación cibernética que podrían ser destructivos para todas las partes involucradas[32]. Durante varios años ha habido un acuerdo tácito sobre la aplicabilidad del derecho internacional y sus principios al ciberespacio. Lo que queda es armonizar las propuestas y confrontar algunas de ellas con la realidad técnica del ciberespacio. Las prácticas reguladas reconocidas y legales, o el razonamiento válido, aplicado en el mundo material pueden encontrar sus límites en un modo intangible y aún más en el mundo híbrido como el en que entramos[33].

---

[29] Deibert, R; Palfrey, J.; Rohozinski, R. y Zittrain, J. (2010) *Access Controlled. The Shaping of Power, Rights, and Rule in Cyberspace*. Editorial The MIT Press, p.6.

[30] Véase en este sentido: https://cybermap.kaspersky.com/es/stats/. Un sitio web que expone en tiempo real el mapa de las ciber amenazas en el mundo.

[31] Standage, T. (1998) *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-line Producers*, Editorial New York: Berkeley Books.

[32] Comisión Europea (2017) Recomendación de la Comisión de 13.9.2017 sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala, C(2017) 6100 final de 13 de septiembre de 2017, Bruselas, texto disponible en: C(2017)6100/F1 - ES (europa.eu).

[33] Palfrey, J. y Gasser, U. (2008) *Born Digital: Understanding the First Generation of Digital Natives*. Editorial New York: Basic Books.

1.1. La Seguridad cibernética y el Derecho Internacional

El aumento dramático de los ataques cibernéticos que involucran a Estados y actores no estatales constituye una amenaza real para la paz y la seguridad internacionales. En su informe de 2015[34], el Grupo de Expertos Gubernamentales de las Naciones Unidas (en adelante GEG) expresó su inquietud[35] sobre las "*tendencias preocupantes*" marcadas por un aumento dramático del número de actos maliciosos dirigidos contra, entre otras cosas, la infraestructura vital de los Estados. Este hecho alarmante es compartido por todos los actores del ámbito de la seguridad digital y cibernética, independientemente de si son Estados, organizaciones internacionales o actores privados[36].

Estos ataques no solo amenazan las infraestructuras críticas, sino que también son una fuente importante de tensiones entre los Estados. Todos los días, las infraestructuras críticas se vuelven cada vez más dependientes de Internet, y la violación de la seguridad de la red tiene repercusiones significativas en los derechos humanos, especialmente cuando no pueden ejercerse como resultado de la destrucción de las plataformas de servicios sociales por un ataque cibernético. Las autoridades estatales no deberían tratar estos ciberataques con superficialidad, sino deben involucrarse más, porque los estados tienen el deber de proteger a sus ciudadanos tanto en el entorno offline como en el entorno online.

---

[34] Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional (2015) *Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional A/70/174*, texto disponble en https://undocs.org/A/70/174.

[35] El 27 de diciembre de 2013, la Asamblea General de las Naciones Unidas aprobó por unanimidad la resolución 68/243, en la que se tomaba nota "de los resultados del Grupo de Expertos Gubernamentales de 2012/2013 y se solicitaba al Secretario General la creación de un nuevo Grupo que presentaría un informe a la Asamblea General en 2015. El nuevo Grupo de Expertos Gubernamentales, compuesto por 20 expertos, celebró su primera reunión en Nueva York en julio de 2014 y escogió al Brasil para ocupar la Presidencia. El Grupo celebró su segundo período de sesiones en Ginebra en enero de 2015 y otras dos sesiones más en Nueva York. El Grupo se puso de acuerdo en presentar un informe amplio en junio de 2015 (A/70/174) sobre las normas, reglas o principios de la conducta responsable de los Estados en el ciberespacio, así como medidas de fomentar la confianza, la cooperación internacional y la creación de capacidad que podría tener una aplicación más amplia a todos los Estados. También se ocupa con la interpretación las normas del Derecho Internacional en la utilización de tecnologías de información y comunicaciones". Recuperado de: https://www.un.org/es/ga/about/background.shtml.

[36] En febrero de 2017, los participantes en la Conferencia de la OSCE sobre Protección de Infraestructura Crítica enfatizaron aún más "la importancia crucial de proteger este tipo de infraestructura contra los ataques cibernéticos para garantizar la paz y la seguridad internacional". *Cyber Security for Critical Infrastructure: Strengthening Confidence Building in the OSCE, Vienna, 15 February 2017,* Recuperado de: https://www.osce.org/event/cyber-security-for-critical-infrastructure.

Solo en unos años, el universo digital se ha convertido en un espacio de confrontación, no solo entre los Estados, sino también entre los Estados y ciertos actores no estatales, cuyas actividades desestabilizadoras son una preocupación importante para la comunidad internacional en su conjunto. El Secretario General de las Naciones Unidas refiere que: "*entre los problemas complejos que han surgido se encuentra el creciente uso malicioso de las TIC por parte de extremistas, terroristas y grupos delictivos organizados*". El fenómeno es aún más complicado porque algunos Estados tienen vínculos más o menos estrechos con estos grupos no estatales y los utilizan como "intermediarios" o "representantes", para desarrollar actividades maliciosas contra los intereses de otros Estados.

Realmente, en sus orígenes, el ciber espionaje es una acción patrocinada por los estados que representa el origen de otras dos nociones modernas, a saber: la guerra y las armas cibernéticas. Estas nuevas amenazas nacidas en el espacio virtual han sido utilizadas por los estados para obligar a los ciudadanos a renunciar a parte de sus derechos y libertades civiles en el nombre de la seguridad colectiva o personal. Tal como, en los EE. UU., el espionaje cibernético por parte de los chinos es un argumento clave utilizado para apoyar la controvertida Ley de Protección e Intercambio de Inteligencia Cibernética (CISPA)[37], una regulación que permitiría a las autoridades acceder a grandes cantidades de datos de usuarios sin una orden judicial o autorización previa.

> *"Cyber Intelligence Sharing and Protection Act - Amends the National Security Act of 1947 to add provisions concerning cyber threat intelligence and information sharing. Defines «cyber threat intelligence» as intelligence in the possession of an element of the intelligence community directly pertaining to: (1) a vulnerability of a system or network of a government or private entity; (2) a threat to the integrity, confidentiality, or availability of such a system or network or any information stored on, processed on, or transiting such a system or network; (3) efforts to deny access to or degrade, disrupt, or destroy such a system or network; or (4) efforts to gain unauthorized access to such a system or network, including for the purpose of exfiltrating information. Excludes intelligence pertaining to efforts to gain unauthorized access to such a system or*

[37] El proyecto CISPA fue presentado por Mike Rogers en la Cámara de Representantes en noviembre del año 2011. El objetivo del proyecto de ley es "proporcionar el intercambio de cierta información sobre amenazas cibernéticas entre la comunidad de inteligencia y las entidades privadas de seguridad cibernética, y para otros fines".

network that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access"[38].

Además de este fenómeno importante y preocupante para la paz y la seguridad internacional, los actores privados también desempeñan un papel de liderazgo en campo de la seguridad digital. Al respecto, la actividad del sector privado se está desarrollando en prácticamente todas las áreas, desde la prevención de ataques cibernéticos y la seguridad de las infraestructuras digitales hasta las medidas de "active cyber defense" (defensa cibernética activa), incluido el uso de técnicas ofensivas como el "hacking back".

Sin embargo, las actividades del sector privado que actúan en el área de la seguridad cibernética plantean varios problemas y controversias, de naturaleza política, ética, técnica y legal. El propósito de este análisis es contribuir a la reflexión sobre estos temas y analizar un aspecto importante que sin duda estará en el centro de las preocupaciones de la comunidad internacional en los próximos años: los papeles de los actores públicos y privados en los mecanismos de protección de la paz y seguridad del espacio digital, en el marco del derecho internacional.

En el año 2013, los miembros del GEG reconocieron la aplicación del derecho internacional, incluida la Carta de las Naciones Unidas, en el ciberespacio. Este reconocimiento fue un hito importante para el GEG, así como para la paz y la seguridad digital. El ciberespacio ya no es una "tierra sin ley", más bien, puede ser regulado por el derecho internacional, como son prácticamente todas las actividades internacionales. Pero la tarea en este campo es infinitamente más compleja. Específicamente, determinar cómo se aplica el derecho internacional en el espacio digital nos lleva inevitablemente al problema de la identificación e interpretación de las reglas existentes, pero también a la cuestión de su relevancia y sus limitaciones en el ciberespacio.

---

[38] La Ley de Protección e Intercambio de Inteligencia Cibernética enmienda la Ley de seguridad nacional de 1947 para agregar disposiciones relativas a la inteligencia e intercambio de información sobre amenazas cibernéticas. Define la "inteligencia de amenazas cibernéticas" como "inteligencia en posesión de un elemento de la comunidad de inteligencia directamente relacionada con: (1) una vulnerabilidad de un sistema o red de un gobierno o entidad privada; (2) una amenaza a la integridad, confidencialidad o disponibilidad de dicho sistema o red o cualquier información almacenada, procesada o en tránsito por dicho sistema o red; (3) esfuerzos para negar el acceso o degradar, interrumpir o destruir dicho sistema o red; o (4) esfuerzos para obtener acceso no autorizado a dicho sistema o red, incluso con el propósito de exfiltrar información. Excluye la inteligencia relacionada con los esfuerzos para obtener acceso no autorizado a dicho sistema o red que solo involucran violaciones de los términos de servicio del consumidor o los acuerdos de licencia del consumidor y no constituyen de otra manera acceso no autorizado" - Summary: H.R.3523 — 112th Congress (2011-2012) – disponible en: https://www.congress.gov/bill/112th-congress/house-bill/3523.

Está claro que existen muy pocos instrumentos legales en el derecho internacional específicamente dedicados a la seguridad cibernética. No solo las convenciones internacionales en este campo son escasas, sino que su impacto también es limitado, ya sea debido al pequeño número de participantes o la naturaleza restringida de su tema[39].

El Convenio de Budapest sobre Ciberdelincuencia es, posiblemente, la más efectiva para por el momento[40]. En este contexto, se deben aplicar las reglas convencionales y consuetudinarias, a pesar de que no se han diseñado específicamente para regular el ciberespacio. Tal práctica de aplicar reglas a áreas fuera de su ámbito de aplicación original no es inusual en el derecho internacional. Sin embargo, se requiere cierta precaución. El número limitado de normas internacionales vinculantes diseñadas específicamente para la regulación del ciberespacio parece ser una prueba de la renuencia de muchos Estados a actuar decisivamente para el desarrollo de nuevas normas convencionales sobre seguridad cibernética. En cuanto a las soluciones de seguridad cibernética elegidas y las normas de protección relacionadas, también debemos asegurarnos de que estén en línea con las disposiciones internacionales de derechos humanos y no creen una limitación desproporcionada en ellas.

Esta situación ha dejado el camino abierto para varias iniciativas privadas basadas sobre el rechazo de cualquier regulación ("¡deje a Internet libre!"), o incluso la promoción de una autorregulación del ciberespacio por parte de los propios actores privados. Algunos actores importantes en la industria digital también se han embarcado en un nuevo camino, dedicándose a proponer normas para regular no solo su propio comportamiento en una lógica similar a la autorregulación, sino también para el comportamiento de los Estados.

La iniciativa más notable al respecto es la de Microsoft, que en 2015 propuso a los Estados una serie de normas de seguridad cibernética[41], seguida de la publicación en

---

[39] Por ejemplo, El Convenio de la Unión Africana sobre seguridad cibernética y protección de datos personales de 2014 no ha sido ratificada por ningún estado todavía.

[40] El Convenio de Budapest sobre ciberdelincuencia, ratificado por 52 paises, es el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en Internet mediante la armonización de leyes entre naciones, el aumento de la cooperación entre las naciones firmantes y la mejora de las técnicas de investigación. Ha sido elaborado por el Consejo de Europa en Estrasburgo, con la participación de Canadá, Japón y China como estados observadores.. Recuperado de: 9https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26882/1/Convenio_de_Budapest_y_Ciberdelincuencia_en_Chile.pdf.

[41] Microsoft Org. (2016) *From Articulation to Implementation: Enabling Progress on Cybersecurity Norms* (De la elaboración hasta la implementación: permitir el progreso en las normas de ciberseguridad), disponible en:

2016 de un documento sobre su implementación y, en febrero de 2017, de una convocatoria para la adopción de una nueva Convención de Ginebra para proteger a los civiles de los ataques en Internet[42]. Numerosas iniciativas académicas también han abordado la cuestión de la identificación e interpretación del derecho internacional en el ciberespacio, entre cuales el logro más conocido es la publicación del Manual de Tallin[43].

> "*El manual de 282 páginas no es un cuerpo normativo oficial de la OTAN, pero es una guía importante para situaciones que se puedan plantear en el ciberespacio, toma normas vigentes de carácter internacional sobre conflictos armados como la Declaración de San Petersburgo de 1868 o las Convenciones de Ginebra de 1949, y las aplica adaptándolas al ciberespacio. El Manual es el resultado de un trabajo de tres años de análisis de las normas internacionales que pueden aplicarse para combatir los ataques de la guerra cibernética elaborado por un grupo de expertos independientes que emiten opiniones bajo su absoluta responsabilidad, pero crea el primer cuerpo de ideas sobre a la materia*"[44].

Este papel importante de los actores privados en el ciberespacio constituye un cambio radical del panorama del derecho internacional y las relaciones entre los actores públicos y privados. Tradicionalmente, el derecho internacional debe intervenir para proteger ciertas categorías específicas de actores no estatales, ya sea contra las acciones de Estados extranjeros (protección de extranjeros, protección de inversiones, etc.) o contra las acciones de Estados bajo la jurisdicción de los cuales se encuentran los actores privados (por ejemplo, en el campo de los derechos humanos, la protección de las minorías o los pueblos indígenas).

También puede intervenir para imponer obligaciones directamente tanto a los actores no estatales como a los Estados, por ejemplo, en la lucha contra la piratería o en

---

https://mscorpmedia.azureedge.net/mscorpmedia/2016/06/Microsoft-CybersecurityNorms_vFinal.pdf.

[42] Smith, B. (2017) *The need for a Digital Geneva Convention*, RSA Conference, San Francisco, 14 February 2017, recuperado de:. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention.

[43] Los expertos en informática y ciberseguridad han elaborado una especie de corpus normativo - el *"Tallinn Manual on the International Law Applicable to Cyber Warfare*", denominado comúnmente *"Manual de Tallin"*, que lleva el nombre de la capital de Estonia, publicado en abril de 2013, donde se compiló y perpetró el primer ataque cibernético de un país a otro. La iniciativa de crear un tal manual pertenece al Centro de Defensa Cibernética de la OTAN Cooperativa de Excelencia. Disponible en: http://nuclearenergy.ir/wp-content/ uploads/2013/11/tallinn_manual.pdf

[44] Fonseca, C.E., Perdomo, I.L., Arozarena Gratacos, L.M., Ulises Ortiz, J. (2014) *El Manual de Tallin y la Aplicabilidad del Derecho Internacional a la Ciberguerra*, Revista de la ESG no.588-143, disponible en: http://www.cefadigital.edu.ar/bitstream/1847939/993/1/Revista%20ESG%20no.588-2014_Fonseca_172.pdf

la prevención y represión de ciertos crímenes internacionales como el genocidio, crímenes contra la humanidad, crímenes de guerra, crimen organizado y terrorismo.

Desde el 11 de septiembre de 2001, la lucha contra el terrorismo ha puesto en primer plano la cuestión del papel de los actores no estatales en el derecho internacional y los derechos y obligaciones de los Estados en relación con ellos[45].

Cualesquiera que sean los desafíos planteados por estas preguntas al derecho internacional, en general, las relaciones entre los Estados y los actores no estatales han quedado afectadas por un claro desequilibrio a favor de los Estados, vinculado no solo a la diferencia en el estatus legal entre los primeros (titulares de soberanía y poderes importantes) y los últimos ("sujetos" a los Estados), pero también debido a la diversidad de facto de poder, recursos y capacidades de cada uno. De hecho, el Estado casi siempre ha sido percibido como el propietario de un poder incomparable, lo que le confiere una situación superior a las de los actores privados (individuos, minorías, inversores, etc.), que dependen tanto de su protección como también de sus poderes de regulación, jurisdicción o aplicación de la ley[46].

Este modelo tradicional se ve profundamente afectado por el paradigma de la seguridad cibernética. Y esta interrupción tiene lugar mientras el ciberespacio constituye un desafío importante en términos de seguridad nacional, como lo destacan muchos Estados que han publicado en los últimos años sus "estrategias de seguridad cibernética nacional". Sin embargo, las estrategias de ciberseguridad deben diseñarse e implementarse de acuerdo con el derecho internacional y con los derechos humanos, de modo que estén protegidos y no limitados[47]. Las principales compañías tecnológicas parecen ser tan poderosas en prevenir ataques cibernéticos, atribuirlos y responder a actos maliciosos, como los Estados y a veces aún más.

Michael N. Schmitt y Sean Watts expresan que:

> *"Clásicamente, los actores estatales y no estatales se diferenciaron no solo por las disparidades en el estado legal, sino también por desequilibrios significativos en los recursos y capacidades. No es sorprendente que el derecho internacional desarrolle un sesgo centrado en el estado para dar cuenta de estos desequilibrios. Sin embargo, el ciberespacio y las operaciones cibernéticas han*

[45] Moore, A. D. (2011) *Privacy, security, and government surveillance: Wikileaks and the new accountability*. Public Affairs Quarterly Volume 25. no 2/2011. pp.162-188.
[46] Taylor, J. S. (2005) *In Praise of Big Brother*. Public Affairs Quarterly. vol. 19, no. 3/2005, pp. 227–246
[47] Deudney, D. H. (2007) *Bounding Power: Republican Security Theory from the Polis to the Global Village*, Editorial Princeton University Press, p. 244.

cerrado una serie de brechas anteriormente significativas entre las capacidades de los actores estatales y no estatales para comprometer la paz y la seguridad internacionales. De hecho, algunos actores no estatales ahora igualan, si no superan, las capacidades cibernéticas de muchos estados a este respecto"[48].

Teniendo en cuenta el análisis del artículo realizado por el profesor Scott J. Shackelford *"¿Debería la ciberseguridad ser un derecho humano? Explorando la responsabilidad compartida de la paz cibernética*"[49], sobre las estrategias de seguridad cibernética de 34 países, la importancia de los derechos fundamentales ocupa un plazo secundario entre los objetivos de estos documentos. Solo el 60% de las estrategias estudiadas el derecho a la vida privada goza de garantías, al mismo tiempo que el derecho a la libre expresión esta mencionado solo el 10% de estos programas.

Las capacidades técnicas de los gigantes digitales y su fortaleza económica no son accesibles para muchos de los Estados, especialmente para los menos tecnológicamente avanzados. La arquitectura misma de Internet parece reforzar esta situación, al constituir un desafío para el modo tradicional de una gobernanza "centralizada" de los Estados, aparentemente favoreciendo el papel de los actores privados que están activos en el ciberespacio[50]. Por estas razones, las empresas privadas están cada vez más involucradas en la seguridad cibernética, ya sea de forma autónoma o en conjunto con los Estados, en relaciones "públicas-privadas" multifacéticas que van mucho más allá de los patrones tradicionales[51]. La estructura de estas relaciones y las complejas asociaciones entre los Estados y los actores privados en los campos de la ciberdefensa y el ciberataque, así como sus consecuencias legales y políticas, aún no se han identificado y teorizado.

Se argumenta que el papel clave de los actores privados en estas áreas durará, en primer lugar porque estos actores se ven directamente afectados por la ciberdelincuencia y los ciberataques y, en consecuencia, consideran que deben protegerse a sí mismos; y en segundo lugar, debido a que en Internet los datos, la inteligencia artificial, el Internet de

---

[48] Schmitt, M.N. y Watts S. (2016) *Beyond State-Centrism: International Law and Non-state Actors in Cyberspace*, Journal of Conflict & Security Law, Vol. 21, No. 3, p. 1.

[49] Shackelford, S. J. (2017) *Should Cybersecurity Be a Human Right? Exploring the "Shared Responsibility" of Cyber Peace*. Stanford Journal of International Law No. 2019, Kelley School of Business Research Paper No. 17-55, Recuperado de: https://ssrn.com/abstract=3005062.

[50] David Lyons, D. (2001) *Surveillance Society: Monitoring Everyday Life*, Editorial Buckingham, UK: Open University Press.

[51] Choi, J., Kaplan, J., Krishnamurthy, C. y Lung, H. (2017) *Hit or myth? Understanding the true costs and impact of cybersecurity programs*, McKinsey Digital, recuperado de: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/hit-or-myth-understanding-the-true-costs-and-impact-of-cybersecurity-programs.

las cosas (IoT), la nube (cloud) y otras maravillas digitales que aparecen día tras día, tienen un enorme potencial de crecimiento que las empresas están decididas a defender y explotar[52].

El mercado de seguridad cibernética en sí mismo está en auge a medida que las amenazas a la seguridad digital continúan creciendo con el tiempo. En este contexto, existe una necesidad urgente de reflexionar en profundidad sobre los papeles de los Estados y de los actores privados con respecto a la paz y la seguridad en el ciberespacio[53]. Esta reflexión debe tener en cuenta la extrema complejidad del problema, marcada por la gran diversidad de los actores involucrados[54]: posibles perpetradores de ciberataques (Estados, actores privados apoyados o tolerados por Estados, terroristas, ciberdelincuentes, compañías que conducen espionaje o querer obtener una ventaja competitiva, hackers individuales, grupos de hackers patrióticos, etc.); posibles víctimas de ataques (Estados, administraciones y comunidades, empresas, medios de comunicación, particulares, etc.); aquellos involucrados en estos ataques (por ejemplo, los Estados a través de los cuales transitan los ataques cibernéticos, las empresas y las personas cuyos sistemas son utilizados por los atacantes sin el conocimiento de los propietarios); y, finalmente, aquellos que podrían estar involucrados en una respuesta a un ciberataque (Estados, empresas privadas que actúan en beneficio propio, empresas privadas que responden en nombre de otra empresa, etc.). Esta situación crea una cantidad impresionante de combinaciones, que cada una, a su manera, afectan el tipo y la idoneidad de una respuesta[55].

También, se debe tener en cuenta el carácter internacional o transnacional frecuente de los ciberataques, lo que hace que esta problemática sea casi naturalmente una problemática relacionada con el derecho internacional. El objetivo de nuestro estudio es, precisamente, presentar las principales respuestas que el derecho internacional aporta hoy a estas preguntas. Voluntariamente adoptaremos aquí una definición amplia del término "ataque cibernético" para examinar los roles de los estados y los actores privados en la prevención y respuesta a los ataques cibernéticos. Las estrategias de ciberseguridad

[52] Maurer, T. (2011) *Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security?*, Discussion Paper 2011-11, Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School. p. 11.
[53] Ibidem.
[54] Joyner, C. C. y Lotrionte, C. (2001) *Information Warfare as International Coercion: Elements of a Legal Framework*, EJIL, vol 12, no. 5, pp. 825-865.
[55] Lefebvre, N. (2015), *Les services de renseignement européens face au terrorisme : coopération ou cloisonnement*, Presses Académiques Francophones, Saarbrücken.

deben diseñarse e implementarse de acuerdo con el derecho internacional y con los derechos humanos, de modo que estén protegidos y no limitados[56]. Por ende, es importante que toda la comunidad se involucre más activamente en la defensa de los derechos humanos en un sentido amplio, para analizar cuidadosamente cada caso de delito cibernético y descubrir qué se esconde detrás de él.

Al nivel europeo notamos una preocupación de las instituciones comunitarias en los esfuerzos de desarrollar medidas que se ajusten a los amplios objetivos de la estrategia de ciberseguridad de la UE[57]. Los responsables están conscientes que el marco legislativo sigue incompleto y la falta de una política común de los estados en materia de seguridad cibernética impide el pleno desarrollo tecnológico. El sueño de convertir el ciberespacio europeo en el entorno digital más seguro del mundo plantea un desafío que vamos a tratar en el tercer capítulo de esta tesis.

Por ende, como señala el Tribunal de Cuentas Europeo, un desafío clave es "*garantizar una rendición de cuentas y una evaluación significativas mediante la transición hacia una cultura del rendimiento con prácticas de evaluación integradas*"[58].

1.2. El marco regulatorio internacional relativo a los ciberataques

Incluso en períodos de conflicto armado debe garantizarse la protección de los derechos humanos básicos de la población civil y de los combatientes, y esto es tema del derecho internacional humanitario. La historia del derecho internacional humanitario está estrechamente asociada al de la Cruz Roja. La Cruz Roja surgió del trabajo de Henri Dunant, un humanitario suizo, que organizó los servicios de ayuda de emergencia en la batalla de Solferino en 1859.

La Convención de Ginebra de 1864, el primer acuerdo multilateral sobre derecho humanitario comprometió a los gobiernos a cuidar de los heridos de guerra, enemigos o amigos. Este Convenio fue ampliado por los Convenios de La Haya de 1899 y 1907 y los Convenios de Ginebra de 1906 y 1929.

---

[56] Neelie, K. (2013) *Using cybersecurity to promote European values*, recuperado de: http://europa.eu/rapid/pressrelease_SPEECH-13-104_en.htm.

[57] European Commission (2016), Communication from the Commission to the European Parliament, the European Council and the Council, "*Enhancing Security in a world of mobility; improved information exchange in the fight against terrorism and stronger external border*", COM(2016)602, Brussels, 14 September 2016.

[58] Tribunal de Cuentas Europeo (2019) *Desafíos de una política eficaz de ciberseguridad en la UE*. Recuperado de: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_ES.pdf.

Después de la Segunda Guerra Mundial, durante la cual se produjeron enormes abusos de sobre los derechos humanos, el derecho internacional conoció una transformación amplia y los estados acordaron en codificar y publicar disposiciones claras e imperativas relativas a la protección legal para combatientes y civiles. Las reglas que rigen la conducción de las operaciones militares, conocidas como la "Ley de La Haya", y las leyes que protegen a las víctimas de la guerra (los cuatro Convenios de Ginebra de 1949) son resultado de las negociaciones y los acuerdos estatales de aquella época. Casi todos los países del mundo se adhirieron a estos convenios.

Hoy en día, la distinción entre "derecho de Ginebra" y "derecho de La Haya" casi no existe porque los dos Protocolos adicionales de 1977 a los Convenios de Ginebra introducen reglamentaciones similares, de ambos tipos. El Protocolo adicional I[59] hace referencia a la protección de civiles y bienes de carácter civil durante los conflictos armados internacionales y el Protocolo adicional II[60] hace referencia a la protección de civiles y bienes de carácter civil en conflictos armados nacionales.

Uno de los principios fundamentales del derecho internacional humanitario es el principio de proporcionalidad. Pongamos por caso, no se pueden utilizar armas que causen un sufrimiento excesivo e innecesario, o que no puedan estar seguros de alcanzar un objetivo militar. Los Convenios de Ginebra prohíben sin discriminación los homicidios ilegítimos, las torturas, los juicios injustos y los trabajos forzados durante conflictos internacionales y nacionales. Los Convenios también exigen respeto y protección de los miembros de las fuerzas armadas heridos, enfermos y náufragos, así como de los prisioneros de guerra, en tiempos de conflicto armado internacional[61]. El Cuarto Convenio se refiere a la protección de los civiles en tiempo de guerra. Los Protocolos adicionales amplían la protección a todas las personas afectadas por conflictos armados y prohíben los ataques de los combatientes a poblaciones civiles y bienes de carácter civil.

La Conferencia Mundial de Derechos Humanos (1993) convenció a los Estados que aún no lo habían hecho a que se adhirieran a los Convenios de Ginebra del 12 de

[59] El Protocolo adicional I a los Convenios de Ginebra entró en vigor el 7 de diciembre de 1978 y, cuenta con 174 Estados parte. Disponible en: https://www.icrc.org/es/document/protocolo-i-adicional-convenios-ginebra-1949-proteccion-victimas-conflictos-armados-internacionales-1977.

[60] El Protocolo Adicional II a los Convenios de Ginebra entró en vigor el 7 de diciembre de 1978 y esta ratificado por 169 estados. El texto es disponible en: https://www.icrc.org/es/doc/resources/documents/misc/protocolo-ii.htm

[61] Llanos Mansilla, H. (1976) El derecho humanitario y su aplicación en caso de conflictos armados de carácter interno. *Revista Chilena de Derecho* vol. III. pp. 37-48.

agosto de 1949 y a sus Protocolos y a que adoptaran todas las medidas nacionales apropiadas, incluidas las legislativas, para su plena aplicación.

Como intermediario neutral en conflictos armados, el Comité Internacional de la Cruz Roja[62] intenta, ya sea por iniciativa propia o basando su acción en los Convenios de Ginebra y sus Protocolos adicionales, brindar, al nivel internacional, protección y asistencia a las víctimas de las acciones violentas[63].

En el entorno digital las guerras se llevan de otra forma, las heridas y los daños que pueden provocar los ataques cibernéticos pueden tener un alcance mayor que una explosión de una bomba clásica. Un *black out* causado por un ataque cibernético sobre la única fuente de electricidad de una ciudad puede causar la muerte de cientos de personas (personas en terapia intensivas, en transporte común subterráneo, en ascensores etc.). No queremos imaginar un ataque cibernético sobre una central nuclear.

En este nuevo contexto la guerra clásica se ha convertido en guerra cibernética y los choques entre los soldados se han convertido en ataques cibernéticos a base virus informático, troyanos u otro tipo de programa malware. Como en la guerra clásica, hay también víctimas entre los civiles que no tienen nada en común con los ataques cibernéticos, pero soportan las consecuencias. Desde este punto de vista, es necesario elaborar un marco regulatorio internacional relativo a las guerras cibernéticas y la protección de los derechos humanos en este tipo de confrontaciones.

El derecho internacional no ofrece una definición aceptada por unanimidad del término "ataque cibernético", mientras que las estrategias nacionales de seguridad cibernética adoptadas por varios Estados, proponen definiciones muy diferentes de este término. Pese a esta diversidad, se puede observar que las definiciones existentes parecen converger hacia un enfoque amplio del término "ataque cibernético". Es el caso de la estrategia de ciberseguridad de Canadá:

> *"Los ciberataques incluyen el acceso, uso, manipulación, interrupción o destrucción no intencionados o no autorizados (a través de medios electrónicos) de información electrónica y/o la infraestructura electrónica y física utilizada*

[62] Fundado en 1863, el Comité Internacional de la Cruz Roja y la Federación de Sociedades de la Cruz Roja y de la Media Luna Roja forman, con las Sociedades Nacionales de la Cruz Roja y de la Media Luna Roja, el Movimiento Internacional de la Cruz Roja y de la Media Luna Roja. El CICR recibió el Premio Nobel de la Paz en 1917, 1944 y 1963. Recuperado de: https://www.icrc.org/es/quienes-somos/historia.

[63] Comité Internacional de la Cruz Roja (1975) *Manual de la Cruz Roja Internacional: convenios, estatutos y reglamentos, resoluciones de la Conferencia Internacional de la Cruz Roja y del Consejo de Gobernadores de la Liga de Sociedades de la Cruz Roja*.11ª edición. Ginebra, disponible en: https://www.icrc.org/es/guerra-y-derecho/plataforma-derecho-politicas-humanitarias.

para procesar, comunicar y/o almacenar esa información. La gravedad del ciberataque determina el nivel apropiado de respuesta y/o medidas de mitigación: es decir, seguridad cibernética"[64].

Para el Comité Internacional de la Cruz Roja (CICR):

"Las operaciones cibernéticas pueden describirse en términos generales como operaciones contra una computadora o un sistema informático a través de un flujo de datos. Dichas operaciones pueden tener como objetivo hacer cosas diferentes, por ejemplo, infiltrarse en un sistema y recopilar, exportar, destruir, cambiar o cifrar datos o desencadenar, alterar o manipular procesos controlados por el sistema informático infiltrado. Por estos medios, una variedad de objetivos en el mundo real puede ser destruidos, alterados o interrumpidos, como las industrias, las infraestructuras, las telecomunicaciones o los sistemas financieros"[65].

Con base en el diccionario Technopedia:

"Un ciberataque es la explotación deliberada de sistemas informáticos, empresas y redes que dependen de la tecnología. Los ciberataques utilizan código malicioso para alterar el código, la lógica o los datos de la computadora, lo que resulta en consecuencias perjudiciales que pueden comprometer los datos y conducir a delitos cibernéticos, como el robo de información y de identidad"[66].

Por consiguiente, para los fines de nuestro análisis, el término podría definirse de manera suficientemente amplia como para incluir una gran variedad de técnicas y propósitos.

Como hace notar el Parlamento de Reino Unido:

"El término ciberataque puede referirse a cualquier cosa, desde estafas de correo electrónico a pequeña escala hasta sofisticados ataques a gran escala con diversos motivos políticos y económicos. Los ataques a gran escala pueden tener una serie de objetivos interrelacionados, tales como: obtener acceso no autorizado a información confidencial; causando interrupciones en la

[64] Gobierno de Canada (2010) *Canada's Cyber Security Strategy: For a stronger and more prosperous Canada*. Texto disponible en: http://publications.gc.ca/site/eng/9.693830/publication.html.
[65] Comité Internacional de la Cruz Roja (2011) *Derecho internacional Humanitario y los desafíos de los conflictos armados actuales*, Geneva, octubre 2011, p. 36, disponible en: www.icrc.org/eng/.
[66] Disponible en: https://www.techopedia.com/definition/24748/cyberattack.

infraestructura IT; o causar interrupción física (por ejemplo, a sistemas industriales)"[67].

A la luz del derecho internacional positivo, el desafío es identificar las posibles reacciones que puedan adoptar los Estados frente a la amplia gama de "ataques cibernéticos" dirigidos tanto contra sus instituciones, como en contra de sus ciudadanos, personas jurídicas y físicas.

El derecho internacional acepta tanto el concepto de daño "inmediato" (o directo - resultante de la violación de un derecho legalmente protegido del propio Estado como actor de derecho internacional) como el concepto de daño "indirecto", donde el daño para los intereses de los particulares se considerará un daño indirectamente sufrido por su propio Estado nacional[68]. Por consiguiente, bajo el llamado mecanismo de "protección diplomática", un Estado tiene derecho a presentar una demanda internacional contra otro Estado donde uno de sus nacionales ha sufrido daños como resultado de un acto ilegal de otro Estado. Luego se dice que el Estado "toma el caso" para sus personas físicas o jurídicas al afirmar su propio derecho a garantizar, en la persona de sus sujetos, el respeto de las normas del derecho internacional.

Parece bastante obvio que la reacción de los Estados dependería de la gravedad del daño causado por los ciberataques; un ataque más grave lógicamente permitiría una reacción más severa. Sin embargo, la gravedad del daño no puede ser ni el único ni el criterio decisivo para identificar y clasificar las respuestas relevantes que podrían ser aceptadas por el derecho internacional. Por lo tanto, uno puede imaginar situaciones en las que, a pesar de la gravedad del daño causado por un ciberataque, no hubiera sido posible que un Estado respondiera de manera vigorosa, como, por ejemplo, mediante la adopción de contramedidas[69]. Tal podría ser el caso donde un ciberataque haya sido lanzado únicamente por un actor privado, y el acto no puede ser atribuido directamente a un Estado, o el Estado desde donde operaba el actor privado no puede ser condenado por no haber cumplido con su obligación de diligencia debida[70].

Por otra parte, los Estados podrían responder a un ciberataque mediante la adopción de contramedidas, incluso si el ataque puede haber causado un daño limitado o

---

[67] House of Parliaments (2011) *Post Note 389 - Cyber Security in the UK*, disponible en: https://www.parliament.uk/documents/post/postpn389_cyber-security-in-the-UK.pdf,
[68] Levin, L. (2009) *Human Rights. Questions and Answers*. Editorial: UNESCO Publishing, p. 90.
[69] Finnemore, M.y Sikkink, K (1998) *International Norm Dynamics and Political Change*. The Review of International Organization 52.4, pp. 894-905.
[70] Deibert R. (2012) idem.

incluso ninguno, ya que, como veremos, el daño no es una condición para el ejercicio de contramedidas (sin embargo, puede influir en la evaluación con respecto a la proporcionalidad de la reacción)[71].

Desde el punto de vista del derecho internacional, es preferible adoptar otro criterio para clasificar las reacciones que son permisibles en el caso de un ciberataque: el del hecho internacionalmente ilícito.

La expresión "acto internacionalmente ilícito" significa una acción u omisión atribuible a un Estado, que debe constituir una violación del derecho internacional[72].

A continuación, veremos que ciertas reacciones a los ciberataques siempre están permitidas, incluso en los casos en que es imposible demostrar que un Estado ha cometido una violación del derecho internacional. Por otro parte, otras reacciones son admisibles solo si se puede establecer que un Estado ha cometido un acto internacionalmente ilícito, por una acción u omisión.

1.2.a. Posibles reacciones en ausencia de una violación demostrada del derecho internacional

Las medidas que se presentarán a continuación están disponibles para los Estados (a veces bajo ciertas condiciones) siempre que estos consideran oportuno reaccionar ante un ciberataque sobre las personas físicas o/y jurídicas dentro de su territorio o sobre el mismo estado. Dicho de otra manera, para recurrir a estas reacciones:

• no es relevante si el ciberataque fue iniciado por un Estado, un actor no estatal que actuó en conexión con un Estado o un actor no estatal que actuó sin ninguna relación con un Estado;

• no importa si el ciberataque se puede atribuir o no a un Estado;

• es irrelevante si este ciberataque puede considerarse o no una violación del derecho internacional.

En otras palabras, las reacciones que se describen a continuación se admiten si existe o no un *acto internacionalmente ilícito* de un Estado, pero estamos en presencia de

[71] Garcia T. (2017) *Les entreprises militaires et de sécurité privées appréhendées par le droit*. Editorial: Mare & Martin.

[72] Roberto Ago (Relator Especial). 1978. *El hecho internacionalmente ilícito del Estado como fuente de responsabilidad internacional*, A/CN.4/307 Y ADD. 1 y 2. Séptimo informe sobre la responsabilidad de los Estados, Anuario de la Comisión de Derecho Internacional, vol. II (primera parte), recuperado de: https://legal.un.org/ilc/documentation/spanish/a_cn4_307.pdf

un ciberataque que produjo sus efectos sobre la población o el territorio de un otro Estado que decide reaccionar[73]. Existen tres tipos de reacciones que son las siguientes:

1.2.a.1. Reacciones basadas en la activación de los mecanismos de cooperación internacional y solución de controversias.

El desarrollo de la cooperación internacional se encuentra en el centro de los mecanismos con respecto a las reacciones de los Estados a los ataques cibernéticos, como se refleja en el informe de 2015 del GEG, que dedica mucho sobre este tema en la Parte V, titulada Cooperación y asistencia internacional en el campo de la seguridad informática y la creación de capacidad[74]. Dicha cooperación puede llevarse a cabo entre los Estados implicados, pero también con la asistencia de las organizaciones internacionales competentes.

• Apertura de canales de cooperación y dialogo diplomático entre los Estados implicados

Independientemente si el ciberataque del cual un Estado es víctima constituye un *acto internacionalmente ilícito*, la primera reacción para el Estado víctima es, sin duda, dirigirse al Estado (o Estados) de donde se lanzó el ataque o que fue transitado por el ataque antes de producirse, para solicitar su intervención y cooperación.

De hecho, los actores no estatales (organizaciones o personas privadas) podrían lanzar operaciones cibernéticas maliciosas transnacionales desde el territorio de ciertos Estados sin su conocimiento. Por consiguiente, es natural que el Estado víctima informe a los Estados implicados y solicite que actúen lo antes posible para poner fin a estas operaciones cibernéticas[75]. Los Estados tienen como corolario de su soberanía el deber de no permitir que su territorio sea utilizado de manera tal que socave el derecho al respeto de la integridad territorial de otro Estado: "*sic utere tuo ut alienum no laedas*". El GEG también ha subrayado que "*los Estados también deben responder a las solicitudes*

[73] Clarke, R. A. y Knake, R. (2010) *Cyber War: The Next Threat to National Security and What to Do about It*. Editorial Harper Collins, p. 115

[74] Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional (2015) *Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional A/70/174*, texto disponble en https://undocs.org/A/70/174.

[75] Anuario de la Comisión de Derecho Internacional (2001) *Informe de la Comisión de Derecho Internacional sobre la labor realizada en su 53.º período de sesiones (23 de abril a 1.º de junio y 2 de julio a 10 de agosto de 2001)*, Volumen II (segunda parte): informe de la Comisión a la Asamblea General, A/CN.4/SER.A/2001/Add.1 (Part 2), recuperado de:
https://legal.un.org/ilc/publications/yearbooks/spanish/ilc_2001_v2_p2.pdf

apropiadas para mitigar la actividad maliciosa de las TIC dirigida a la infraestructura crítica de otro Estado que emana de su territorio"[76].

Una notificación al Estado de donde los actores no estatales han lanzado ciberataques, seguida de la continuación de ataques ilícitos, podría considerarse una violación de la diligencia debida, permitiendo que el Estado víctima adopte contramedidas. Por ello, recurrir a los mecanismos diplomáticos tradicionales de cooperación no es solo el camino más seguro y probablemente el más efectivo a seguir, sino que también es necesario para demonstrar que el Estado es consciente de la existencia de los ataques lanzados desde su territorio por los actores privados y que no interviene para evitarlos[77].

La cooperación interestatal para poner fin a un ciberataque puede tomar varias formas, por supuesto. Si el Estado, desde el cual se iniciaron los ciberataques, no tiene los medios técnicos para actuar, el Estado víctima o incluso terceros Estados podrían ofrecer su asistencia técnica.

Esto se enfatiza particularmente en el informe GEG, según el cual "*los Estados deberían responder a las solicitudes de asistencia de otro Estado cuya infraestructura crítica esté sujeta a ataques cibernéticos teniendo en cuenta la debida consideración a la soberanía"*[78].

Al mismo tiempo se pueden desarrollar operaciones de tipo *hack-back* para neutralizar a los actores no estatales, con el consentimiento y bajo el control tanto del Estado víctima como del Estado de origen del ataque. Evidentemente, la búsqueda de una cooperación interestatal efectiva no impide que el Estado víctima de un ciberataque tome unilateralmente las medidas técnicas necesarias para neutralizar los efectos de ese ataque, pero cumpliendo con sus obligaciones previstas por las normas de derecho internacional.

El diálogo constructivo y la cooperación entre los Estados deberían ser, en consecuencia, las primeras reacciones a los ciberataques lanzados por actores no estatales. Si dicha cooperación no produce los resultados deseados, los Estados también pueden adoptar los métodos tradicionales de solución pacífica de controversias[79], tales como:

---

[76] Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional (2015) idem.

[77] Adler, E (2004) *Communitarian International Relations: The Epistemic Foundations of International Relations*. Editorial Routledge, p.83

[78] Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional (2015) idem.

[79] Véase, por ejemplo, el artículo 2, punto 3 de la Carta de las Naciones Unidas ("*Los Miembros de la Organización arreglarán sus controversias internacionales por medios pacíficos de tal manera que no se*

negociación, mediación, investigación o recurrir a mecanismos para la conciliación o resolución de conflictos.

• Recurrir a la asistencia de las organizaciones internacionales competentes

Como expresa el informe GEG de 2015, la asistencia mutua entre los Estados para gestionar un ataque cibernético podría ser apoyada "*por las organizaciones internacionales competentes, incluidas las Naciones Unidas y sus agencias*"[80].

La mejor manera de actuar es que un Estado, que es víctima de un ciberataque, apele al Consejo de Seguridad de la ONU si la situación es lo suficientemente grave como para ser considerada una amenaza para la paz y la seguridad internacional. Dependiendo de la situación, el Consejo de Seguridad podría actuar en el marco del Capítulo VI de la Carta de las Naciones Unidas (arreglo pacífico de controversias) o el Capítulo VII (acción en caso de amenazas a la paz, quebrantamientos de la paz o actos de agresión). En el primer caso, el Consejo podría, por ejemplo, basándose en del artículo 34 de la Carta, "*investigar toda controversia, o toda situación susceptible de conducir a fricción internacional o dar origen a una controversia, a fin de determinar si la prolongación de tal controversia o situación puede poner en peligro el mantenimiento de la paz y la seguridad internacionales"*.

También podría, con base en del artículo 37, "*recomendar los términos de arreglo que considere apropiados*". En el segundo caso, si el Consejo considera que la situación es bastante grave como para constituir una "amenaza a la paz" en el sentido del artículo 39, puede recurrir a las medidas provisionales mencionadas en el artículo 40 de la Carta, o a medidas de coerción non-militares (artículo 41) o incluso militares (artículo 42). Sin embargo, hasta ahora, el Consejo de Seguridad de la ONU nunca tuvo que adoptar tales medidas en el caso de un ciberataque.

Otra opción, quizás más asequible para los Estados interesados, sería abordar los mecanismos de cooperación regional. Un ejemplo es la Agencia de la Unión Europea para la Seguridad de las Redes y la Información (ENISA)[81], que es la institución europea responsable de garantizar un alto nivel de seguridad de las redes y la información en colaboración con las autoridades nacionales y otras instituciones europeas, y que está

pongan en peligro ni la paz y la seguridad internacionales ni la justicia.") y el Capítulo VI de la Carta titulado "*Arreglo pacífico de controversias*", disponible en: https://www.un.org/es/charter-united-nations/.

[80] Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional (2015) idem.

[81] Véase el sitio web de ENISA (www.enisa.europa.eu/).

trabajando para desarrollar una cultura de seguridad de la red de información en toda la Unión. En el capítulo III se presenta detalladamente el papel y las funciones de ENISA en el ámbito de ciberseguridad europea.

Otro ejemplo es el Equipo de Respuesta de Emergencia de Asia Pacífico (APCERT) que, entre otras cosas, tiene la tarea de mejorar la cooperación regional e internacional de Asia Pacífico en seguridad de la información, desarrollar conjuntamente medidas para tratar incidentes de seguridad de redes a regionales o gran escala y ayudar otros CERT[82] y CSIRTS[83] en la región para llevar a cabo respuestas informáticas de emergencia eficientes y efectivas[84].

Un último ejemplo, es el Equipo de respuesta inmediata (*Rapid Response Team* - RRT) de la OTAN, desarrollado dentro la capacidad de respuesta ante incidentes informáticos de la OTAN (NCIRC[85]) y compuesto por expertos en defensa cibernética. Esta fuerza es responsable de "ayudar a los Estados miembros que solicitan ayuda en caso de un ataque de importancia nacional"[86]. La principal misión del NCIRC es desarrollar guías de seguridad y reducir las vulnerabilidades de las redes informáticas de la OTAN. En caso de un ataque cibernético los equipos inspeccionan los dispositivos digitales y el tráfico de red emparentado con el incidente para determinar las causas del incidente y su impacto. Al mismo tiempo se buscan formas de limitar el daño y, si es apropiado, se trata de identificar la fuente y los responsables del compromiso. Como ha subrayado la autora María José Caro Bejarano en su análisis sobre la seguridad cibernética:

> *"con los RRT, la OTAN podrá ofrecer, bajo petición, asistencia profesional y bien organizada a sus miembros y socios, pero principalmente a aquellos países que aún no tienen los recursos para establecer capacidades de ciberdefensa de*

[82] Un Equipo de Respuesta ante Emergencias Informáticas (CERT, del inglés *Computer Emergency Response Team*) es un equipo de expertos informáticos, un centro de respuesta a incidentes de seguridad en tecnologías de la información. Su misión es identificar amenazas informáticas y desarrollar medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información.

[83] Un equipo de respuesta a incidentes de seguridad informática (CSIRT, del inglés *Computer Security Incident Response Team*) es una entidad organizativa concreta o una estructura interna de una organización que tiene la responsabilidad de coordinar y respaldar la respuesta a un evento o incidente de seguridad informática.

[84] Véase el sitio web de APCERT (https://www.apcert.org/)

[85] NATO Computer Incidents Response Capability Technical Centre – NCIRC. Este organismo es responsable de la provisión de los servicios de ciberseguridad técnicos y operacionales antes ciber agresiones a la OTAN.

[86] Véase el *"Equipo de reacción rápida de la OTAN para combatir el ciberataque"*, 13 de marzo de 2012 (www.nato.int/cps/en/natohq/news_85161.htm?selectedLocale=en).

este tipo. Es una versión del principio militar de mutua asistencia y defensa colectiva"[87].

1.2.a.2. Reacciones basadas en actos de regresión

Si la cooperación y la negociación no producen los efectos deseados, el Estado víctima también puede recurrir a actos de regresión. Tal acto es: "*una medida hostil, legal en sí misma, tomada por un Estado en respuesta a la conducta hostil de otro sujeto de derecho internacional, independientemente de si esa conducta es legal o no*".[88] No existen condiciones establecidas por el derecho internacional para el inicio de actos de regresión; el Estado adoptante no necesita demostrar que un *acto internacionalmente ilícito* ha sido cometido por otro Estado, ni tiene que atribuir el ciberataque a otro Estado, incluso si, a nivel político, establecer el origen del ataque sería muy útil para legitimar el acto de regresión ante la comunidad internacional.

Como se explicó anteriormente, no existen condiciones establecidas por el derecho internacional para el inicio de actos de regresión: el Estado adoptante no necesita demostrar que otro Estado ha cometido un *acto internacionalmente ilícito*, ni tiene que atribuir el ataque cibernético a otro Estado, incluso si, a nivel político, establecer el origen del ataque sería muy útil para legitimar el acto de regresión ante la comunidad internacional[89].

El orden jurídico internacional no impone condiciones para el ejercicio de actos de regresión; aparte, por supuesto, de su conformidad con el derecho internacional. Más específicamente, desde un punto de vista legal, no hay necesidad de respetar ningún principio de necesidad o proporcionalidad[90]. Por eso, el acto de regresión podría ser de una magnitud lo suficientemente grande como para enviar un mensaje agresivo a otro Estado que tendría que suspender el ciberataque, si el ataque esta producido en su territorio o bajo su jurisdicción, por sus propios agentes, o si no está tomando las medidas necesarias en el contexto de su obligación de diligencia debida. En ciertas situaciones,

---

[87] Caro Bejarano, M. J. (2012) *Ciberdefensa. Equipos de respuesta inmediata de la OTAN*. Ministerio de Defensa, Instituto Español de Estudios Estratégicos recuperado de: http://www.ieee.es/Galerias/fichero/docs_informativos/2012/DIEEEI16-2012_NatoRapidReactionTeam_MJCaro.pdf

[88] Salmon, J. (2001) *Dictionnaire de droit international public*. Editorial Bruyant Bruxelles, p. 1007.

[89] Anuario de la Comisión de Derecho Internacional (2001) idem.

[90] Brunnee, J. and. Toope, S. J. (2010*) Legitimacy and Legality in International Law: An Interactional Account*. Editorial Cambridge University Press.

tales actos de regresión podrían, por supuesto, ser mal percibidos por el Estado en cuestión o considerados inapropiados o incluso contraproducentes[91].

Ahora, estas son consideraciones políticas y estratégicas: a nivel legal, sea cual sea el alcance o la naturaleza *desproporcionada* (en comparación con los efectos de un ciberataque) del acto de regresión, no hay violación del derecho internacional. Desde un punto de vista estratégico, se podría considerar que los Estados pueden verse tentados a emprender fuertes actos de regresión, ya que podrían ayudar a "*apaciguar*" a la opinión pública después de un ciberataque, al demostrar que el Estado lesionado reacciona "*fuertemente*".

Se pude aludir que estos actos fuertes, quizás podrían ser más efectivos para obtener la cooperación del Estado en cuestión, evitando recurrir a medidas más "serias" como las contramedidas militares. Dicho esto, la práctica diplomática muestra que, si el Estado receptor considera que las medidas son hostiles e inapropiadas, podría responder a su vez mediante actos de regresión sobre la base del principio de reciprocidad[92].

En primer lugar, existen medidas diplomáticas, que pueden ir desde la simple convocatoria de un embajador hasta la interrupción completa de las relaciones diplomáticas a través del cierre temporal de la misión diplomática; la reducción de los efectivos de representación diplomática; o la declaración, en nombre del Estado receptor, de ciertos miembros del personal diplomático del Estado remitente como "*personae non gratae*", acompañada de una convocatoria para abandonar el país rápidamente[93].

En segundo lugar, medida podría ser el llamado "*nombrar y avergonzar*". La publicación, por parte de las más altas autoridades del Estado víctima, de un informe que establezca de manera convincente que el ciberataque fue cometido por agentes de otro Estado o por actores privados ubicados en el territorio de este último o que actúan bajo su control, no solo puede enviar un fuerte mensaje sobre la situación del Estado víctima y la conducta del Estado agresor, pero también legitima las próximas reacciones más significativas.

También, un conjunto de medidas podría referirse a la suspensión de beneficios otorgados sin obligación legal al otro Estado (por ejemplo, ayuda económica o militar); la suspensión de inversiones pendientes o ya realizadas en el otro Estado; la suspensión

[91] Etzioni, A. (2007) *Security First: For a Muscular, Moral Foreign Policy,* Editorial New Haven: Yale University Press.
[92] Jensen, E. T. (2010) Cyber Warfare and Precautions against the Effects of Attacks, *Texas Law Review* 88.7, pp. 1533–1569.
[93] Anuario de la Comisión de Derecho Internacional (2001) idem.

de negociaciones; la cancelación de visitas oficiales; la negación a participar en actividades políticas o culturales comunes, etc.[94]

Finalmente, una ronda de actos de regresión podría ser la adopción de embargos contra productos del otro Estado, o en contra de algunas de sus empresas consideradas involucradas en el ciberataque, o la adopción de sanciones contra ciertas entidades o individuos que se presume están involucrados en el ciberataque. Ahora, para que esas sanciones se consideren actos o regresiones, debe garantizarse que no se viole ninguna norma del derecho internacional, como las derivadas de los compromisos contraídos en el contexto de la protección internacional de los derechos humanos[95].

En general, cualquier medida que no cruce el "umbral de ilicitud" en el derecho internacional puede adoptarse como parte de una estrategia de recurso a los actos de regresión. Esto también se refiere, por supuesto, a ciertas "operaciones cibernéticas" contra el otro Estado que se considerarían lícitas de acuerdo con los criterios actuales del derecho internacional.

1.2.a.3. Reacciones a base de mecanismos excepcionales de autoprotección (estado de necesidad, caso fortuito, fuerza mayor)

El derecho internacional reconoce tres mecanismos excepcionales de autoprotección que permiten a un Estado responder a ciertas situaciones, si es necesario, mediante medidas que, en otras circunstancias, se considerarían ilegales. La característica común de estos tres mecanismos es que ninguno de ellos supone la existencia de una violación del derecho internacional por el Estado contra cuyos derechos se dirigen. También proporcionan a los Estados que los invocan "*un escudo contra una reclamación bien fundada por el incumplimiento de una obligación internacional*"[96].

La Comisión de Derecho Internacional de las Naciones Unidas ha clasificado estos tres mecanismos como *circunstancias que excluyen la ilicitud*. Según la lógica de la Comisión, las circunstancias en cuestión constituyen hechos que justifican la abolición

[94] Roberto Ago (Relator Especial). 1978. *El hecho internacionalmente ilícito del Estado como fuente de responsabilidad internacional*, A/CN.4/307 Y ADD. 1 y 2. Séptimo informe sobre la responsabilidad de los Estados, Anuario de la Comisión de Derecho Internacional, vol. II (primera parte), recuperado de: https://legal.un.org/ilc/documentation/spanish/a_cn4_307.pdf .
[95] Ibidem.
[96] Delaume, G. R. (1971) *Excuse for non-performance and force majeure in economic development agreements*, Columbia Journal of Transnational Law, Nueva York, vol. 10, N.° 2, p. 242

de la ilegalidad de un acto o, para decirlo de manera más simple, borran excepcionalmente la ilegalidad de un acto[97].

Sin embargo, es aconsejable no tratar de generalizar la invocación de estos mecanismos en reacción a un ciberataque. La Comisión de Derecho Internacional de las Naciones Unidas [98] y la Corte Internacional de Justicia han enfatizado el hecho de que estos mecanismos son admitidos solo como "excepcionales". De hecho, los tribunales internacionales rara vez aceptan su invocación, tan raramente de hecho que algunos autores han llegado a cuestionar la existencia de algunos de ellos[99]. Si bien consideramos que estos tres mecanismos son aceptados por el derecho internacional positivo, nosotros creemos que, por varias razones, especialmente debido a las condiciones muy estrictas bajo las cuales se aplican estos mecanismos, solo pueden aceptarse de manera excepcional, disminuyendo así su papel en la paleta de reacciones aceptables a los ataques cibernéticos.

• Fuerza mayor

Como plantea el artículo 23 del documento de la Comisión de Derecho Internacional, "*Artículos sobre la responsabilidad de los Estados por hechos internacionalmente ilícitos*":

"1. La ilicitud de un acto de un Estado que no esté en conformidad con una obligación internacional de ese Estado se excluye si el acto se debe a fuerza mayor, es decir, la ocurrencia de una fuerza irresistible o de un evento imprevisto, más allá del control del Estado, haciendo que sea materialmente imposible en las circunstancias cumplir con la obligación.

2. El párrafo 1 no se aplica si: (a) la situación de fuerza mayor se debe, sea sola o en combinación con otros factores, a la conducta del Estado que la invoca; o (b) el Estado ha asumido el riesgo de que ocurra esa situación".

Por lo tanto, la fuerza mayor se refiere a una situación en la que el Estado está obligado a actuar de una manera que no está en conformidad con una obligación internacional que se le impone. Difiere del caso fortuito y del estado de necesidad en el

[97] Christakis, T. (2007) *Les circonstances excluant l'illicéité : une illusion optique ?* en Droit du pouvoir, pouvoir du droit, Mélanges offerts à Jean Salmon, Bruxelles, Editorial Bruylant, 2007, p. 201-248 ; T. Christakis T. (2007) *Nécessité n'a pas de Loi' ? Rapport introductif sur la nécessité en droit international* en T. Christakis y K. Bannelier (eds), La nécessité en droit international, Colloque de la Société française pour le droit international, Editorial Pedone, Paris, p. 9- 62.

[98] Anuario de la Comisión de Derecho Internacional (2001) idem.

[99] Heathcote, S. (2005) *State of Necessity and International Law*, Thesis No. 772, University of Geneva, Geneva.

sentido de que la conducta del Estado "*es involuntaria o al menos no implica ningún elemento de libre elección*"[100]. Como explicó la Comisión, la imposibilidad material de cumplir con la obligación que origina una situación de fuerza mayor "*puede deberse a un evento natural o físico (por ejemplo, un cambio climático que puede desviar a las aeronaves del Estado al territorio de otro Estado, terremotos, inundaciones o sequías) o a la intervención humana (pérdida de control sobre una parte del territorio del Estado como resultado de una insurrección o devastación de un área por operaciones militares llevadas a cabo por un tercer Estado), o alguna combinación de ambos*"[101]. Sin embargo, estas excepciones están reguladas. En particular, se requiere que "*la situación debe ser irresistible, de modo que el Estado en cuestión no tenga ninguna posibilidad real de escapar de sus efectos*"[102]. Sin embargo, la fuerza mayor no se extiende a las circunstancias en que el cumplimiento de una obligación se ha hecho difícil pero aún es posible. Por lo tanto, es difícil imaginar en qué circunstancias la "fuerza mayor" podría justificar un ciberataque (o una reacción al mismo mediante una práctica de hack-back).

- ***Caso fortuito***

De acuerdo con el artículo 24 de los Artículos elaborados por la Comisión de Derecho Internacional:

> *"1. La ilicitud del hecho de un Estado que no esté en conformidad con una obligación internacional de ese Estado queda excluida si el autor de ese hecho no tiene razonablemente otro modo, en una situación de peligro extremo, de salvar su vida o la vida de otras personas confiadas a su cuidado.*
>
> *2. El párrafo 1 no se aplica si: a) La situación de peligro extremo se debe, únicamente o en combinación con otros factores, al comportamiento del Estado que la invoca; o b) Es probable que el hecho en cuestión cree un peligro comparable o mayor".*

Por consiguiente, el caso fortuito, se refiere a una situación en la que un agente de un Estado (un individuo cuyas acciones son atribuibles al Estado) se encuentra en una situación peligrosa, ya sea personalmente o por medio de personas que están a su cargo para protegerlas y, razonablemente, no tiene otros medios para salvar las vidas en cuestión además de violar el derecho internacional. A diferencia de una situación de fuerza mayor,

[100] Anuario de la Comisión de Derecho Internacional (2001) idem.
[101] Ibidem
[102] Ibidem

el agente del Estado no actúa involuntariamente, sino que elige violar el derecho internacional para salvar las vidas, incluso si esta elección es casi imprescindible por la situación de peligro[103].

En la práctica, el caso fortuito ha sido invocado principalmente para justificar intrusiones no autorizadas en el territorio aéreo o marítimo de otros estados por parte de barcos o aeronaves en peligro, como resultado de los fenómenos naturales, fallas mecánicas o problemas de navegación[104]. En este contexto, es difícil imaginar una situación de intrusión no autorizada en el ciberespacio de otro Estado como la única forma de salvar vidas, dicha asunción debería seguir siendo excepcional en el contexto de una respuesta a los ataques cibernéticos.

- ***Estado de necesidad***

Según el artículo 25 del documento de la Comisión de Derecho Internacional – *Artículos sobre la responsabilidad de los Estados por hechos internacionalmente ilícitos*:

"1. Ningún Estado puede invocar el estado de necesidad como causa de exclusión de la ilicitud de un hecho que no esté en conformidad con una obligación internacional de ese Estado a menos que ese hecho:

a) Sea el único modo para el Estado de salvaguardar un interés esencial contra un peligro grave e inminente; y

b) No afecte gravemente a un interés esencial del Estado o de los Estados con relación a los cuales existe la obligación, o de la comunidad internacional en su conjunto.

2. En todo caso, ningún Estado puede invocar el estado de necesidad como causa de exclusión de la ilicitud si: a) La obligación internacional de que se trate excluye la posibilidad de invocar el estado de necesidad; o

b) El Estado ha contribuido a que se produzca el estado de necesidad".

A diferencia de la fuerza mayor, el estado de necesidad no se refiere a comportamientos involuntarios o determinados. A su vez el caso fortuito, la necesidad no radica en un peligro para la vida de las personas que un agente del Estado debe proteger, sino en un grave peligro que amenaza los intereses esenciales del Estado.

---

[103] Jensen, E. T. (2010) Cyber Warfare and Precautions against the Effects of Attacks, *Texas Law Review* 88.7, pp. 1533–1569.

[104] Anuario de la Comisión de Derecho Internacional (2001) idem.

Esta circunstancia es probablemente una de las tres más probables para ser invocada por los Estados que reaccionan a los ataques cibernéticos, o incluso los inician, al afirmar que existe "*un peligro grave e inminente*" para sus "*intereses esenciales*". De hecho, el Manual Tallin 2.0, ha dedicado muchos párrafos al tema en mención. Cabe señalar, que existe una gran diferencia entre los documentos elaborados por la Comisión de Derecho Internacional de las Naciones Unidas y el Manual de Tallinn. En efecto, la Comisión había formulado el artículo 25 de manera negativa: un Estado no puede invocar el estado de la necesidad a menos que para "*enfatizar la naturaleza excepcional de la necesidad y las preocupaciones sobre su posible abuso"*[105].

El Manual de Tallin parece distinguirse de esta frase cautelosa, formulando su propia regla sobre la aplicación del estado de necesidad de una manera positiva: *"un Estado puede actuar bajo las circunstancias del estado de necesidad en respuesta a los actos que presentan un peligro grave e inminente para sus intereses esenciales, ya sea de naturaleza cibernética o no cibernética, cuando hacerlo es el único medio de protegiéndolos"*[106].

Esto es sorprendente que la Comisión enfatice que el estado de necesidad "*rara vez estará disponible para defender el incumplimiento de una obligación y que está sujeto a limitaciones estrictas para salvaguardar contra posibles abusos*"[107], dada una serie de "características especiales", Los ejemplos previstos por la Comisión, así como la aceptación muy limitada de este mecanismo por parte de las jurisdicciones internacionales, parecen confirmar la validez del enfoque cauteloso adoptado por la Comisión y advertir contra cualquier intento de acudir frecuente al estado de necesidad como mecanismo general de justificación de los ciberataques.

Llevaría demasiado tiempo realizar un análisis detallado de las condiciones muy restrictivas de invocar un estado de necesidad en el derecho internacional con relevancia en el dominio de la reacción a los ataques cibernéticos. Sin embargo, las condiciones principales son:

• la existencia de un peligro grave e inminente. Se puede invocar un estado de necesidad solo para proteger un interés esencial del Estado contra un peligro grave e inminente. No hace falta decir que un Estado no puede agitar a los fantasmas para justificar una violación

[105] Ibidem
[106] Schmitt, M.N. (2013) *Tallinn Manual on the International Law applicable to cyber welfare*. Cambridge University Press. p. 41.
[107] Anuario de la Comisión de Derecho Internacional (2001) idem.

del derecho internacional y que no puede haber estado de necesidad sin un "peligro" particularmente importante, inmediato y debidamente probado en el momento pertinente: *"vani timoris justa excusatio non est"*.[108] La Comisión también limitó considerablemente el margen de apreciación que deja a los Estados al enfatizar que "*el peligro debe establecerse objetivamente*".

• este peligro debe afectar negativamente a "un interés esencial" del Estado. Este interés puede, estar relacionado con la protección del ciberespacio y la infraestructura vital u otras áreas de actividad del Estado[109].

• la exclusividad de los medios utilizados. El requisito de que el acto incriminado debe constituir "el único medio de proteger un interés esencial contra un peligro grave e inminente" impone unos límites restrictivos. En consecuencia, el estado de necesidad no puede equipararse a fuerza mayor: el Estado elige voluntariamente violar la ley para proteger sus propios intereses y, desde este punto de vista, la condición de exclusividad de los medios busca limitar, en la medida de lo posible, cualesquiera violaciones[110]. Por supuesto, este criterio ha sido criticado por algunos autores que enfatizaron que los Estados no podrán eludirlo fácilmente[111]. Sin embargo, la Comisión no ha ofrecido ninguna clemencia en este asunto, insistiendo en su comentario del artículo 25 que *"El estado de necesidad se excluye si hay otros medios (por lo demás legales) disponibles, incluso si pueden ser más costosos o menos convenientes"*[112].

• la calidad del derecho lesionado. Nunca se puede invocar un estado de necesidad para justificar un acto que "*perjudica gravemente un interés esencial del otro Estado (o Estados) interesado(s), o de la comunidad internacional en su conjunto*". Según la Comisión, "*el interés en el que se basa debe superar todas las demás consideraciones, no solo desde el punto de vista del Estado actuante, sino en una evaluación razonable de los intereses divergentes, ya sean individuales o colectivos*"[113]. Por ende, es necesario una especie de control de proporcionalidad entre los dos "intereses esenciales" en cuestión. Este criterio establece una jerarquía estricta: el interés sacrificado debe ser inferior al interés salvaguardado.

---

[108] Salmon, J. (1984) *Faut-il codifier l'état de nécessité en droit international?*, Essays in international law in honour of Judge Manfred Lachs, Études de droit international en l'honneur du juge Manfred Lachs, Martinus Nijhoff, The Hague (Boston), pp. 251-254.
[109] Jensen, E. T. (2010) idem.
[110] Arguilla, J. y Ronfeldt, D., (1999) *The Advent of Netwar: Analytic Background*, Studies in Conflict & Terrorism 22.3, pp.193–206;
[111] Ibidem
[112] Anuario de la Comisión de Derecho Internacional (2001) idem.
[113] Ibidem

• "*manos limpias*" significa que el Estado que comete el hecho ilícito no debe haber contribuido a que ocurra el estado de necesidad[114].

• la barrera del *jus cogens*. Un estado de necesidad nunca puede justificar el incumplimiento de una "obligación derivada de una norma imperativa de derecho internacional general", como se destaca en el artículo 26 del Proyecto de artículos de la Comisión. Por lo tanto, no se puede invocar el estado de necesidad, por como, para cometer un acto de agresión contra otro Estado.

1.2.b. Posibles reacciones en caso de una violación demostradas del derecho internacional por parte de un otro Estado

Las reacciones que se va a analizar son legalmente posibles solo si un Estado ha violado el derecho internacional de una forma u otra durante la realización de un ciberataque. Por consiguiente, la existencia demostrada de un "acto internacionalmente ilícito" es indispensable en este caso[115]. Por supuesto, no hay obligación del Estado víctima de recurrir a las reacciones que se analizarán aquí: queda a discreción del Estado interesado a utilizar los mecanismos analizados anteriormente, que siempre están disponibles si los considera más apropiados en algunas situaciones. También debe enfatizarse que: de acuerdo con una norma fundamental del derecho internacional, "*todo acto internacionalmente ilícito del Estado conlleva su responsabilidad internacional*"[116].

Esto significa que un Estado lesionado por tal acto, puede hacer cumplir los mecanismos de responsabilidad internacional recurriendo siempre que sea posible, por ejemplo, a un tribunal arbitral o la Corte Internacional de Justicia y solicitar que el Estado responsable cesa el acto ilegal, no lo repite y ofrece una reparación completa por la lesión causada por su acto internacionalmente ilícito. Dejando a un lado la pregunta sobre la responsabilidad internacional del Estado que ha lanzado un ciberataque, nos centraremos en las dos reacciones a disposición de los Estados como respuesta a la ilegalidad de un ciberataque, a saber, contramedidas no forzadas y defensa propia en caso de agresión armada.

---

[114] Lotrionte, C. (2012) *State Sovereignty and Self-defense in Cyberspace: A Normative Framework for Balancing Legal Rights*, en Emory International Law Review 26/2012, pp. 825–919;
[115] Anuario de la Comisión de Derecho Internacional (2001) idem.
[116] Ibidem.

1.2.b.1. Contramedidas pacíficas

Este tipo de contramedidas pueden definirse como: "*medidas que de otro modo serían contrarias a las obligaciones internacionales de un Estado lesionado con respecto al Estado responsable, si no fueron tomadas por el primero en respuesta a un acto internacionalmente ilícito por parte de este último con el fin de procurar el cese y la reparación*"[117].

Las contramedidas resultan de las prácticas de "justicia privada" que son en gran medida inaceptables en la mayoría de los sistemas legales estatales porque estos sistemas se basan en el principio de "*nadie puede hacer justicia sobre uno mismo*" y donde el Estado es, en virtud de su soberanía, el garante de la aplicación de la ley[118].

En el orden jurídico internacional, las contramedidas "*son una característica de un sistema descentralizado por el cual los Estados lesionados pueden tratar de reivindicar sus derechos*"[119]. En ausencia de una autoridad superior a los Estados, capaz de imponer una solución, en ausencia de un tercero imparcial que tenga siempre y automáticamente jurisdicción sobre las disputas entre Estados, estos últimos están autorizados a *hacer justicia a sí mismos*, recurriendo a actos que en principio son ilegales.

Los Estados lesionados pueden recurrir a las violaciones del derecho internacional contra los Estados responsables de tales violaciones, pero solo para obligar a estos últimos a cumplir con sus obligaciones internacionales, al cesar violación y remediar las consecuencias. En tal caso, la ilicitud de las contramedidas ejercidas por el Estado víctima se "borra", porque es una respuesta justificada a un acto ilícito que comienza desde otro Estado, y su función es llevar a ese Estado al camino de la legalidad. Contrariamente al estado de necesidad o caso fortuito que deben considerarse como "excluyente o mitigante de la responsabilidad" de los Estados, las contramedidas son claramente circunstancias "que impiden la ilicitud"[120].

---

[117] Ibidem.

[118] Sin embargo, los sistemas legales nacionales prevén ciertas situaciones en las que la víctima de una violación de la ley puede recurrir a ciertos mecanismos de autoprotección sin recurrir a los tribunales: esto es particularmente cierto respecto de la excepción de incumplimiento (exceptio non adimpleti contractus) en el derecho civil o autodefensa en derecho penal. Pero estos mecanismos, que tienen sus equivalentes en el derecho internacional, difieren mucho de la autorización generalizada de contramedidas en el derecho internacional.

[119] Anuario de la Comisión de Derecho Internacional (2001) idem.

[120] Llorens, M. P. (2017). *Los desafíos del uso de la fuerza en el ciberespacio*. Anuario mexicano de derecho internacional, 17, 785-816. Recuperado de: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-46542017000100785&lng=es&tlng=es

La jurisprudencia internacional parece confirmar esta visión de las contramedidas como "justificación" de un acto ilegal. Esto también se establece por el hecho de que, hasta ahora, nunca se ha tenido en cuenta en la práctica de los Estados o de las jurisdicciones internacionales la existencia de una obligación de compensar las pérdidas sufridas como resultado de la adopción de contramedidas[121].

Por lo tanto, en caso de ciberataque que constituya un "acto internacionalmente ilícito", el Estado víctima tiene el derecho, si así lo desea, y bajo ciertas condiciones, de reaccionar contra Estado atacante, recurriendo a medidas que normalmente son violaciones del derecho internacional. Estas contramedidas no tienen que ser de la misma naturaleza que el acto ilícito original. Como resultado, el Estado víctima puede llevar a cabo en el curso de contramedidas una acción de hack-back o "un ciberataque a cambio", pero también, puede adoptar cualquier otra medida pacífica contraria a la ley: suspensión de la ejecución de un acuerdo internacional; sanciones económicas contrarias a las normas internacionales; u otras violaciones de sus obligaciones contraídas con el Estado atacante[122].

Si estas contramedidas cumplen con las condiciones de activación y ejercicio que se analizarán en adelante, se considerarán justificadas y no implicarán la responsabilidad de su autor.

• Condiciones de activación: la existencia de un hecho internacionalmente ilícito de un Estado

Las contramedidas solo están permitidas contra el Estado responsable de un acto internacionalmente ilícito y deben dirigirse exclusivamente contra él. El artículo 2 de los *Artículos sobre la responsabilidad de los Estados por hechos internacionalmente ilícitos* aclara que:

> *"Hay un hecho internacionalmente ilícito de un Estado cuando la conducta consiste en una acción u omisión:*
>
> *(a) es atribuible al Estado de conformidad con el derecho internacional; y*
>
> *(b) constituye una violación de una obligación internacional del Estado*".

[121] Opinión Consultiva de la Corte Internacional de Justicia sobre la legalidad de la amenaza o el empleo de las armas nucleares (1996) *I.C.J. Reports 1996*, p. 160. El documento en español puede consultarse en: https://undocs.org/es/A/51/218.

[122] Shackelford, S. J. (2009) *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, Berkeley Journal of International Law, 27/1/2009, pp. 192-251.

Por lo tanto, en principio, la ocurrencia de daño material no es necesario para recurrir legalmente a contramedidas; un simple daño moral o legal puede ser suficiente[123].

Por otra parte, para que exista un acto internacionalmente ilícito, deben cumplirse dos condiciones acumulativas: el incumplimiento de una obligación internacional y la atribución de dicho incumplimiento a un Estado determinado.

- **Condición de violación de una obligación internacional**

Infringir una obligación internacional es una condición sine qua non, para la adopción de contramedidas que, por definición, constituyen la respuesta a un acto ilícito original de otro Estado y son un medio para obligar al respeto de las obligaciones internacionales. Dependiendo de la naturaleza y los efectos de un ataque cibernético, se podrían haber violado varias reglas del derecho internacional, desde violaciones de *jus contra bellum* o *jus in bello* hasta abusos menos graves de la soberanía de un Estado, a través de la violación de principios como el de no intervención o el derecho de los pueblos a la libre determinación[124].

Un primer análisis de los textos del derecho internacional revela las incertidumbres en la distinción entre el principio de no intervención y el principio de no interferencia en los asuntos internos de un país. Podría considerarse que el primero se refiere a la protección del territorio del Estado, de su dominio, y que su violación implicaría, por lo tanto, la realización de operaciones materiales en territorio extranjero; mientras que este último se referiría a la interferencia, sin la autorización del Estado, en el ámbito del ejercicio de sus poderes soberanos nacionales y por ende, afectaría la soberanía del Estado[125].

---

[123] La naturaleza del "daño" sufrido por el "Estado lesionado" depende, por lo tanto, de los requisitos de la norma primaria violada por el Estado responsable. Como subrayó la Comisión: "*A veces se dice que la responsabilidad internacional no se realiza mediante la conducta de un Estado sin tener en cuenta sus obligaciones a menos que exista algún elemento adicional, en particular, el daño a otro Estado. Pero si se requieren tales elementos, hay que analizar el contenido de la obligación primaria, y no existe una regla general al respecto*". Anuario de la Comisión de Derecho Internacional (2001) idem.

[124] La interferencia grave en el proceso electoral de un Estado, que da como resultado un resultado distorsionado podría, por ejemplo, considerarse una violación de este principio. Cabe recordar que, según la codificación de este principio en la Declaración sobre los principios del derecho internacional sobre las relaciones de amistad y la cooperación entre los Estados de conformidad con la Carta de las Naciones Unidas, adoptada por la Asamblea General de las Naciones Unidas en 1970: "*En virtud del principio de igualdad de derechos y libre determinación de los pueblos consagrados en la Carta de las Naciones Unidas, todos los pueblos tienen el derecho de determinar libremente, sin interferencia externa, su condición política* [...]". A / RES 2625 (XXV) de 24 de octubre de 1970.

[125] Combacau J. y Sur S. (2001) *Droit international public*, Politique étrangère, n°3 - 1994 - 59eannée. pp. 877-879; Dupuy, P-M y Kerbrat, Y. (2014) *Droit international public*, Editorial Dalloz, Paris,12eme édition, p. 130.

Entre los textos internacionales más conocidos, la famosa Declaración sobre Principios de Derecho Internacional referente a las Relaciones de Amistad y la Cooperación entre los Estados de conformidad con la Carta de la ONU, adoptada por la Asamblea General de las Naciones Unidas en 1970, establece que:

"*Ningún Estado o grupo de Estados tiene derecho a intervenir, directa o indirectamente, por cualquier motivo, en los asuntos internos o externos de cualquier otro Estado. En consecuencia, la intervención armada y todas las demás formas de interferencia o intento de amenazas contra la personalidad del Estado o contra sus elementos políticos, económicos y culturales, constituyen una violación del derecho internacional"* [126].

La Corte Internacional de Justicia enfatizó en la Sentencia de 1986[127] en el Caso de Actividades Militares en Nicaragua que:

> "*Por consiguiente, una intervención prohibida debe tener relación con asuntos en los que cada Estado tiene permitido, por el principio de soberanía del Estado, decidir libremente. Una de ellas es la elección de un sistema político, económico, social y cultural, y la formulación de la política exterior. La intervención es ilícita cuando utiliza métodos de coerción con respecto a tales elecciones, que deben seguir siendo libres. El elemento de coerción, que define, y de hecho forma la esencia misma de la intervención prohibida es particularmente obvio en el caso de una intervención que utiliza la fuerza, ya sea en forma directa de acción militar o en forma indirecta de apoyo para actividades terroristas armadas dentro de otro Estado*".

Probablemente deberían llevarse a cabo estudios más detallados, a fin de definir mejor la distinción entre los dos principios y su contenido e identificar cuándo podrían considerarse que se han violado en el caso de un ataque cibernético. Así, por ejemplo, no cabe duda de que un ciberataque que manipula los resultados electorales en un país podría constituir una violación del principio de no injerencia[128]. Sin embargo, es más complicado definir a partir de qué punto, el mero pirateo de mensajes electrónicos de ciertas figuras

---

[126] Resolución 2625 (XXV) de la Asamblea General de las Naciones Unidas, disponible en: https://dudh.es/declaracion-sobre-los-principios-de-derecho-internacional-referentes-a-las-relaciones-de-amistad-y-a-la-cooperacion-entre-los-estados-de-conformidad-con-la-carta-de-las-naciones-unidas/.

[127] *Fallo de 27 de junio de 1986 de la Corte Internacional de Justicia* - Caso de las actividades militares y paramilitares en Nicaragua y contra Nicaragua, paragrafo §205, disponible en: https://www.dipublico.org/cij/doc/79.pdf.

[128] Egan, B. J. (2017) *International Law and Stability in Cyberspace*, 35 Berkeley J. Int'l Law. 169/2017. Recuperado de: http://scholarship.law.berkeley.edu/bjil/vol35/iss1/5.

políticas y su distribución en los medios o su publicación en Internet, se consideraría una violación del mismo principio.

En segundo lugar, es interesante observar la posición del Manual 2.0 de Tallinn que intentó determinar en qué circunstancias un ciberataque podría constituir una violación de la soberanía de un Estado. Según los expertos invitados a publicar en este libro:

> "*El carácter legal preciso de las operaciones cibernéticas remotas que se manifiestan en el territorio de un Estado es algo inestable en el derecho internacional. [...] Primero, la mayoría de los Expertos acordaron que las operaciones cibernéticas constituyen una violación de la soberanía en caso de que ocasionen daños o lesiones físicas [...]. En segundo lugar, los expertos acordaron que, además del daño físico, la causa remota de la pérdida de funcionalidad de la infraestructura cibernética ubicada en otro Estado a veces constituye una violación de la soberanía, aunque no se pudo lograr un consenso sobre el umbral preciso en el que esto es así. […]. Hubo un acuerdo total de que una operación cibernética que requiera reparación o reemplazo de componentes físicos de la infraestructura cibernética equivale a una violación porque tales consecuencias son similares a daños o lesiones físicas. [...] En tercer lugar, no se pudo llegar a un consenso sobre si, y de ser así, cuándo, una operación cibernética que no resulta en daño físico ni pérdida de funcionalidad equivale a una violación de la soberanía"*[129].

El Manual 2.0 de Tallin también consideró que "*aunque el espionaje cibernético en tiempo de paz por parte de los Estados no viola per se el derecho internacional, el método por el cual se lleva a cabo podría hacerlo*". Por otro lado, otros autores han considerado que el ciber espionaje constituye una violación del principio de no injerencia en los asuntos internos de los Estados[130].

La tercera y última observación se refiere al incumplimiento de la obligación de diligencia debida, que es particularmente relevante para el problema derivado de los ciberataques llevados a cabo por actores privados. Como hemos visto en la primera parte, en virtud de su soberanía, los Estados tienen la obligación de no permitir a sabiendas que su territorio se utilice para actos contrarios a los derechos de otros Estados. Si un Estado

---

[129] Schmitt, M. N. (2013) *Tallin Manual on the International Law applicable to cyber welfare*. Cambridge University Press. p. 31.

[130] Buchan, R. (2018) *Cyber espionage and international law*, Editorial Hart Publishing, pp. 168-189;

está al tanto (o debería haber estado al tanto) de un ataque cibernético iniciado por actores privados desde su territorio, y aún no hizo nada para evitarlo y cesarlo, entonces podría estar violando su deber de debida diligencia, por lo tanto, permitiendo que el Estado lesionado tome contramedidas, incluidas medidas de represión, contra él y contra los actores privados que operan en su territorio, hasta que el Estado responsable adopte las medidas necesarias para poner fin al ciberataque[131].

- **Condición relativa al autor de la violación de derecho internacional - un Estado responsable identificado**

Para que un Estado adopte contramedidas, la violación del derecho internacional por acción (por ejemplo, ciberataque) u omisión (por ejemplo, incumplimiento de la debida diligencia) debe ser atribuible al Estado contra el cual se adoptan las contramedidas. Por eso, la atribución parece ser una condición fundamental para la adopción de contramedidas que están justificadas sobre la base del derecho internacional.

Una primera observación sobre esta condición se refiere a los mecanismos de atribución. Es necesario distinguir entre la identificación de los atacantes como una operación técnica vinculada a la ciencia forense (ciber forense), y la atribución como una operación legal, a pesar de que los dos están estrechamente vinculados. De hecho, el derecho internacional establece mecanismos muy precisos que permiten atribuir la conducta de los actores privados a los Estados, bajo ciertas condiciones estrictas[132].

La segunda observación se refiere a las dificultades en identificar la fuente del ataque desde el punto de vista de la informática forense. Poco tiempo atrás, la atribución de ataques en el ciberespacio se consideraba particularmente difícil. A pesar de los progresos realizados y los esfuerzos de algunos para presentar la atribución como un problema ahora resuelto, persisten enormes dificultades. Estas dificultades existen debido a una multitud de factores que incluyen, en particular, la falta de capacidad técnica de varios países; el uso por parte de hackers de técnicas de ocultamiento particularmente sofisticadas (el "spoofing") para sugerir que el ataque fue iniciado por otra persona; y, por lo general, la falta de tiempo para establecer con certeza el origen del ataque antes de adoptar contramedidas que frecuentemente toman la forma de "hack-back"[133].

---

[131]. Mueller, M. L. (2010) *Networks and States: The Global Politics of Internet Governance*. Editorial Cambridge MIT Press, p. 164.
[132] Schmitt, M. N. (2013) idem. p. 35.
[133] Llorens, M. P. (2017) idem.

La complejidad y las limitaciones de la atribución de un ciberataque son reconocidos por varios Estados. Últimamente, el propio presidente de los Estados Unidos habló sobre el tema y señaló que "*a menos que atrape a los piratas informáticos en el acto, es muy difícil determinar quién estaba hackeando*", o incluso que "*hackear es algo muy difícil de probar*"[134].

Para resolver el problema de la atribución a nivel internacional, algunos Estados propusieron la creación de un mecanismo centralizado internacional que poseería la experiencia técnica necesaria para llevar a cabo operaciones de atribución confiables e independientes. En cambio, otros Estados se opusieron a esta idea, considerando que el proceso de atribución incluye no solo consideraciones técnicas y legales sino también políticas y funciones gubernamentales esenciales, que son parte del ADN de la seguridad nacional de los Estados. Además, estos países expresaron dudas sobre la capacidad de un organismo internacional para cumplir efectivamente este papel, ya que su pura creación podría incluso ser contraproducente. En conclusión, consideraron que el proceso de atribución, tanto desde el punto de vista técnico como legal, debería seguir siendo prerrogativa de los propios Estados[135].

La tercera y última observación se refiere a la cuestión de las pruebas necesarias con respecto a la atribución del ataque antes de la adopción de contramedidas. Este es un tema crucial que ha dado lugar a muchas negociaciones entre los Estados y también dentro del GEG, incluso en relación con ciertas acusaciones de ataques cibernéticos.

Sin embargo, el derecho internacional positivo está bastante claro a este respecto: no requiere que los Estados prueben sus alegaciones sobre la existencia de una violación del derecho internacional por parte de otro Estado, antes de la adopción de contramedidas contra él. Esta es un área donde el antiguo dicho "*nemo iudex en causa sua*"[136] no se aplica. En ausencia de una autoridad centralizada en el sistema legal internacional, automáticamente competente para evaluar los hechos e interpretar las

[134] Clem, R. (2018) *Clearing the Fog of War: public versus official sources and geopolitical storylines in the Russia-Ukraine conflict*, Eurasian Geography and Economics Journal, no. 58, pp. 1-21.
[135] Domínguez Bascoy, J. (2014) *La ciberseguridad: aspectos jurídicos internacionales*. Cursos de derecho internacional y relaciones internacionales de Vitoria-Gasteiz = Vitoria-Gasteizko nazioarteko zuzenbide eta nazioarteko herremanen ikastaroak, N.º. 1, 2015, págs. 161-224
[136] Es una expresión latina que se emplea en Derecho, especialmente en Derecho Procesal, para indicar que el juez no puede ser parte en un proceso en el que tenga intereses personales, antes bien, ha de quedar siempre como una tercera persona, imparcial, entre las dos partes. Su traducción literal sería «ningún juez lo es de su propia causa».

reglas aplicables a los Estados, este poder, incluidas las contramedidas[137], se deja a los Estados para decidir y aplicar.

Como lo señaló en 1978 un Tribunal Arbitral con respecto a un caso emblemático sobre contramedidas entre los Estados Unidos y Francia:

> *"De conformidad con las normas del derecho internacional actual, y a menos que resulte lo contrario de obligaciones especiales derivadas de tratados particulares, en particular de mecanismos creados en el marco de organizaciones internacionales, cada Estado establece por sí mismo su situación legal frente a otros Estados"*[138].

La Comisión de Derecho Internacional de las Naciones Unidas codificó esta regla en los *Artículos sobre la responsabilidad de los Estados por hechos internacionalmente ilícitos*. Según la Comisión:

> *"Un Estado que toma contramedidas actúa bajo su propio riesgo, si su visión de la cuestión de la ilicitud resulta no estar bien fundada. Un Estado que recurre a contramedidas basadas en su evaluación unilateral de la situación lo hace bajo su propio riesgo y puede incurrir la responsabilidad por su propia conducta ilícita en el caso de una evaluación incorrecta"*[139].

Esto significa que un Estado no tiene la obligación legal de presentar pruebas relacionadas con la atribución de un ciberataque antes de adoptar contramedidas frente al Estado acusado de ser la fuente del ataque. Si, por otro lado, se demuestra en una etapa posterior que el Estado lesionado se equivocó en el asunto de la atribución, las contramedidas adoptadas ya no estarán justificadas sobre la base del derecho internacional, y su responsabilidad internacional se activará, junto con la obligación de reparar el daño sufrido por el Estado acusado injustamente de ser el autor del ciberataque.

A este respecto, debe mencionarse que, dadas las circunstancias, la existencia de una creencia razonable o la buena fe del Estado que realiza las contramedidas, aún no sería suficiente para excluir su responsabilidad si, a pesar de todo, estaba equivocado en materia de atribución[140].

---

[137] Sicilianos, L. A. (1990) *Les réactions décentralisées à l'illicite : Des contremesures à la légitime défense*, Revue internationale de droit comparé no. 4, Paris, p. 950.

[138] El caso relativo al Acuerdo de los servicios aéreos, de 27 de marzo de 1946, entre los Estados Unidos de América y Francia, Decisión de 9 de diciembre de 1978, RIAA, vol. XVIII, p. 81;

[139] Den Dekker, G. (2001) *The Law of Arms Control: International Supervision and Enforcement*, Editorial Martinus Nijhoff Publishers, pag 206.

[140] Domínguez Bascoy, J. (2014) idem.

Aunque, incluso si el derecho positivo, en su forma actual, no parece exigir a los Estados que demuestren sus acusaciones de ciberataques, lo mejor para los Estados sería presentar ciertas pruebas con fines políticos y para defender la legitimidad de las contramedidas a los ojos de la opinión pública. Además, la cantidad y calidad de dicha evidencia debe estar de acuerdo con la escala y la severidad de las contramedidas adoptadas. Es en este sentido que el GEG de la ONU enfatizó en su Informe de 2015 que *"las acusaciones de organizar y ejecutar actos ilícitos contra los Estados deben ser fundamentadas"*[141].

- ***Condiciones de ejercicio de las contramedidas***

Si bien el derecho internacional permite el uso de contramedidas y mecanismos de *justicia privada* en las condiciones antes mencionadas, en ninguna circunstancia se puede considerar dicha práctica como un retorno a la ley de la selva. El orden jurídico internacional rige estrictamente el ejercicio de contramedidas mediante la imposición de una serie de condiciones que demuestran que estos "poderes ejecutivos" disponibles para los Estados deben utilizarse de manera prudente para evitar abusos y poner en peligro la estabilidad y la seguridad internacional. Sin entrar en los detalles de estas condiciones, destacaremos brevemente algunos de ellos para fundamentar el análisis.

- **El carácter reparatorio de las contramedidas;**

El Estado lesionado puede tomar contramedidas contra el Estado culpable del acto internacionalmente ilícito solo para inducir a ese Estado la responsabilidad para cumplir con sus obligaciones de cesación o reparación, en virtud del derecho internacional. Por lo cual, las contramedidas no tienen una función punitiva y no deben considerarse como una expresión de la ley de represalias ("lex talionis"). Más bien, representa una medida reparatoria, una respuesta cuyo único objetivo es garantizar el respeto del derecho internacional por parte del Estado que lo violó por primera vez. Las contramedidas deben ser reversibles[142] y cesar "tan pronto como el Estado responsable haya cumplido sus obligaciones" en virtud del derecho internacional[143].

---

[141] Bannelier, K. y Christakis, T. (2017) *Cyberattaques - Prévention-Réactions : Rôles des Etats et des acteurs privés*, Les Cahiers de la Revue Défense Nationale, Paris.
Recuperado de: SSRN: https://ssrn.com/abstract=2957795.

[142] Sverrisson, H. B. (2008) *Countermeasures, the International Legal System, and Environmental Violations*, Editorial Cambria Press.

[143] Wood, M. M.; Pronto, A. y Wood M. (2010) *The International Law Commission 1999-2009: Volume IV: Treaties, Final Draft Articles, and Other Materials*, vol. IV, Editorial OUP Oxford, p. 332.

• El carácter no forzado de las contramedidas;

La Comisión de Derecho Internacional de las Naciones Unidas ha codificado la norma de que las contramedidas "*no afectarán la obligación de abstenerse de la amenaza o el uso de la fuerza como se establece en la Carta de las Naciones Unidas"*[144]. Esta regla que también está codificada en otros instrumentos importantes del derecho internacional[145], excluye la posibilidad de recurrir a contramedidas militares o de reaccionar con medidas de tipo hack-back que podrían considerarse como una violación de la prohibición de la amenaza o el uso de fuerza en el derecho internacional. Esto, por supuesto, plantea una pregunta sobre cuándo se puede considerar que una acción específica ha cruzado la fina línea de la existencia de un uso prohibido de la fuerza. Este es un gran debate sobre "*jus ad bellum*" y el tema de largos análisis teóricos[146] que desafortunadamente no podemos analizar en este documento.

No obstante, un estudio reciente de Marco Roscini propone una definición amplia de operaciones cibernéticas que podría caracterizarse como una violación del Artículo 2, párrafo 4 de la Carta sobre la prohibición de la amenaza y el uso de la fuerza. De acuerdo con la conclusión del autor:

> *"Aquellos preocupados de que, al calificar las operaciones cibernéticas seriamente disruptivas como un uso de la fuerza, el riesgo de conflictos interestatales aumentará deberían tranquilizarse: de hecho, el uso de la fuerza, en sí mismo, no es suficiente para otorgar al Estado víctima el derecho a reaccionar en defensa propia, a menos que sea lo suficientemente grave como para equivaler a un ataque armado"*[147].

Además del estigma que se le atribuye, la única consecuencia de calificar las operaciones cibernéticas seriamente disruptivas como el uso de la fuerza es que no podrían llevarse a cabo en contramedidas, lo que sin duda es un resultado positivo, teniendo en cuenta el grave impacto negativo que podrían tener sobre el orden público de las sociedades digitalmente dependientes.

---

[144] Anuario de la Comisión de Derecho Internacional (2001) idem. art. 49, parag. 3

[145] Véase también la Declaración de 1970 sobre los principios del derecho internacional sobre las relaciones amistosas y la cooperación entre los Estados de conformidad con la Carta de la ONU, según la cual "*los Estados tienen el deber de abstenerse de actos de represalia que impliquen el uso de la fuerza*".

[146] Corten, O. (2010) *The Law Against War*, Editorial Hart, Oxford & Portland, pp. 50-125.

[147] Roscini, M. (2014) *Cyber Operations as a Use of Force en* Nicholas Tsagourias and Russell Buchan (eds.), Research Handbook on International Law and Cyberspace, Edward Elgar Publishing, 2015, 233-254, U. of Westminster School of Law Research Paper No. 16-05, recuperado de: https://ssrn.com/abstract=2631078

• Las contramedidas no deben violar otras obligaciones importantes de los Estados;

De conformidad con la norma codificada por el artículo 50 de la Resolución[148] (AG/56/83) de la Asamblea General de las Naciones Unidas de adopción de los artículos sobre la responsabilidad del Estado por hechos internacionalmente ilícitos, presentados por la Comisión de Derecho Internacional, las contramedidas no deben violar las obligaciones relacionadas con la protección de los derechos humanos fundamentales, las obligaciones de carácter humanitario que prohíben las represalias y las obligaciones derivadas de normas imperativas de derecho internacional general. Esta regla es particularmente importante porque prohíbe el uso de contramedidas que puedan afectar, directa o indirectamente, las obligaciones de los Estados en materia de derechos humanos, que no están inicialmente, sujetas al principio de reciprocidad en virtud del derecho internacional.

• Las contramedidas deben respetar el principio de proporcionalidad;

Como expresa el artículo 51 de la Resolución (AG/56/83)[149], "*las contramedidas deben ser proporcionable al perjuicio sufrido, teniendo en cuenta la gravedad del hecho internacionalmente ilícito y los derechos en cuestión*". A diferencia de los actos de regresión donde el principio de proporcionalidad es irrelevante, en el caso de las contramedidas desempeña un papel fundamental. La idea general es que la adopción de contramedidas, que están autorizadas con el motivo de "corregir" un desequilibrio creado por el acto ilícito original de otro Estado y con el único propósito de empujar a este último al "camino de la legalidad internacional", no debe crear un nuevo desequilibrio ni conducir a resultados injustos.

El cumplimiento del principio de proporcionalidad debe evaluarse caso por caso, teniendo en cuenta no solo el elemento puramente "cuantitativo" de la lesión sufrida, sino también factores "cualitativos" como la importancia del interés protegido por la norma infringida y la gravedad de la violación [150]. Por otro lado, el principio de proporcionalidad no exige que el Estado lesionado responda de la misma forma, adoptando contramedidas

[148] Naciones Unidas (2002) *Resolución aprobada por la Asamblea General [sobre la base del informe de la Sexta Comisión (A/56/589 y Corr.1)]*, A/RES/56/83, Responsabilidad del Estado por hechos internacionalmente ilícitos, Quincuagésimo sexto período de sesiones, recuperado de: https://undocs.org/es/A/RES/56/83.
[149] Ibidem.
[150] Sverrisson, H. B. (2008) idem.

en el mismo campo que las medidas originales. En cambio, los Estados tienen una amplia discreción a este respecto siempre que su respuesta no resulte excesiva y desproporcionada con el acto que lo motivó[151].

• **Las contramedidas deben respetar las condiciones procesales previas;**

El derecho internacional también impone una serie de requisitos procesales codificados por el artículo 52 de la Resolución (AG/56/83). Antes de tomar contramedidas, el Estado lesionado debe, primero, solicitar al Estado responsable que cumpla con sus obligaciones en virtud del derecho internacional y, luego, notificarle sobre cualquier decisión de tomar contramedidas y ofrecer negociar. El Estado lesionado puede tomar medidas urgentes de forma excepcional si son necesarias para salvaguardar sus derechos. Sin embargo, de conformidad con los mecanismos judiciales para la solución de controversias, no se pueden tomar contramedidas y, si ya se han tomado se deben suspender, si la disputa está pendiente ante un tribunal o tribunal cuya sentencia será vinculante para los Estados. Es decir, la lógica unilateral de contramedidas ya no tiene justificación, ni razón de ser, cuando el carácter "descentralizado" del sistema internacional está sombreado por la existencia de un mecanismo obligatorio e imparcial de solución de controversias a través de un proceso legal[152].

1.2.b.2. Autodefensa a en caso de ataque armado

A diferencia de las contramedidas que, como hemos visto, no pueden implicar el uso de la fuerza armada, la autodefensa brinda a los Estados la posibilidad de recurrir a la fuerza para responder a un ataque armado contra ellos. La posibilidad de invocar la autodefensa en respuesta a un ciberataque ha movilizado en gran medida la doctrina internacional y se han publicado varios estudios al respecto para examinar el tema desde el punto de vista de "*jus ad bellum"* y *"jus in bello*"[153]. Sin embargo, está claro que, por el momento, el debate sobre estos temas tiene principalmente una dimensión teórica: nunca, hasta donde sabemos, un Estado ha acusado oficialmente a otro Estado de haber llevado a cabo un "ataque armado" utilizando medios cibernéticos; nunca un Estado ha remitido tal asunto al Consejo de Seguridad; y nunca un Estado ha invocado el Artículo 51 de la Carta para responder a un ciberataque del cual se consideró víctima.

[151] Bannelier, K. y Christakis, T. (2017) idem.
[152] Domínguez Bascoy, J. (2014) idem.
[153] Roscini, M. (2014) idem.

Por eso, el debate es en gran medida de carácter progresista y puede haber un fuerte contraste entre la práctica de los Estados y el gran interés académico por "*jus ad bellum*" y "*jus in bello*" en el ámbito cibernético. Como hemos visto, las reacciones a los ciberataques están casi exclusivamente vinculados a la "Ley de la Paz". Aun cuando, dadas las predicciones alarmantes de muchos especialistas que consideran que el ciberespacio podría convertirse rápidamente en un lugar de confrontación armada entre los Estados y, por esto, dar lugar a situaciones de tipo "cyber Pearl Harbor"[154], se puede comprender la anticipación de la comunidad académica. Además, explica por qué varios Estados u organizaciones internacionales han abordado estos problemas mediante la adopción de estrategias nacionales de defensa cibernética para enfrentar o gestionar diferentes posibles escenarios.

Teniendo en cuenta estas consideraciones, así como la amplitud de los estudios publicados sobre el tema de la "guerra cibernética", limita aquí a unas breves observaciones, examinando las condiciones de activación y las condiciones de ejercicio de autodefensa en respuesta a un ciberataque[155].

Para que un Estado pueda invocar la defensa propia y responder por medios militares (o asimilados) a un ciberataque, debe ser víctima de un "ataque armado". De acuerdo con las provisiones del Artículo 51 de la Carta de las Naciones Unidas:

> "*Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. Las medidas tomadas por los Miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales*".

[154] Bumiller, E y Shanker, T. (2012) *Panetta Warns of Dire Threat of Cyberattack on U.S.*, N.Y. Times Journal, 12 October 2012, disponible en: https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

[155] National Research Council (2010) *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, National Academies Press, Washington, DC.

Cabe señalar, que la Carta de las Naciones Unidas presenta la autodefensa como un "derecho natural". Sin embargo, la autodefensa debe entenderse como una excepción al principio general de la prohibición del uso de la fuerza[156]. La consecuencia legal es que depende del Estado que invoque este "derecho" excepcional para demostrar la existencia de Las condiciones necesarias para su existencia. Por lo tanto, la carga de la prueba recae en quienes invocan una situación de defensa legítima.

Para que un Estado pueda invocar la legítima defensa, debe ser víctima de un ataque *armado* que, sin duda, puede adoptar diversas formas. Más allá de los casos clásicos, como la invasión o el bombardeo del territorio de un Estado, existen otras posibilidades, como: el ataque de la marina o la fuerza aérea de un Estado, el envío de fuerzas paramilitares, mercenarios, etc. Cabe destacar que la naturaleza de las armas utilizadas no importa tanto: el ataque puede ser ejercido por armas convencionales, armas de destrucción masiva o incluso elementos transformados en armas debido a sus efectos devastadores, como el uso de las fuerzas de la naturaleza. (desviación de un río, erupción inducida de un volcán, etc.) con fines hostiles[157]. Desde este punto de vista, no hay duda de que el ataque armado puede ejercerse utilizando medios digitales, pero para ser considerado un ataque que permite la autodefensa, los efectos de un tal "ciberataque" deben ser similares a los que resultan del uso de armas convencionales[158].

Esto nos lleva a otro criterio que es el de la gravedad: para calificar como "*ataque*", y así permitir una acción en defensa propia, una ofensiva debe tener un cierto nivel de gravedad. Por lo tanto, un uso limitado de la fuerza, como un incidente fronterizo (una patrulla militar que ataca a otra patrulla), constituye una violación del Artículo 2 párrafo 4 de la Carta, lo que implica la responsabilidad internacional de su autor, pero no necesariamente constituye un "ataque armado" y, en consecuencia, no permite que el otro Estado invoque un derecho de legítima defensa.

La Corte Internacional de Justicia ha tenido la oportunidad de enfatizar este punto en varias ocasiones, es el caso de las actividades militares en Nicaragua (1986),

---

[156] Christakis, T. y Bannelier, K. (2009) *La légitime défense a-t-elle sa place dans un code relatif à la responsabilité des Etats?*, en Constantinides (A.), Zaïkos (N.), (ed.), *The Diversity of International Law*, Essays in Honour of Professor Kalliopi Koufa, Institute of International Public Law and International Relations of Thessaloniki, Martinus Nijhoff, The Hague, pp. 519-533.
[157] Tannenwald, N. (2007) *The Nuclear Taboo: The United States and the Nonuse of Nuclear Weapons since 1945*. Cambridge University Press. p 207.
[158] Domínguez Bascoy, J. (2014) idem.

donde se manifestó que es *"necesario distinguir las formas más graves del uso de fuerza (los que constituyen un ataque armado) de otras formas menos graves"*. La idea detrás de este criterio es evitar el riesgo de escalada que ocurriría si los Estados emprendieran acciones militares en defensa propia con demasiada facilidad para responder a incidentes menores. En conclusión, un ataque cibernético con efectos limitados en el territorio del Estado víctima podría constituir una violación del derecho internacional sin ser considerado como un "ataque armado" que le da al Estado víctima la oportunidad de invocar la legítima defensa[159].

Otra pregunta fundamental se refiere a quién puede cometer un ataque. Tradicionalmente, se ha aceptado en el derecho internacional que solo un Estado puede cometer un ataque contra otro Estado. Sin embargo, desde los ataques del 11 de septiembre de 2001, varios autores[160] han considerado que los grupos de particulares también pueden cometer un "ataque armado" en el sentido del artículo 51 y que esta noción debería abarcar a cualquier persona que pueda lanzar un ataque de cierta gravedad.

Como lo hace notar esta teoría, la autodefensa podría ejercerse no solo contra otros Estados, sino también contra estos grupos como los grupos terroristas, incluidos Al-Qaeda o ISIS. La aceptación de tal teoría no viene sin problemas. El principal problema, es el hecho de que estos grupos no poseen su propia base territorial y están ubicados dentro de los territorios de los Estados que a veces no pueden eliminarlos[161].

No obstante, cualquier acción militar contra estos grupos sin el consentimiento del Estado dentro de cuyo territorio se encuentran, podría considerarse como una violación de la soberanía de ese Estado o incluso como un ataque armado. Este debate adquiere una nueva dimensión en el contexto de una reacción a los ataques cibernéticos posiblemente lanzados por una impresionante multitud de actores privados.

Es por esta razón, entre otras, que la Corte Internacional de Justicia ha adoptado un enfoque cauteloso al rechazar la aplicación de la autodefensa fuera de las relaciones interestatales. En consecuencia, su Opinión consultiva de 9 de julio de 2004 sobre las Consecuencias Legales de la Construcción de un Muro en el Territorio Palestino Ocupado, la Corte enfatizó que: "*El Artículo 51 de la Carta reconoce [...] la existencia*

[159] Shackelford, S. J. (2009) idem.
[160] En este sentido: Domínguez Bascoy, J. (2014) idem; Roscini, M. (2014) idem; Sverrisson, H. B. (2008).
[161] Wohlstetter, A. (1959) *The Delicate Balance of Terror*, Revista *Foreign Affairs* 37.1, pp. 211–234;

de un derecho inherente de auto defensa en caso de ataque armado de un Estado contra otro Estado"[162].

El debate continúa en el derecho internacional. Aunque, todos están de acuerdo en que el derecho positivo acepta la posibilidad de caracterizar un ataque armado producido por un grupo no estatal como un "ataque indirecto" cometido indirectamente por el Estado en cuyo territorio se encuentra el respectivo grupo. Esta interpretación autoriza al Estado víctima a invocar su derecho a la legítima defensa para provocar una respuesta militar contra el Estado que cometió el "ataque" indirecto[163].

Por último, pero no menos importante, hay otro debate en la doctrina sobre la posibilidad de un Estado a invocar el derecho a la autodefensa, aunque no se ha producido ningún "ataque armado" en términos del Artículo 51 de la Carta. Más específicamente, algunos autores[164] consideran que el derecho internacional reconoce ahora la teoría de la "legítima defensa preventiva", según la cual, un Estado puede responder a una amenaza inminente de ataque. Otros, han ido tan lejos como para apoyar la "autodefensa preventiva", según la cual un Estado podría reaccionar a lo que considera una amenaza distante, pero aún no materializada[165]. Por tanto, el Manual de Tallin sugirió que la teoría de la "autodefensa preventiva" en los ciberataques ya podría ser parte del derecho internacional[166]. Pese a que, un análisis en profundidad del estado actual del derecho positivo parece mostrar que el derecho internacional no acepta la "legítima defensa preventiva", de manera que, se necesita precaución en un área donde los riesgos de abuso y desestabilización del sistema internacional son muy importantes.

El respeto de los principios de necesidad y proporcionalidad representa unas las principales condiciones en la legitima defensa. Como destacó la Corte Internacional de Justicia en su Opinión Consultiva de 8 de julio de 1996 en el caso relativo a la legalidad

---

[162] A/ES-10/273 - Opinión Consultiva de la Corte Internacional de Justicia sobre las consecuencias jurídicas de la construcción de un muro en el territorio palestino ocupado (2004) Décimo período extraordinario de sesiones de emergencia, Tema 5 del programa, Medidas ilegales israelíes en la Jerusalén oriental ocupada y el resto del territorio palestino ocupado, disponible en: https://www.icj-cij.org/files/advisory-opinions/advisory-opinions-2004-es.pdf

[163] Sverrisson, H. B. (2008) idem.

[164] Potter, Evan H. (2002) Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century. Editorial: McGill-Queen's University Press.

[165] Hollis, D. B. (2014) *Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?*, en Cyberwar: Law & Ethics for Virtual Conflicts (J. Ohlin et al., eds., Oxford University Press, 2014); Temple University Beasly School of Law Legal Studies Research Paper nº 2014-16.

[166] Véase el Manual 1 de Tallinn, "Regla 13: El derecho a usar la fuerza en defensa propia surge si se produce un ataque armado cibernético o es inminente".

de la amenaza o el uso de armas nucleares: "*la sumisión del ejercicio del derecho de legítima defensa a las condiciones de necesidad y la proporcionalidad es una regla del derecho internacional consuetudinario*"[167].

Tradicionalmente, los requisitos de *necesidad* y *proporcionalidad* con respecto a una acción realizada en defensa propia son las dos caras de la misma moneda. De hecho, la acción militar en defensa propia solo puede justificarse si es una medida diseñada para poner fin al ataque armado. El uso de la fuerza en defensa propia debe ser "necesario y proporcional" en la medida en que el Estado no pueda lograr este resultado (poner fin al ataque) mediante un comportamiento diferente que no implique el uso de la fuerza armada, o mediante un uso más restringido de esa fuerza.

No hace falta decir que este criterio de proporcionalidad plantea preguntas muy difíciles y técnicas[168], pero la idea fundamental es que, como en el caso de las contramedidas, la autodefensa debe apuntar solo a repeler el ataque sin causar un nuevo desequilibrio. Según el artículo 51 de la Carta de las Naciones Unidas, los Estados tienen la obligación procesal de informar al Consejo sobre cualquier acción militar emprendida en defensa propia. El incumplimiento de esta obligación no confiere un carácter ilícito a la acción per se (ya que un ataque sigue siendo un ataque), pero constituye una violación de la Carta y podría tener otras consecuencias onerosas para el Estado en autodefensa.

En consecuencia, la Corte Internacional de Justicia ha sostenido reiteradamente que, al no informar al Consejo de Seguridad sobre sus acciones militares en el territorio de otro Estado, se puede percibir que el Estado en acción no se considera a sí mismo que está actuando en defensa propia. Al mismo tiempo, a base del artículo 51 la legítima defensa representa un derecho "subordinado" a la acción del Consejo de Seguridad:

> "*Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. Las medidas tomadas por los Miembros en ejercicio del*

[167] Opinión Consultiva de la Corte Internacional de Justicia sobre la legalidad de la amenaza o el empleo de las armas nucleares (1996) *I.C.J. Reports 1996*, p. 160. El documento en español puede consultarse en: https://undocs.org/es/A/51/218.
[168] Corten, O. (2010) *The Law Against War: The Prohibition on the use of Force in Contemporary International Law*, Editorial Hart Publishing, pp. 569.

derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales".

Aquí encontramos la visión "*multilateralista*" de los redactores de la Carta que quisieron condenar el uso unilateral de la fuerza en las relaciones internacionales tanto como pudieron: la acción unilateral en defensa propia se considera "necesaria" (y por lo tanto justificada) solo en ausencia de medidas de seguridad colectiva apropiadas. Como se mencionó en la introducción, un Estado nunca ha remitido una situación de "ciberataque armado" al Consejo de Seguridad de la ONU. Esta posibilidad sigue siendo teórica por el momento.

CAPITULO II. Seguridad cibernética activa y Seguridad cibernética defensiva

El libre acceso a Internet puede convertirse en cada momento en un nuevo derecho humano reconocido al nivel mundial. Los gobiernos y las organizaciones internacionales abogan por el reconocimiento formal de su contenido y de su importancia para la libertad de expresión, opinión e intercambio de información. Junto con la inclusión del derecho al internet en las declaraciones y cartas internacionales, también es importante reconocer formalmente la seguridad cibernética como derecho humano emergente que garantiza en cierta medida la paz cibernética en el entorno virtual.

Este capítulo investiga los matices de este debate y analiza las implicaciones de tal designación desde la perspectiva de los movimientos de responsabilidad social corporativa (RSC) y la diligencia debida en ciberseguridad.

En última instancia, es importante aprovechar una variedad de herramientas multidisciplinarias del derecho, las ciencias sociales y las humanidades para promover la paz cibernética, por ejemplo, mediante la ampliación de los programas de desarrollo de la fuerza laboral y la búsqueda de lecciones de áreas relacionadas, como la sostenibilidad. Ningún individuo, organización o nación es una isla en el ciberespacio. Ese punto quedó claro con el ataque de WannaCry "ransomware", de 2017, supuestamente planeado por Corea del Norte, que infectó a más de 200.000 computadoras repartidas en 150 países.

Las consecuencias de esta campaña destacaron hasta qué punto el software obsoleto puede afectar negativamente no solo a los propietarios de las computadoras, sino en última instancia al ecosistema de Internet en general. De hecho, en respuesta, el presidente y director legal de Microsoft, Brad Smith[169], declaró:

> *"Debemos tomar de este reciente ataque [ransomware] como una determinación renovada para una acción colectiva más urgente. Necesitamos que el sector tecnológico, los clientes y los gobiernos trabajen juntos para protegerse contra los ataques de ciberseguridad. Se necesitan más acciones, y se necesitan ahora"*.

Las empresas afectadas un mes después por el ataque NotPetya, de junio de 2017, no hicieron caso a esa advertencia, aunque los atacantes utilizaron la misma

[169] Smith, B. (2017) *The Need for Urgent Collective Action to Keep People Safe Online: Lessons from last Week's Cyberattack*, Microsoft Corporation, recuperado de: https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/.

vulnerabilidad que WannaCry. Solo algunas partes interesadas del sector público y privado se están dando cuenta.

En este contexto, el Departamento de Seguridad Nacional de EE. UU. ha destacado la importancia de la "responsabilidad compartida" de las empresas para protegerse contra los ataques cibernéticos. Los consumidores no pueden proteger sus servicios públicos, sistemas bancarios o incluso sus datos personales por sí mismos, y deben depender de las empresas para manejar esa seguridad y del gobierno para ayudar a responsabilizar a los oportunistas.

En lugar de definirse exclusivamente en términos de económicos (*return on investment – RoI*), las medidas de ciberseguridad deben ser analizadas desde una perspectiva relacionada con el impacto en la sostenibilidad[170] corporativa y social general. El esfuerzo de incluir el acceso al Internet como unas de las libertades fundamentales[171] debe ser seguido de una política que apoya las medidas de ciberseguridad como garantías de los derechos humanos, tanto en línea como fuera de línea.

De hecho, el acceso a Internet puede considerarse un derecho humano emergente. Tanto las organizaciones internacionales como los gobiernos nacionales han empezado una acción conjunta de propaganda con el fin de reconocer formalmente su importancia para la libertad de expresión, opinión e intercambio de información.

El siguiente paso para ayudar a garantizar cierta medida de paz cibernética puede ser que la ciberseguridad también sea reconocida como un derecho humano. Sin embargo, hasta ahora, la conexión entre la ciberseguridad y los derechos humanos ha sido subestimada en la doctrina[172].

Pero ¿qué es la diligencia debida en ciberseguridad y en qué se parece o se diferencia de las concepciones de la diligencia debida en materia de derechos humanos? En el contexto transaccional del sector privado, este término se ha definido como "la revisión de la gobernanza, de los procesos y de los controles que se utilizan para proteger los activos de información"[173].

---

[170] Shackelford, S.J.; Fort, T.L. y Charoen, D. (2016) *Sustainable Cybersecurity. Applying Lessons From the Green Movement to Managing Cyber Attacks,* University of Illinois Law Review, recuperado de: https://illinoislawreview.org/print/volume-2016-issue-5/sustainable-cybersecurity-applying-lessons-from-the-green-movement-to-managing-cyber-attacks/

[171] Rothkopf, D. (2015) *Is Unrestricted Internet Access a Modern Human Right?*, recuperado de: https://foreignpolicy.com/2015/02/02/unrestricted-internet-access-human-rights-technology-constitution/

[172] Sarfaty, G. A. (2013) *Human Rights Meets Securities Regulation*, 54:1 Va J Int'l L 97, recuperado de: https://core.ac.uk/download/pdf/228422158.pdf

[173] Shackelford, S. J. (2017) *Cybersecurity as Social Responsibility: Business, Music, and the Symphony of Cyber Peace,* Indiana Law Journal, Kelley School of Business Research Paper No. 17-69, recuperado de: https://ssrn.com/abstract=3037221

En pocas palabras, la diligencia debida se refiere a actividades para identificar y comprender los riesgos que enfrenta una organización. Las obligaciones de diligencia debida en ciberseguridad pueden existir entre estados, entre actores no estatales (por ejemplo, corporaciones privadas, usuarios finales) y entre actores estatales y no estatales, y se refiere a las obligaciones internacionales de los actores estatales y no estatales para ayudar a identificar y aplicar las mejores prácticas de ciberseguridad para promover la seguridad de la infraestructura crítica de TIC. Así, la norma "compromete a los Estados a garantizar que ninguna acción que se origina en su territorio en tiempos de paz viola los derechos de otros Estados"[174].

Las políticas de diligencia debida en ciberseguridad implican dos técnicas de defensa que los estados pueden aplicar en el espacio virtual: una técnica ofensiva o una técnica defensiva. A lo largo de esta investigación se analizará cada tipo de política de ciberseguridad, la compatibilidad con la protección de los derechos fundamentales y las opiniones de la doctrina sobre la aplicación de cada tipo de medida de seguridad empleada por los estados.

2.1. La política de seguridad cibernética activa (ofensiva)

La política de seguridad cibernética activa u ofensiva se basa en la idea de que "*la mejor defensa es un buen ataque*". La práctica más conocida de seguridad ofensiva es el "hack-back". El término "hack-back", o "hacking back" o "hackeo inverso", realmente no tiene una definición oficial y prácticamente ninguna organización internacional ha abordado realmente este tema crucial pero altamente sensible. Este término, que podría traducirse en español como "contra piratería", "piratería a cambio" o incluso "contraataque", describe una actividad fácilmente comprensible: el hecho, para la víctima de un ciberataque, de tomar represalias contra su autor. El término "hack-back" indica que la respuesta a un ciberataque puede usar técnicas que son casi tan variadas como el ataque ("hacking") en sí. Como Renee Albersheim escribió en 1999:

> *"La contra piratería o el hack-back implica devolver el ataque a un hacker. Un hacker es alguien que a través de diversos medios técnicos obtiene acceso a un sistema informático sin autorización. Con un hack-back, un administrador del*

[174] Bendiek, A. (2016). *Due Diligence in Cyberspace: Guidelines for International and European Cyber Policy and Cybersecurity Policy*, Berlin: Stiftung Wissenschaft und Politik German Institute for International and Security Affair.

sistema identifica al pirata informático cuando ingresa al sistema y envía una respuesta similar. El objetivo es evitar daños en el sistema del administrador, mientras se daña el sistema del atacante con la esperanza de que esto disuada al pirata informático de intentar volver a atacar"[175].

Sin embargo, para evitar calificar a la víctima que reacciona a un ataque como "hacker" (ciertamente "*a cambio*", pero "*hacker*" de todos modos) es recomendable usar eufemismo: el termino de "defensa cibernética activa". Este neologismo[176] no solo evita el uso de palabras que pueden tener una connotación peyorativa para describir la reacción de la víctima, sino que también permite aportar un alto grado de legitimidad a la reacción de la víctima siendo relacionado al concepto legal de "autodefensa". Además, esta expresión oscurece el carácter ofensivo de las medidas adoptadas: no es una contraofensiva sino una "defensa activa".

La literatura de especialidad considera que el término "defensa cibernética activa" se utiliza para describir varias actividades que proceden desde la "defensa pasiva" y pueden desarrollarse en ciertas técnicas particularmente agresivas como la destrucción de las redes, sistemas o datos del atacante, a través de otras medidas como la desconexión, la inactivación de *botnets*, la suspensión temporal de la funcionalidad sistema o acceso a datos, etc. El hecho de instalar y activar un firewall o antivirus podría también ser calificado como "defensa cibernética activa". Además, ciertas técnicas son difícil de localizar con precisión entre los dos extremos posibles del espectro de la ciberdefensa (pasivo/ ofensivo). Pongamos por caso, los famosos "*honeypots*" (ollas de miel) destinados a atraer adversarios conocidos o potenciales para identificarlos y posiblemente neutralizarlos. La función principal de estos *honeypots* es atraer a los piratas en una zona determinada para desenmascararlos, pero también se pueden usar para monitorizar el sistema del adversario para anticipar y prevenir futuros ataques. En una lógica más agresiva, las "ollas de miel" también podrían usarse para introducir en el sistema del

[175] Albersheim, R. (1999) *The Legal Implications of Corporate Reverse Hacking*, Preventive Law Reporter, vol. 18, p. 8, disponible en: https://heinonline.org/HOL/LandingPage?handle=hein.journals/prevlr18&div=8&id=&page=.

[176] Si este término es relativamente nuevo en el contexto cibernético, el término "defensa activa" ya se había utilizado (no sin generar controversias) en el contexto de la guerra convencional ya en 1974. El Departamento de Defensa de los Estados Unidos, en el Diccionario de Fuerzas Armadas y Términos Asociados, define "defensa activa" como "el empleo de acciones ofensivas limitadas y contraataques para negar un área o posición en disputa al enemigo".

adversario capacidades ciber ofensivas que puedan robar o destruir datos, suspender el funcionamiento de las redes o causar daños irreversibles a sus sistemas informáticos[177].

Siendo así, en este análisis preferimos no usar este término complejo de "defensa cibernética activa" y usaremos el término "*hack-back*" para enfocarnos en las técnicas de respuesta ofensiva. A continuación, se detalla las ventajas del hack-back, los riesgos y las normas de derecho internacional sobre este tema.

2.1.a. Las ventajas de la práctica del hack-back

Varios argumentos se han movilizado para apoyar el hack-atrás, pero los riesgos e inconvenientes de esta práctica son numerosos. Se han presentado al menos seis argumentos para exaltar los beneficios del hack-back.

• **El hack-back puede completar las acciones gubernamentales**. Uno de los argumentos clave presentados a favor de la represión es que los gobiernos no pueden proteger eficazmente a las personas jurídicas y físicas de los ciberataques. La acción del gobierno, descrita como lenta y cargada de dificultades, en última instancia ofrecería pocas garantías a las víctimas. Por tanto, el hack-back permitiría evitar la lentitud de un poder ejecutivo y jurisdiccional a veces incapaz de actuar en el espacio digital. Como señaló Jan Messerschmidt:

> *"Los hack-backs evitan algunos de los desafíos más problemáticos de los remedios tradicionales, que incluyen «juicios largos, asuntos jurisdiccionales espinosos, jurados que no comprenden la tecnología y tribunales lentos» que no ayudan cuando los virus y gusanos informáticos pueden propagarse a velocidades notables. La aplicación de la ley tradicional generalmente carece de los recursos o de la experiencia necesaria para responder adecuadamente a los ataques cibernéticos, y es en gran medida ineficaz en casos de intrusiones transfronterizas"*[178].

Desde un punto de vista ético, la incapacidad del Estado de actuar eficazmente para proteger a las personas físicas y jurídicas contra los ciberataques abriría el camino a

[177] Gervais, M. (2012) *Cyber Attacks and the Laws of War*, Berkeley Journal of International Law, 30/2/ 2012.
[178] Messerschmidt, J. (2013), *Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm*, Columbia Journal of Transnational Law, 52(1).

una derogación del "contrato social" que había transferido al Estado soberano el "monopolio de restricción legítima":

> *"Si existe un contrato social para intercambiar nuestros poderes ejecutivos naturales por seguridad colectiva, que parece un acuerdo razonable, basado en la capacidad del estado de cumplir con su propósito de protegernos. Si el estado falla en cumplir con este deber con respecto a una amenaza particular, el contrato social no se anula completamente, pero el monopolio del estado sobre la violencia podría regresar a los ciudadanos para defenderse"*[179].

• ***El hack-back representa una respuesta rápida y eficiente.*** Este argumento manifiesta que: los ataques cibernéticos requieren una respuesta inmediata para contrarrestar efectivamente al adversario. Además, requerían un trabajo de anticipación que pasa por el desarrollo de señuelos que permitan rastrear las actividades de los piratas en el sistema de la compañía, asignar el ataque y prevenir nuevos ataques, mediante técnicas de defensa cibernética activa.

De modo que, aceptar un enfoque puramente *reactivo* del estado significaría dejar la iniciativa al adversario. Además, dada la experiencia técnica y el poder de las grandes empresas informáticas (Google, Microsoft, Apple, etc.) y de las empresas especializadas en ciberseguridad, las respuestas privadas podrían ser más efectivas que las públicas. En este contexto, recordamos que el "hack-back" fue popularizado por la respuesta inmediata de Google al ciberataque de McAfee denominado "Operación Aurora".

A finales del año 2009, Google se había dado cuenta de que era víctima de un ciberataque significativo y sofisticado. En ese momento, consideró que se requería una respuesta inmediata para evitar el robo y la alteración de los códigos fuente, identificar a los piratas informáticos y detener su ataque. El contraataque le permitió establecer que otras treinta empresas, principalmente estadounidenses, fueron atacadas por la operación, avisar las autoridades competentes y a las otras víctimas[180]. Esta necesidad de autoprotección rápida sería aún más importante desde el desarrollo del Internet de las

[179] Lin, P. (2016) *Ethics of Hacking Back: Six arguments from armed conflict to zombies*, p. 8, disponible en: http://ethics.calpoly.edu/hackingback.pdf.
[180] Zetter, K. (2010) *Google Hack Attack Was Ultra Sophisticated, New Details Show*, disponible en: https://www.benton.org/headlines/google-hack-attack-was-ultra-sophisticated-new-details-show.

cosas (IoT), que supone la comercialización de miles de millones de objetos conectados[181].

• ***El hack-back despliega un efecto disuasorio significativo.*** El efecto disuasorio del hack-back ha sido defendido a menudo por sus partidarios. Desde el punto de vista de un informe publicado en mayo de 2013, la Comisión Estadounidense sobre el Robo de Propiedad Intelectual, recomendó al gobierno y al Congreso de los EE.UU. que las empresas estadounidenses tengan la oportunidad de responder a los ataques cibernéticos de una manera "*disuasiva basada en amenazas*". Según la Comisión:

> *"Los conceptos de seguridad efectivos contra ataques dirigidos deben basarse en el hecho de que una defensa perfecta contra la intrusión es imposible. El concepto de seguridad disuasiva basada en amenazas está diseñado para introducir contramedidas direccionadas en contra específicos piratas informáticos hasta el punto de que decidan que ya no vale la pena realizar los ataques"*[182].

La idea es que una respuesta rápida y sólida del sector privado podría aumentar significativamente los riesgos y los costos para los piratas informáticos y obligarlos a abandonar futuros ataques cibernéticos. Si un posible pirata informático sabe que una empresa como Google contraatacaría y que habría graves consecuencias para él, es probable que se abstenga de lanzar un ciberataque, incluso se han hecho analogías con la disuasión nuclear; sin embargo, en el contexto existe una gran diferencia entre las dos situaciones y, como veremos, el efecto disuasorio del hack-back está lejos de ser la solución en algunos casos[183].

• ***Las prácticas de hack-back permiten a las empresas esconder sus vulnerabilidades***.

Las empresas pueden ser reservadas con la idea de cooperar con las autoridades estatales y, por ende, pueden preferir proporcionar su propia defensa, ya sea pasiva o activa. Pedir ayuda o asesoramiento por parte de las autoridades del Estado presenta la posibilidad de que sus defectos de seguridad y otras vulnerabilidades se hagan públicos.

---

[181] Katyal, N. (2005) *Community Self-Help*, Journal of Law, Economics and Policy, Vol. 1, p. 60.
[182] The Commission on the Theft of American Intellectual Property (2017) IP Commission report - The theft of American intellectual property, The National Bureau of Asian Research, disponible en: http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf,.
[183] Kanuck, S. (2010) *Sovereign Discourse on Cyber Conflict Under International Law*. Texas Law Review, vol. 88, pp. 1571 y ss.

Esto podría afectar negativamente la reputación de la empresa (por ejemplo, que no es capaz de proteger los datos del cliente), afectar el precio de las acciones de la empresa (o sus bonos) o incluso ser utilizado por sus competidores con fines de publicidad negativa. En términos más generales, las empresas privadas también pueden no desear que los departamentos gubernamentales accedan a sus sistemas, sus datos y los datos de sus clientes[184].

Las revelaciones de Snowden han demostrado el alcance de la vigilancia masiva llevada a cabo por los servicios secretos de ciertos estados y el hecho que la proliferación de leyes de vigilancia en todo el mundo no alivia estos temores. A nivel institucional, una solución podría ser una separación orgánica dentro de los Estados entre las actividades de inteligencia y la seguridad cibernética. El ejemplo de Francia podría ser útil a este respecto, porque la Agencia Nacional de Seguridad Cibernética[185] (ANSSI) se encuentra fuera de la comunidad de inteligencia. Esto permite que ANSSI coopere con empresas privadas y otras administraciones, que generalmente están menos inclinadas a cooperar con los servicios de inteligencia, al tiempo que fomenta la gestión responsable de las vulnerabilidades informáticas.

En España la autoridad competente es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN) [186] que es una estructura del centro Nacional de Inteligencia. Su misión y atribuciones son regulados por la Ley 11/2002, el Real Decreto 421/2004 y en el Real Decreto 3/2010. El CCN-CERT es responsable de la seguridad de los sistemas clasificados y los sistemas de la Administración y de empresas pertenecientes a sectores designados como estratégicos, que debe proteger antes los ataques cibernéticos. Al mismo tiempo, para los sistemas que no son clasificados, existe el Instituto Nacional de Ciberseguridad[187] (INCIBE) como responsable para la ciberseguridad, una empresa pública organizada como sociedad anónima estatal, bajo la tutela y propiedad del Ministerio de Asuntos Económicos y Transformación Digital de España.

---

[184] Pana, A. (2019) *Rolul factorului uman în asigurarea protecţiei datelor personale prelucrate în cadrul comunităţilor virtuale. (El papel del factor umano en la protection de los datos personales en las comunidades virtuales)*; Revista Pandectele Române, nr. 6/2019, Wolters Kluwer România, p. 79-91.
[185] Véase el sitio web de l'Agence Nationale de la Sécurité des Systèmes d'information (www.ssi.gouv.fr/).
[186] https://www.ccn-cert.cni.es/sobre-nosotros/mision-y-objetivos.html
[187] La sociedad anónima se dedica a apoyar y asesorar en materia de seguridad informática a los ciudadanos, empresas públicas y privadas, así como a las administraciones públicas y sus organismos, y a las instituciones académicas y de investigación, especialmente a los administradores de infraestructuras críticas. Asimismo, participa en la Estrategia Nacional de Ciberseguridad. Mas información en: https://www.incibe.es/.

En Rumania, el Centro Nacional Cyberint[188] es la estructura responsable para proteger la seguridad cibernética del país y está organizado como una dirección del Servicio Nacional de Inteligencia. No tiene propia capacidad jurídica.

• Las prácticas de hack-back pueden solucionar problemas delicados de extraterritorialidad.

Estas medidas de seguridad ayudan a los Estados a proteger a las personas jurídicas ubicadas en el extranjero, que son víctimas de ciberataques. Es cierto que, en virtud de su jurisdicción propria reconocida por el derecho internacional, el Estado puede actuar para la protección de sus nacionales en el extranjero, pero dicha acción puede estar sujeta al ejercicio de la jurisdicción territorial del Estado en cuyo territorio se encuentren estas personas atacadas.

Al mismo tiempo las prácticas de hack-back ayudan a los Estados a proteger incluso las empresas extranjeras en su territorio, respetar los objetivos de confidencialidad y discreción y evitar los riesgos del ciber espionaje industrial. Esto es posible porque el hack-back evita estas dificultades al brindar a estas compañías la oportunidad de defenderse contra los ataques cibernéticos sin tener que permitir a los Estados el acceso a sus sistemas informáticos[189].

• El hack-back es capaz de fomentar los negocios y la investigación.

Finalmente, el hack-back tiene la vocación de enriquecer enormemente el potencial de investigación y desarrollo para la industria activa de defensa cibernética. Dada la escala de amenazas, el mercado de seguridad cibernética es particularmente lucrativo. A pesar de las continuas dudas sobre la legalidad de las actividades de hack-back, las compañías que ofrecen herramientas activas de ciberdefensa están aumentando, independientemente de si pueden ser compañías especializadas en ciberseguridad o son solo grandes actores industriales que desarrollan actividades en este campo para no perderse lo que consideran "*un vasto mercado emergente del sector privado para soluciones de ciberseguridad*"[190].

---

[188] Mas información en: https://www.sri.ro/cyberint.

[189] Bannelier, K. y Christakis, T. (2017) *Cyberattaques - Prévention-Réactions : Rôles des Etats et des acteurs privés*, Les Cahiers de la Revue Défense Nationale, Paris, recuperado de: SSRN: https://ssrn.com/abstract=2957795.

[190] Thompson, K. (2014) *Lockheed Martin Moves to Dominate Cyber Defense of Electric Grid & Energy Complex*, Revista Forbes, 14 March 2014, recuperado de:

2.1.b. Las desventajas y los riesgos asociados al hack-back.

El hack-back implica varios riesgos: riesgos para el sistema internacional y su estabilidad, riesgos para los Estados y riesgos para las empresas también. En adelante vamos a presentar unos de estos riesgos principales.

2.1.b.1. Riesgo a desencadenar un conflicto internacional

El uso de técnicas de hack-back por parte de actores privados de técnicas cibernéticas ofensivas contra actores no estatales en el territorio de otro Estado, e incluso contra un Estado mismo, podría conducir a una escalada rápida, transformando un evento inicialmente aislado en una verdadera crisis internacional. El Estado atacado (o que desea defender a sus nacionales) podría responder denunciando la atribución del ciberataque inicial como errónea o denunciando que las medidas de hack-back no son necesarias ni proporcionadas en vista de las circunstancias. Esta respuesta podría en sí misma generar una contrarréplica del otro Estado que podría desear defender a sus personas físicas o jurídicas considerando que han sido atacadas dos veces.

Por eso, el hack-back puede conducir a la entrada de los dos Estados en un peligroso círculo vicioso de ataques y contraataques. Según otro escenario, los terceros Estados cuyas personas físicas o jurídicas serían las víctimas colaterales de las medidas de hack-back, también podrían decidir actuar contra el iniciador de la medida[191].

Obviamente, estos tipos de escenarios estarían en total contradicción con los objetivos del derecho internacional contemporáneo, que ofrece a los Estados diferentes mecanismos para la solución pacífica de disputas entre sí (o de disputas que afectan a sus nacionales y bienes). Como hemos presentado más arriba, la reacción normal en el caso de un ciberataque debería dirigirse al Estado donde se originó el ataque, pidiéndole que actúe con urgencia y ponga fin al ataque en virtud de su obligación de diligencia debida.

Es preferible favorecer la cooperación y el desarrollo de operaciones conjuntas para encontrar una solución pacífica de las controversias, de acuerdo con los principios de derecho internacional[192]. Permitir que las empresas "*hagan justicia por sí mismas*"

www.forbes.com/sites/lorenthompson/2014/03/14/lockheed-martin-moves-todominate-cyber-defense-of-electric-grid-energy-complex/.

[191] Kanuck, S. (2010) idem.

[192] Lin, P. (2016) idem.

podría generar un aumento dramático en las amenazas a la seguridad internacional, teniendo en cuenta los riesgos de escalada.

2.1.b.2. Riesgos a desestabilizar la paz internacional

Estos riesgos de seguridad podrían desestabilizar fácilmente el sistema internacional. Si un Estado permite el hack-back y sus empresas la practican, es muy probable que otros Estados hagan lo mismo. Como el derecho internacional se basa en el principio de reciprocidad, ese curso conduciría inevitablemente a una simetría legal entre las empresas de los diferentes Estados. Como no sería posible que el hack-back estuviera legalmente reservado para compañías en ciertos Estados, en teoría, podría ser ejercido por cualquier compañía ubicada en cualquier parte del mundo. Cuando somos conscientes de las dificultades que enfrenta el derecho internacional para establecer estándares de coexistencia pacífica entre menos de 200 estados, apenas podemos imaginar lo que sucedería si el derecho internacional tuviera que lidiar con más o menos 200 millones de compañías existentes en todo el mundo decididas a lanzar ataques transfronterizos si son atacados[193].

2.1.b.3. Riesgos a comprometer la política exterior.

Una actividad de hack-back prematura o descoordinada, realizada sin consultar con las autoridades, podría crear tensiones diplomáticas y complicar la política exterior de un Estado. Esto ha sido particularmente evidente cuando las compañías privadas de ciberseguridad han atribuido públicamente un ciberataque a un Estado extranjero[194].
En un extenso informe[195] publicado en febrero de 2013, la empresa de ciberseguridad Mandiant describió la evidencia que había acumulado contra un grupo, denominado Advanced Persistent Threat 1 (APT1), que había comprometido a 141 empresas en siete años.

La compañía Mandiant identificó un edificio en Shanghái de donde se lanzaban los ataques cibernéticos sobre empresas estadounidense y concluyó que APT1 es la Unidad 61398 del Ejército de Liberación Popular de China. Según su investigación,

[193] Messerschmidt, J. E. (2005) *Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm*, Columbia Journal of Transnational Law, Vol. 52, No. 1, p. 293.
[194] Segal, A. (2016) *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*, Editorial Public Affairs; 1st Edition.
[195] Disponible en: https://issuu.com/dragonjar/docs/mandian-apt1-report.

Mandiant alegó que "*el Partido Comunista de China está encargando al Ejército de Liberación Popular de China para cometer ciber espionaje sistemático y robo de datos contra organizaciones de todo el mundo"*[196]. El informe proporcionó no solo información sobre los métodos de ataque de APT1, sino también detalles y fotos de varias "personas APT1" que "*tomaron malas decisiones de seguridad operativa*" que permitieron a Mandiant identificarlos.

El informe Mandiant desencadenó un cambio radical en la política de EE. UU. hacia China en cuestiones de ciberseguridad. Impulsó al gobierno de Obama a comenzar a acusar abiertamente al gobierno chino por el robo de propiedad intelectual. Menos de un mes después de la publicación del informe, el Asesor de Seguridad Nacional, Tom Donilon, pronunció un discurso ante la Sociedad de Asia y pidió al gobierno chino que "*tome medidas serias para investigar y poner fin a estas actividades*"[197].

Después de este informe, el gobierno de EE. UU. ha alentado la cooperación con las empresas de ciberseguridad para enfrentar a los ataques patrocinados por el estado chino. Pero no está claro que los incentivos de las empresas de EE. UU., que tienen razones comerciales para atribuir ataques patrocinados por el estado, siempre se alinearán con los valores públicos que se supone que debe servir el gobierno de EE. UU.

2.1.b.4. Riesgos a erosionar la autoridad del Estado.

Más allá del orden internacional, el orden interno en sí mismo podría verse amenazado. Aceptando la idea de que "*los Estados no pueden garantizar la seguridad en el ciberespacio*"; que el "*contrato social*" está, por lo tanto, roto[198]. Puede resultar ser peligroso que el monopolio del Estado sobre la violencia legítima se pone así en cuestión.

El orden legal estatal se basa en la idea de prioridad de la justicia institucional sobre la justicia privada que prevaleció en el "*Estado natural*" antes de la creación de sociedades civilizadas[199]. Contradecir el principio "*nadie puede tomar la ley en sus propias manos*" (o "*nadie puede hacerse justicia a sí mismo*") sería lo mismo que permitir los comportamientos antisociales, que probablemente sembrarán el desorden. Es cierto

[196] Mandian (2013) *APT1 Report, Exposing one of China's Cyber Espionage Units*. Recuperado de: https://issuu.com/dragonjar/docs/mandian-apt1-report.
[197] Franzen, C. (2013) *US national security advisor warns China: 'We will take action... against cyber threats'.* Recuperado de: https://www.theverge.com/2013/3/11/4091112/white-house-advisor-tom-donilon-warns-china-cyber-attacks.
[198] Ibidem.
[199] Rousseau, J. J. (1996) "*El contrato social",* libro II, cap. I, Edit. Alba, Madrid.

que, en teoría, los Estados podrían evitar la erosión de sus poderes de regulación y prohibir el hack-back interno, al tiempo que permitan el hack-back transnacional.

2.1.b.5. Riesgos relacionados con la ciberdefensa activa "automática"

La ciberdefensa activa se está volviendo cada vez más "automatizada" y papel de factor humano pasa en el plan secundario de la política de defensa. Para responder de manera más efectiva a los ataques cibernéticos y adaptarse a la creciente complejidad de los medios utilizados, la defensa cibernética activa utiliza el aprendizaje automático y la inteligencia artificial, eliminando el factor subjetivo insertado por el ser humano en la decisión[200]. Esta decisión elimina la posibilidad de elegir si un acto de hack-back es oportuno o será mejor adoptar otra medida para responder a un ataque cibernético. La automatización aumenta la adaptabilidad, la reactividad, la precisión y, en definitiva, la efectividad del hack-back, pero también los riesgos de error en caso de mal diseño y programación del sistema o en caso de su manipulación por un acto malicioso externo[201].

2.1.b.6. Riesgos a afectar los derechos de las personas no implicadas.

Los terceros inocentes podrían convertirse en víctimas de las actividades de hack-back. Esto ocurre, en primer lugar, como resultado de los errores en la atribución. El riesgo es aún más importante cuando la acción de hack-back podría iniciarse sin tomar el tiempo necesario para atribuir el ataque con relativa certeza. La experiencia acumulada por las compañías privadas de seguridad muestra que los agentes de seguridad privada poco entrenados y entusiastas pueden actuar de manera inoportuna o incluso abusiva[202].

El riesgo de daño colateral también se deriva de la naturaleza de algunos ataques cibernéticos. En el contexto de un ataque de denegación de servicio (DDoS), por ejemplo, los piratas informáticos pueden usar computadoras "*zombies*"[203] sin el conocimiento de

---

[200] Pana, A (2019) idem.
[201] Dinstein, Y. (2011) *War, Agression and Self Defence*, Fifth, Editorial: Cambridge University Press.
[202] Ibidem.
[203] "En informática, un zombie -o zombi- es un ordenador conectado a la red que ha sido comprometido por un hacker, un virus informático o un troyano. Puede ser utilizado para realizar distintas tareas maliciosas de forma remota. Este uso se produce sin la autorización o el conocimiento del usuario del equipo. Los zombis se utilizan de manera frecuente para realizar ataques de denegación de servicio (DDOS), un término que hace referencia a la saturación organizada de sitios web debido a la afluencia de un gran número de equipos al mismo tiempo. El gran número de usuarios que realizan peticiones simultáneas al servidor que aloja una página concreta tiene por objeto provocar un bloqueo y evitar que los usuarios legítimos puedan acceder". Definición disponible en: https://www.pandasecurity.com/es/security-info/zombie/.

sus propietarios; poner los *botnets* fuera de servicio durante una operación de hack-back podría afectar los derechos de las partes inocentes.

2.1.b.7. Riesgos para la inteligencia y la lucha contra el crimen.

Las técnicas de hack-back pueden afectar algunas áreas de actividad del Estado. Las acciones individuales de un actor privado contra un pirata informático podrían, por ejemplo, poner en peligro las operaciones realizadas contra el mismo objetivo por los agentes de inteligencia del Estado. Del mismo modo, las acciones de hack-back diseñadas para borrar los datos robados por el pirata informático podrían destruir la evidencia necesaria para el enjuiciamiento y, por lo tanto, obstaculizar las actividades de las autoridades judiciales. Peor aún, la represión podría convertirse en una excusa fácil para los ciberdelincuentes para justificar los actos maliciosos cometidos.[204] Hoy, la prohibición de todas las actividades de piratería por parte de los sistemas legales nacionales permite una distinción clara entre las víctimas y los autores de un ciberataque.

Autorizar el hack-back significaría que esta distinción se difumina: los autores de un ataque cibernético indudablemente pretenderían, en adelante, que no hicieron nada más que responder a los ataques iniciales, prevenir ataques, proteger a las víctimas, reunir pruebas o establecer atribuciones. En consecuencia, la lucha contra el cibercrimen se volvería más compleja.

2.1.b.8. Riesgos de una defensa cibernética activa elitista

Este último riesgo es común para todas las empresas pequeñas porque en el ciberespacio existe una tremenda desigualdad entre los actores[205]. Al mismo tiempo que los grandes actores poseen la gran parte de la tecnología digital, los pequeños no tienen los recursos financieros para adquirir herramientas eficaces de defensa cibernética o los recursos humanos calificados para usarlos. Como resultado, una pequeña proporción de empresas tendría la capacidad técnica y las habilidades para responder a los ataques cibernéticos de manera efectiva y relativamente segura[206]. Asimismo, una autorización general para la represión podría conducir a prácticas similares a las de la mafia por parte de jugadores de ciberseguridad sin escrúpulos que lanzarían ataques contra las empresas sin herramientas activas de defensa cibernética para venderles su "*protección*". Por

[204] Segal, A. (2016) idem.
[205] Messerschmidt, J. E. (2005) idem.
[206] Dinstein, Y. (2011) idem.

último, pero no menos importante, la represión podría convertirse fácilmente en un pretexto para legitimar el ciber espionaje industrial o dañar a los competidores.

2.1.b.9. Riesgos de un "backlash" (reacción violenta)

Las empresas que ejercen hack-back podrían enfrentarse a una llamada "reacción violenta". Si gigantes como Google o Microsoft tienen indudablemente poco que temer, las empresas pequeñas o medianas, que se dedican a contraataques contra hackers poderosos (vinculados, por ejemplo, a una agencia estatal), podrían ser aplastados por el hacker contra ofensivo. La mejor manera de reaccionar es en cooperación de las autoridades de su propio estado[207].

2.1.b.10. Riesgo a producir un efecto disuasorio cuestionable

El supuesto efecto disuasorio del hack-back encuentra importantes limitaciones. Si bien el temor a una fuerte respuesta podría disuadir a los piratas informáticos aislados motivados por el deseo de afirmarse, probablemente no tendrá ningún efecto sobre los terroristas u otros actores con motivos ideológicos o hackers políticos en conexión con los intereses del Estado.

Las normas de derecho internacional conceden, como principio, derechos individuales a los actores no estatales, independientemente de si son individuos, minorías nacionales o empresas. Pero para la eficacidad de estos derechos es necesario que los Estados, los creadores del derecho internacional, los reconozcan y los regulan en los tratados internacionales u otras formas clásicas de formar el derecho internacional (en particular el derecho consuetudinario y los actos unilaterales de las organizaciones internacionales, invertidos por los Estados con un poder normativo). Aun cuando, un análisis del derecho internacional positivo muestra claramente que no existe un derecho de "hack-back" para los actores privados[208].

Por un lado, está claro que no hay reglas específicas elaboradas por los Estados para reconocer el derecho a aplicar medidas de seguridad cibernética ofensiva. Los pocos tratados internacionales que existen en este campo no contienen disposiciones que puedan interpretarse como favorable a la práctica del hack-back. Por el contrario, la idea principal es de conceder a los Estados la misión de combatir el delito cibernético.

---

[207] Ibidem.
[208] Segal, A. (2016) idem.

En cuanto a los instrumentos de soft law (ley blanda), como las normas aprobadas por el Grupo de Expertos Gubernamentales, están lejos de favorecer las acciones unilaterales de los actores no estatales, ya que exhortan a los Estados a *"garantizar que los actores no estatales no utilicen su territorio para comprometerse internacionalmente en hechos ilícitos usando la tecnología de la información y las comunicaciones"*[209]. Por otro lado, las reglas generales del derecho internacional que también se aplican a la seguridad cibernética no pueden interpretarse de ninguna manera como que confieren un derecho de hack-back a los actores no estatales. Las contramedidas ante un ataque informático solo pueden ser adoptadas por los Estados lesionados contra otros Estados en las estrictas condiciones ya analizadas[210].

Por esta razón, son los Estados los que, según la lógica del derecho internacional, tienen derecho a tomar medidas de seguridad ofensiva, mediante la adopción de contramedidas en respuesta al acto internacionalmente ilícito cometido por otro Estado que afectó sus derechos o los derechos de sus nacionales. Sobre la base del derecho internacional, los Estados tienen el derecho no solo de proteger su territorio y soberanía, sino también de ejercer su protección en favor de cualquier persona física o jurídica respecto de la cual tengan competencia, especialmente en el caso de sus nacionales.

Al respecto, los Estados tienen la capacidad de adoptar todas las medidas permitidas por el derecho internacional, incluidas las contramedidas. Este derecho no existe, en principio, para personas privadas. Según el jurista francés Denis Alland[211], *"desde la historia se puede rastrear que el derecho de represalia siempre ha sido un derecho público, un derecho soberano y real"*. Por supuesto, en ciertas circunstancias, los Estados podrían conceder expresamente a los actores privados la posibilidad de ejercer contramedidas, pero esto implica un acto expreso, bajo un control estricto por parte del Estado y el riesgo de que este último asuma su responsabilidad, ya que las reacciones adoptadas posteriormente serían consideradas como acciones del propio Estado.

Del mismo modo, es imposible que los actores privados confíen en la teoría de la "autodefensa" en el derecho internacional. A este respecto, cualquier posible confusión derivada del uso del término "defensa cibernética" (activa o pasiva) debe descartarse

---

[209] Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional (2015) *Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional A/70/174*, texto disponble en https://undocs.org/A/70/174.

[210] Segal, A (2016) idem.

[211] Alland, D. (1994) *Justice privée et ordre juridique international. Étude théorique des contre-mesures en droit international public*, Paris, Editorial Pedone, p. 316.

claramente. El concepto de autodefensa en el derecho internacional, codificado también por el artículo 51 de la Carta de las Naciones Unidas, se refiere a algo muy específico: un ataque armado cometido contra un Estado. La autodefensa, además, solo puede ser invocada por los Estados víctimas. Una persona, una empresa o un actor privado no puede, desde el punto de vista del derecho internacional, ser víctima de "ataque armado" o invocar el derecho de legítima defensa consagrado en el artículo 51 de la Carta. En los últimos años, se ha debatido a cerca de este problema del derecho internacional en cuanto a si, más allá de los Estados, los actores no estatales (y especialmente los grupos terroristas como Al-Qaeda o ISIS) también podrían cometer un ataque armado (y esto, a pesar de la posición tradicional de la Corte Internacional de Justicia, según la cual un ataque armado solo puede ser cometido por un Estado contra otro). Nunca se ha sugerido en la doctrina jurídica de derechos internacional que estos actores puedan ser víctimas de ataques armados, lo que les brinda la posibilidad de invocar la "*autodefensa*" para lanzar ataques contra otros Estados.

Los actores privados tampoco pueden invocar en su defensa otros mecanismos de autoprotección reconocidos por el derecho internacional, como el derecho de persecución. Este importante derecho está codificado en el Artículo 111 de la Convención de las Naciones Unidas sobre el Derecho del Mar de 1982 (Convención de Montego Bay)[212]. Según dicho Artículo, un Estado ribereño tiene el derecho, bajo ciertas condiciones, de emprender la búsqueda de un barco extranjero cuando tenga buenas razones para creer que este barco ha violado las leyes y reglamentos del Estado. Dicha búsqueda debe comenzar cuando el barco extranjero se encuentra dentro de las aguas internas, el mar territorial o la zona contigua del Estado perseguidor, y solo puede continuar fuera del mar territorial o la zona contigua si la búsqueda no ha sido interrumpida.

El derecho de persecución cesa tan pronto como el barco perseguido ingrese al mar territorial de su propio Estado o de un tercer Estado. Podemos ser tentados a

---

[212] *"Se podrá emprender la persecución de un buque extranjero cuando las autoridades competentes del Estado ribereño tengan motivos fundados para creer que el buque ha cometido una infracción de las leyes y reglamentos de ese Estado. La persecución habrá de empezar mientras el buque extranjero o una de sus lanchas se encuentre en las aguas interiores, en las aguas archipelágicas, en el mar territorial o en la zona contigua del Estado perseguidor, y sólo podrá continuar fuera del mar territorial o de la zona contigua a condición de no haberse interrumpido. No es necesario que el buque que dé la orden de detenerse a un buque extranjero que navegue por el mar territorial o por la zona contigua se encuentre también en el mar territorial o la zona contigua en el momento en que el buque interesado reciba dicha orden. Si el buque extranjero se encuentra en la zona contigua definida en el artículo 33, la persecución no podrá emprenderse más que por violación de los derechos para cuya protección fue creada dicha zona".*

inspirarnos de esta antigua regla del mar y considerar la idea de un "*derecho cibernético de persecución*"[213]. Pero al igual que el tradicional "derecho de persecución", una extensión al ciberespacio debería, en principio, reservarse solo a las autoridades estatales.

El artículo 111, apartado (5), de la Convención de Montego Bay, por ejemplo, enfatiza que *"el derecho de persecución sólo podrá ser ejercido por buques de guerra o aeronaves militares, o por otros buques o aeronaves que lleven signos claros y sean identificables como buques o aeronaves al servicio del gobierno y autorizados a tal fin"*.

Finalmente, los actores privados tampoco no pueden invocar la protección de los derechos humanos para ejercer sus propias medidas de represión. Si bien es cierto que algunos instrumentos legales internacionales relacionados con la protección de los derechos humanos (como el Convenio Europeo de Derechos Humanos) proclaman derechos importantes como el derecho a la vida o la protección de la propiedad privada, pero en ningún momento no otorga a las personas un derecho para "tomar la ley en sus propias manos" y usar la justicia vigilante para protegerse[214].

La lógica general de las convenciones internacionales para la protección de los derechos humanos es que los Estados deben actuar para garantizar estos derechos protegiendo a sus beneficiarios antes los ataques de los agentes estatales como de los actores privados, en caso de que el Estado conozca, o haya tenido conocimiento, que existe una amenaza grave (teoría de las obligaciones positivas). De hecho, es imposible borrar al Estado de la ecuación de acción, protección y reacción.

Al mismo tiempo tenemos que mencionar que los actores privados no pueden invocar ni el concepto de autodefensa previsto en la ley nacional para lanzar ataques transfronterizos con carácter defensivo. Más allá del hecho de que en muchos sistemas legales nacionales sería difícil invocar la "*autodefensa*" para responder a un ciberataque, esa posibilidad no cambiaría nada desde el punto de vista del derecho internacional. Es decir, si suponemos que el derecho de hack-back seria reconocido en algunos sistemas legales (que parece no ser el caso por el momento), de ninguna manera implicaría la existencia de tal derecho dentro del orden jurídico internacional, que es un orden jurídico distinto.

Como expresa la Comisión de Derecho Internacional de las Naciones Unidas: "*La caracterización de un acto de un Estado como internacionalmente ilícito se rige por*

[213] Alland, D. (1994) idem.
[214] Messerschmidt, J. E. (2005) idem.

el derecho internacional. Tal caracterización no se ve afectada por la caracterización del mismo acto como legal en el derecho interno".

2.2. La política de seguridad cibernética defensiva

Los Estados pueden ser considerados responsables de los actos de agentes privados en virtud de "*la obligación de todo Estado de no permitir, cuando es evidente, que su territorio sea utilizado para actos contrarios a los derechos de otros Estados*". Esta obligación se refiere directamente a la responsabilidad de los Estados por los actos de los particulares, independientemente de las relaciones entre ellos e independientemente de la naturaleza precisa de los actos de que se trate, ya sean ciberataques, técnicas de hack-back o cualquier otra actividad. Esta obligación genera un deber de "vigilancia", un "*due diligence*" que se deriva directamente de la soberanía de los Estados[215].

El concepto de "ciber-diligencia", que expresa este deber en el ciberespacio, puede desempeñar un papel importante en la construcción de la paz y la seguridad internacionales en la era digital. De hecho, indica un estándar de comportamiento razonable y responsable de los Estados para prevenir y poner fin a los ciberataques lanzados por actores privados desde su territorio contra el territorio o infraestructuras de otros Estados.

"*Qui peut et n'empêche, pèche"* (*El que puede y no previene, peca*). El dicho de Antoine Loysel[216], un abogado francés del siglo XVII, famoso por haber recogido las reglas consuetudinarias del Reino de Francia, refleja bien lo que expresa el concepto de ciber-diligencia en el siglo XXI hacia los Estados soberanos en el ciberespacio: intervenir, cuando sepan y puedan, para prevenir actos que vulneren los derechos de terceros Estados.

[215] Potter, Evan H. (2002) *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century*. McGill-Queen's University Press.
[216] Loisel, A. (2013) *Institutes coustumières, ou Manuel de plusieurs et diverses reigles: sentences & proverbes tant anciens que modernes du droict coustumier & plus ordinaire de la France*, Editorial Hachette Livre BNF.

2.2.1. La soberanía estatal es el punto clave del concepto de ciber-diligencia

En el ciberespacio, la responsabilidad de los Estados de intervenir, donde sea que puedan, se origina directamente en su soberanía sobre la infraestructura dentro de su territorio. Como señalaron los miembros del GEG en su Informe de 2015[217]:

> *"La soberanía de los Estados y las normas y principios internacionales que se derivan de la soberanía se aplican a la conducta de los Estados de actividades relacionadas con las TIC y a su jurisdicción sobre la infraestructura de TIC dentro de su territorio".*

Las normas y los principios que se derivan de la soberanía de los Estados se asocian de hecho con derechos en beneficio de los Estados, pero también, como corolario, con deberes para los Estados. Esta estrecha correlación entre los derechos y deberes de los Estados soberanos ha sido expresada de manera famosa por el Laudo Arbitral dictado en 1928 en el Caso Isla de Palmas[218]. Según él:

> *"La soberanía territorial [...] implica el derecho exclusivo a exhibir las actividades de un Estado. Este derecho tiene como corolario un deber: la obligación de proteger dentro del territorio los derechos de otros Estados, en particular su derecho a la integridad e inviolabilidad en paz y en guerra".*

Los Estados soberanos tienen derecho a que se respete su integridad territorial, pero también tienen el deber de no utilizar o permitir que su territorio sea utilizado de forma que se menoscabe la integridad territorial de otro Estado: "*sic utere tuo ut alienum*

---

[217] En 2013, el informe GEG subrayó que "La soberanía del Estado y las normas y principios internacionales que se derivan de la soberanía se aplican a la realización de actividades relacionadas con las TIC por parte del Estado y a su jurisdicción sobre la infraestructura de TIC dentro de su territorio", GEG 2013, A / 68/98, 24 de junio de 2013, parágrafo §20.

[218] Reports of International Arbitral Awards (1928*) Island of Palmas case (Netherlands, USA), VOLUME II pp. 829-871 - Palmas (Miangas) es una isla de escaso valor económico o ubicación estratégica. Se encuentra a 2,6 km de longitud norte-sur y 1,0 km de ancho este-oeste. Tenía una población de alrededor de 750 en 1932, cuando se decidió el caso. La isla está ubicada aproximadamente a 100 millas al este de la ciudad de General Santos, Filipinas y 400 millas al norte de las islas Talaud, la siguiente parte más al norte de Indonesia. En 898, España cedió Filipinas a Estados Unidos en el Tratado de París (1898) y Palmas se encuentra dentro de los límites de esa cesión. En 1906, Estados Unidos descubrió que Holanda también reclamaba la soberanía sobre la isla, y las dos partes acordaron someterse a un arbitraje vinculante por parte de la Corte Permanente de Arbitraje. El 23 de enero de 1925, los dos gobiernos firmaron un acuerdo a tal efecto. Las ratificaciones se intercambiaron en Washington, DC el 1 de abril de 1925. El acuerdo se registró en la Serie de Tratados de la Sociedad de Naciones el 19 de mayo de 1925. El árbitro del caso fue Max Huber, un abogado suizo. La pregunta que tenía ante sí el árbitro era si la isla de Palmas (Miangas) formaba parte del territorio de los Estados Unidos (refiriéndose a lo que ahora es Filipinas) o territorio holandés (refiriéndose a lo que ahora es Indonesia). El Árbitro de conformidad con el Artículo I del Acuerdo Especial de 23 de enero de 1925 decide que: la isla de Palmas (Miangas) forma en su totalidad una parte del territorio de los Países Bajos.*

non laedas". Como lo hace notar en el Laudo Arbitral de 1925[219] en la Zona Española de Marruecos reclama: *"la responsabilidad por hechos que puedan afectar el derecho internacional y que ocurran en un territorio determinado va de la mano con el derecho a ejercer, a la exclusión de otros Estados, las prerrogativas de soberanía"*.

El deber de utilizar el propio territorio de una manera que no pueda lesionar los derechos de los demás ha sido reiteradamente reafirmado por la jurisprudencia internacional, comenzando por la famosa sentencia de la Corte Internacional de Justicia en el asunto del Canal de Corfú, sobre "*la obligación de todo Estado de no permitir conscientemente que su territorio sea utilizado para actos contrarios a los derechos de otros Estados*".

En virtud de su soberanía, los Estados tienen la obligación de vigilancia, de due-diligence, respecto de las actividades que se desarrollen en su territorio o bajo su control y, en caso de incumplimiento de esta obligación, podrán, en determinadas condiciones, ser considerado responsable de las vulneraciones de los derechos de terceros Estados.

2.2.2. La responsabilidad de los Estados por los ataques transnacionales y los daños provocados a terceros Estados

En el caso del Canal de Corfu[220], la Corte Internacional de Justicia condenó a Albania por incumplir su deber de vigilancia, ya que las minas colocadas en sus aguas territoriales habían causado daños a los buques británicos. En el Fallo, la Corte no condenó a Albania por haber colocado las minas, sino que afirmó que Albania era responsable de los daños causados al Reino Unido en la medida en que, habiendo indudablemente tenido conocimiento de la existencia del campo minado, Albania no había tomado medidas razonables a su alcance para prevenir el incidente y el daño.

Esta obligación de vigilancia, que deriva de la soberanía de los Estados, es sin duda, vinculante para los Estados independientemente de la identidad de los autores de tales actividades. Al respecto, es importante resaltar que: históricamente, esta obligación de vigilancia se desarrolló primero en relación con la responsabilidad de los Estados por

---

[219] Document A/CN.4/169- *Digest of the decisions of international tribunals relating to State Responsibility*, *by the Secretariat,* Extract from the Yearbook of the International Law Commission:-1964,vol. II, disponible en: https://legal.un.org/ilc/documentation/english/a_cn4_169.pdf.

[220] *The Corfu Channel Case, United Kingdom of Great Britain and Northern Ireland v. the People's Republic of Albania* (1949) Judgement of 9th of April 1949, disponible en: http://www.icj-cij.org/docket/index.php?p1=3&p2=3&k=cd&case=1&code=cc&p3=4.

las actividades privadas. La primera aplicación conocida de esta obligación por la jurisprudencia internacional se refería a la responsabilidad de un Estado, el Reino Unido, por actos de empresas privadas. En el caso de Alabama[221], el Reino Unido fue condenado por violar su obligación de diligencia debida al permitir que empresas privadas construyeran y armaran, dentro de su territorio, el buque de Alabama que iba a servir en el ejército confederado contra la Unión durante la guerra de secesión en el Estados Unidos.

Desde entonces, el principio de la diligencia debida ha sido aplicado por la jurisprudencia internacional en relación con muy diversas actividades y en muy diversos campos, como: el derecho del mar, los derechos humanos, la protección del medio ambiente y la protección de las personas, del personal diplomático y de los estados extranjeros contra insurgencias y ataques transfronterizos de grupos no estatales. Es el caso relativo a las actividades armadas en el territorio del Congo entre la República Democrática del Congo y Uganda, este último afirmó, sobre la base del fallo del Canal de Corfú, que la República Democrática del Congo había violado su obligación de debida diligencia al no impedir que los grupos armados lanzaran ataques contra Uganda desde el territorio de la República Democrática del Congo.

Aunque la Corte Internacional de Justicia[222] finalmente se negó a considerar que la incapacidad de la República Democrática del Congo para poner fin a estos ataques constituía, en las circunstancias fácticas de ese caso, un incumplimiento de su obligación de due-diligence admitió, al igual que la República Democrática del Congo, que tal obligación existía para los Estados en el contexto de los ataques transfronterizos por parte de los agentes no estatales.

---

[221] Reports of International Arbitral Awards (1972) Alabama claims of the United States of America against Great Britain Award rendered on 14 September 1872 by the tribunal of arbitration established by Article I of the Treaty of Washington of 8 May 1871, disponible en: https://legal.un.org/riaa/cases/vol_XXIX/125-134.pdf,

[222] El 19 de diciembre de 2005, la Corte dictó su fallo en la causa relativa a las *Actividades armadas en el territorio del Congo* (República Democrática del Congo contra Uganda). La Corte, por unanimidad, agregó que "en lo sucesivo ambas partes han de adoptar todas las medidas necesarias para cumplir todas sus obligaciones con arreglo al derecho internacional, particularmente las que les corresponden de conformidad con la Carta de las Naciones Unidas y la Carta de la Organización de la Unidad Africana y la resolución 1304 (2000) del Consejo de Seguridad de las Naciones Unidas, de 16 de junio de 2000". Por último, la Corte señaló por unanimidad que "ambas partes han de adoptar sin demora todas las medidas necesarias para garantizar el pleno respeto, dentro de la zona de conflicto, de los derechos humanos fundamentales y de las disposiciones aplicables del derecho humanitario".

2.2.3. La utilidad del concepto de ciber diligencia en la política internacional de prevención de los ciberataques

La obligación de no permitir que el territorio de uno sea utilizado para actos contrarios a los derechos de otros Estados es vinculante para los Estados, sin importar solo la actividad del autor, sino también de la naturaleza precisa del acto en cuestión. Tal acto puede consistir en una actividad física o digital, puede ser de alta o baja tecnología.

En el año 2001, la Comisión de Derecho Internacional[223] en su "*Proyecto de artículos sobre la prevención del daño transfronterizo resultante de las actividades peligrosas*", había insistido en que el deber de cuidado de los Estados con respecto a las llamadas actividades peligrosas era necesario para todas las actividades desde el momento en que implican un riesgo de causar un daño transfronterizo significativo. En su comentario al artículo 1[224], la Comisión explicó que se negó a elaborar una lista de tales actividades porque dicha lista quedaría inmediatamente desactualizada por las tecnologías rápidamente cambiantes. Las actividades desarrolladas en el ciberespacio no pueden evadirse de esta regla.

Con base en el Informe de 2015, el GEG[225], sin nombrar expresamente el concepto de ciber-diligencia, expresó esta idea en varios lugares. En particular, mencionó que los Estados "*deberían procurar que su territorio no sea utilizado por agentes no estatales para cometer tales actos*" y que "*no deberían permitir conscientemente que su territorio sea utilizado para actos internacionalmente ilícitos utilizando las TIC*".

Por ende, la cuestión no es si los Estados tienen la obligación de no permitir a sabiendas que agentes privados utilicen su territorio e infraestructuras para lanzar ciberataques contra otros Estados, ya que está claro que esa obligación existe. Más bien, la pregunta es: hasta qué punto y de qué manera se puede imponer esta obligación a los Estados en el ciberespacio, y cuándo podríamos considerar que un Estado "sabía" y "podía" pero no hizo nada para evitarlo.

---

[223] International Law Commission (ILC) (2001) *Draft Articles on Prevention of Transboundary Harm from Hazardous Activities*, disponible en: https://link.springer.com/chapter/10.1007%2F978-1-4020-8367-9_23,

[224] *Article I (Scope) The present articles apply to activities not prohibited by international law which involve a risk of causing significant transboundary harm through their physical consequences.*

[225] Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional (2015) *Informe A/70/174 del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional*, 22 de Julio 2015, disponible en: https://undocs.org/es/A/70/174.

2.2.4. Ciber-diligencia – norma internacional de conducta responsable y razonable

El estándar de due-diligence (diligencia debida) en relación con el deber de utilizar el territorio de una manera que no lesione el derecho de otros Estados designa una obligación de medios y no una obligación de resultado. Esta es una característica fundamental de esta obligación que se acepta unánimemente y que nunca ha sido cuestionada. Requiere que los Estados estén razonablemente vigilantes con respecto a las actividades que se desarrollan dentro de sus territorios, de acuerdo con sus respectivas capacidades.

- ***El carácter de la obligación de ciber-diligencia es de medios y no de resultado***

El ejercicio de la soberanía territorial por parte de los Estados no significa que necesariamente deban estar al tanto de todo lo que ocurre dentro de su territorio, o que estén en condiciones de poder prevenirlo todo. El grado de vigilancia esperado es el de "un buen Gobierno[226]". Todos los juzgados, tribunales y otros órganos internacionales que han tenido que interpretar y aplicar el principio de due-diligence abogan por la teoría de que la prueba de "razonabilidad" debe orientar su aplicación y no imponer una carga imposible o desproporcionada a las autoridades. Esto significa que no se puede presumir que un Estado conoce la existencia de un ciberataque lanzado por particulares desde su territorio contra un tercer Estado.

Como reiteró la Corte Internacional de Justicia en el caso del Canal de Corfú, "*del mero hecho del control ejercido por un Estado sobre su territorio y sus aguas no se puede concluir que ese Estado necesariamente conocía, o debió haber sabido, de cualquier acto ilícito perpetrado en el mismo, ni tampoco que necesariamente conocía, o debería haber conocido, a los autores"*[227].

Por otra parte, podemos decir que los Estados soberanos no pueden ignorar todo lo que ocurre en su territorio. Como lo señaló la Corte en el mismo caso, "*un Estado en cuyo territorio o en cuyas aguas se haya producido un hecho contrario al derecho internacional, puede ser llamado a dar una explicación. También es cierto que ese Estado no puede eludir tal solicitud limitándose a responder que desconoce las circunstancias del hecho y de sus autores. El Estado puede, hasta cierto punto, estar obligado a*

[226] Provost, R. (1992) *State Responsibility in International Law*, Londres: Editorial Routledge.
[227] *The Corfu Channel Case, United Kingdom of Great Britain and Northern Ireland v. the People's Republic of Albania* (1949), idem.

proporcionar detalles sobre el uso de los medios de información e investigación de que dispone"[228].

Un tema delicado, que es particularmente critico en el ciberespacio, es determinar en qué medida un Estado soberano "debe saber", "debería haber sabido" o "debería buscar saber", en particular mediante la vigilancia de las actividades que tienen lugar en su territorio. Este tema ha sido ya ampliamente analizado por la jurisprudencia internacional, particularmente en el campo de los derechos humanos, en el marco de las "obligaciones positivas"[229] de los Estados, o en el campo de la protección del medio ambiente.

Parece que los Estados deben ejercer un control sobre las actividades que se desarrollan en su territorio. No obstante, esto no significa que se les permita usar ese pretexto para desarrollar una vigilancia masiva y, por lo tanto, erosionar las libertades esenciales, comenzando por el derecho a la privacidad y la protección de datos y correspondencia.

Como subrayó la Corte Internacional de Justicia en el caso relativo a la aplicación de la Convención para la Prevención y la Sanción del Delito de Genocidio[230], "*es evidente que todo Estado solo puede actuar dentro de los límites permitidos por el derecho internacional*".

Al respecto, los miembros del GEG recordaron en su Informe de 2013 la necesidad de que los Estados respeten los derechos fundamentales de las personas: "Los esfuerzos estatales para abordar la seguridad de las TIC deben ir a mano con el respeto de los derechos humanos y las libertades fundamentales. establecidos en la Declaración Universal de Derechos Humanos y otros instrumentos internacionales".

---

[228] Ibidem.

[229] En el Caso de las Fábricas de Celulosa en el Río Uruguay (Argentina v. Uruguay), la Corte Internacional de Justicia consideró que la obligación de prevenir implicaba "*el ejercicio del control administrativo aplicable a los operadores públicos y privados, como el monitoreo de las actividades realizadas por dichos operadores, para salvaguardar los derechos de los demás ciudadanos*". Mas información sobre el caso en: https://www.icj-cij.org/en/case/135/judgments

[230] La Convención para la Prevención y la Sanción del Delito de Genocidio es un documento de Naciones Unidas aprobado en 1948. Su principal impulsor fue el jurista polaco Raphael Lemkin que fue el primero en utilizar y definir el delito de genocidio en un libro publicado en 1946 en el que denunció los crímenes nazis cometidos en la Europa ocupada. La Convención fue adoptada por la resolución 260 de la Asamblea General del 9 de diciembre de 1948. Entró en vigor el 12 de enero de 1951. la convención reconoce el genocidio como un delito perseguible por el derecho internacional. Fue firmado por 41 países, es ratificada por 133. Los últimos países en unirse al tratado han sido Yugoslavia, el 12 de marzo de 2001, y Guinea y Suiza, el 7 de septiembre del 2000. El texto de la convención es disponible en: https://www.icrc.org/es/doc/resources/documents/misc/treaty-1948-conv-genocide-5tdm6h.htm.

En 2015, los miembros del GEG volvieron a esta cuestión fundamental haciendo hincapié en la "importancia central" del respeto de los derechos humanos y las libertades fundamentales por parte de los Estados, así como en el hecho de que "*los Estados, al garantizar el uso seguro de las TIC, deben respetar los derechos humanos Las resoluciones 20/8 y 26/13 del Consejo de Derechos Humanos sobre la promoción, protección y disfrute de los derechos humanos en Internet, así como las resoluciones 68/167 y 69/166 de la Asamblea General sobre el derecho a la privacidad en la era digital, para garantizar el pleno respeto de los derechos humanos, incluido el derecho a la libertad de expresión"*[231].

En la base del criterio de razonabilidad no se evalúa en qué medida los Estados conocen o deben conocer las actividades que se desarrollan en su territorio, sino que también se determina si un Estado ha realizado los "mejores esfuerzos" a su alcance para prevenir o impedir la vulneración de los derechos de un tercer Estado. El hecho de que un Estado finalmente falle y, en consecuencia, no logre prevenir tal infracción no constituye en sí mismo un incumplimiento del deber de diligencia.

Como señaló la Corte Internacional de Justicia en el caso relativo a la aplicación de la Convención para la Prevención y la Sanción del Delito de Genocidio, "*un Estado no puede considerase responsable simplemente porque no se logra el resultado deseado*". Sin embargo, incurre la responsabilidad si es evidente que el Estado no tomó todas las medidas que estaban a su alcance y que podrían haber contribuido a prevenir el genocidio. En este ámbito, la noción de *diligencia debida* requiere una evaluación que es de vital importancia[232].

Dada la complejidad del ciberespacio, el despliegue instantáneo y los efectos de los ciberataques, el estándar de diligencia debida obviamente no requiere que los Estados prevengan todos los ciberataques. Pero resulta necesaria una evaluación de las circunstancias y las capacidades de cada uno es en cada caso particular, entre otras cosas.

- ***La responsabilidad común pero diferenciada***

En la práctica, existen varios criterios que pueden determinar la capacidad de un Estado para cumplir con sus obligaciones de diligencia debida en el ciberespacio. Estos

[231] Consejo de Derechos Humanos (2016) *Promoción, protección y disfrute de los derechos humanos en Internet.* Recuperado de: https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_32_L20.pdf
[232] Sivakumaran, S. (2007) *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (Bosnia and Herzegovina v Serbia and Montenegro), en *The International and Comparative Law Quarterly,* Vol. 56, No. 3, pp. 695-708.

criterios se refieren tanto a las circunstancias de cada caso como también de la capacidad de cada Estado que, como reconoce la jurisprudencia internacional, "*varía mucho de un Estado a otro"*[233]. En su trabajo sobre la prevención del daño transfronterizo, la Comisión de Derecho Internacional enfatizó que: "*El nivel económico de los Estados es uno de los factores a tener en cuenta para determinar si un Estado ha cumplido con su obligación de diligencia debida*"[234].

Junto a este criterio económico, en el ciberespacio, la obligación de los Estados de tomar todas las medidas razonables también debe evaluarse de acuerdo con el nivel y las capacidades tecnológicas de cada uno. No todos los Estados tienen la misma capacidad para proteger sus redes informáticas del uso malintencionado. El concepto de ciber diligencia implica, por tanto, el principio de responsabilidad común pero diferenciada entre Estados. Esta responsabilidad se diferencia porque los Estados son desiguales a nivel económico y tecnológico, pero también es común ya que debido a la interconexión que caracteriza al mundo digital, las vulnerabilidades de las infraestructuras esenciales de un Estado pueden tener graves consecuencias en otros. Como señaló el GEG en 2013: "*Los diferentes niveles de capacidad para la seguridad de las TIC entre diferentes Estados pueden incrementar la vulnerabilidad en un mundo interconectado"*[235].

No obstante, conviene recordar que, cualesquiera que sean estas desigualdades, los Estados no pueden desvincularse por completo de sus deberes soberanos. Como ha resaltado la Comisión de Derecho Internacional, se espera vigilancia, empleo de infraestructura y monitoreo de las actividades peligrosas en el territorio de cada Estado, porque esto representa un atributo natural de cualquier Gobierno.

• El deber de prevenir y responder a los ciberataques

En el caso relativo al personal diplomático y consular de los Estados Unidos en Teherán[236], la Corte Internacional de Justicia declaró la responsabilidad internacional de Irán para la detención del personal diplomático y consular como rehenes de los militantes, debido al hecho de que las autoridades iraníes no habían tomado ninguna medida para prevenir o reaccionar ante este acto. Según la Corte:

---

[233] Moore, J. B. (1898) *History and digest of the international arbitrations to which the United States has been a party*, Washington: Gov't Print Off.
[234] International Law Commission (2001)*"Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries",* Yearbook of the International Law Commission, vol. II, Segunda Parte, recuperado de: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.
[235] Grupo de Expertos Gubernamentales (2015) idem.
[236] United States Diplomatic and Consular Staff in Tehran, Judgment, 1. C. J. Reports 1980, p. 3.

"*El estado iraní – que, en su calidad de Estado ante el que estaba acreditada la misión, estaba obligado a tomar las medidas apropiadas para proteger la Embajada de los Estados Unidos – no hizo nada para prevenir el ataque, detenerlo antes de que se completara u obligar a los militantes a retirase de los locales y liberar a los rehenes. esta inacción contrastaba con el comportamiento de las autoridades iraníes en varias ocasiones similares, ocurridas en el mismo periodo, en las que han tomado las medidas apropiadas*".

Interpretando la jurisprudencia presentada, para establecer la responsabilidad, resulta necesario examinar las medidas concretas que los Estados deberían o podrían tomar razonablemente para prevenir el uso de sus infraestructuras digitales por parte de personas privadas para lanzar ciberataques y reaccionar ante estos ataques[237].

En el ciberespacio, cabe preguntarse si esta obligación preventiva debe determinar a los Estados a tomar medidas legislativas y técnicas concretas para evitar el uso malicioso, no autorizado, de sus infraestructuras digitales por parte de particulares contra otros Estados[238].

Podemos afirmar que la obligación de prevención es una obligación de medios que varía según la capacidad de cada Estado. Al respecto, se puede considerar que la capacidad de legislar para prohibir el uso malicioso de la infraestructura digital es una capacidad común para todos los Estados soberanos. Por otro lado, como ya hemos señalado, las capacidades técnicas varían mucho entre los Estados. Para prevenir eficazmente el uso malintencionado, probablemente sea necesario desarrollar una estrecha cooperación técnica entre los Estados. La participación del sector privado es esencial a este respecto, ya que muchas infraestructuras digitales en todo el mundo son privadas.

A la luz de la jurisprudencia y el trabajo realizado en diferentes foros y organismos internacionales, parece que un Estado que manifiestamente está fallando y no protege sus infraestructuras digitales, permitiendo que actores privados las utilicen para lanzar ciberataques contra otros Estados, puede ser considerado responsable por los resultados negativos. Como señaló la Corte Internacional de Justicia en un caso relativo

[237] Lotrionte, C. (2012) *Cyber Operations: Conflict Under International Law*. Georgetown Journal of International Affairs, pp. 15-24. Recuperado de: http://www.jstor.org/stable/43134334

[238] Innerarity, D. (2013) *Un mundo de todos y de nadie. Piratas, riesgos y redes en el nuevo desorden global*. Editorial Espasa Libros Barcelona, p. 15.

a la aplicación de la Convención para la Prevención y la Sanción del Delito de Genocidio, es una violación por omisión de la obligación de prevenir los resultados:

> "*[…] la obligación del Estado de prevenir y el correspondiente deber de actuar surgen en el instante en que el Estado tiene conocimiento, o normalmente debería haber conocido, la existencia de un riesgo grave de que se cometa un genocidio. A partir de ese momento, si el Estado tiene a su disposición medios que puedan tener un efecto disuasorio sobre las personas sospechadas de preparar un genocidio, o razonablemente sospechadas de albergar una intención específica (dolus specialis), tiene el deber de hacer uso de estos medios, según lo permitan las circunstancias"*[239].

Sin embargo, una cuestión delicada se refiere a las obligaciones de los Estados con respecto al desarrollo y la adquisición por parte de agentes privados de armas cibernéticas o técnicas ciber ofensivas que podrían utilizarse para realizar ciberataques transfronterizos.

A veces, la adquisición por parte de algunos actores privados de técnicas destinadas a lanzar ciberataques puede constituir un riesgo suficientemente grave, de tal impacto que se impone a los Estados adoptar medidas para actuar y prevenir. El tema es particularmente sensible, dado que las técnicas utilizadas para realizar ciberataques pueden ser las mismas que las desarrolladas para proteger y defender los sistemas informáticos, en última instancia puede depender de su uso[240]. La cuestión de la comercialización de los denominados bienes y tecnologías de doble uso se analiza ampliamente en El Arreglo de Wassenaar sobre control de Exportaciones de Armas Convencionales y bienes y tecnología de Doble Uso[241].

---

[239] *Case concerning the application of the Convention on the Prevention and Punishment of the Crime of Genocide, Bosnia Herzegovina v. Serbia and Montenegro, Judgment of 26 February 2007, ICJ Reports 2007, §431.*

[240] Schmitt, M.N. (2012) *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*. Harvard International Law Journal, vol. 54

[241] El Arreglo de Wassenaar (WA) es el primer acuerdo global multilateral sobre control de exportaciones de armas convencionales y bienes y tecnología de doble uso firmado en 1996. El acuerdo fue elaborado para promover la transparencia, el intercambio de buenas prácticas e información y mayor responsabilidad en la transferencia de armas convencionales y productos y tecnología de doble uso, para evitar una acumulación desestabilizadora de estos materiales. La adopción de este acuerdo representa un paso importante para los esfuerzos internacionales de mejorar la cooperación y prevenir la adquisición de armamento y bienes sensibles de doble uso que puedan ser usados a nivel militar, si la situación en una región es, o se convierte, en una causa de preocupación para los Estados Participantes. El acuerdo no impide las exportaciones de buena fe y cada estado firmante puede autorizar libremente las exportaciones de bienes y tecnología si no representan un riesgo para los demás miembros. la principal obligación de los estados miembros es de cooperar e informarse recíprocamente sobre las transferencias de los productos mencionados en las listas comunes.

A pesar del interés que presenta, El Arreglo de Wassenaar sigue siendo un instrumento jurídicamente no vinculante. Sin embargo, la evolución en los últimos años del comercio de vulnerabilidades de día cero[242] (es decir, vulnerabilidades no corregidas) impone, sin duda, un análisis exhaustivo desde el punto de vista del derecho internacional. Sería importante analizar en qué medida el comercio por parte de actores privados de vulnerabilidades de día cero podría considerarse constitutivo de riesgos graves de ciberataques, en cuyo caso los Estados, de acuerdo con su deber de vigilancia, deberían actuar regulando o incluso prohibiendo su comercialización y proliferación[243].

La jurisprudencia internacional ha establecido que los Estados de origen tienen la obligación de notificar a los Estados afectados por actividades nocivas que se desarrollan en sus territorios. Esta obligación de notificación ha sido claramente afirmada por la Corte Internacional de Justicia en el caso del Canal de Corfú como un principio general del derecho internacional.

Esto significa que, en el ciberespacio, los Estados que saben que los ciberataques se lanzan desde su territorio y sus infraestructuras contra otros Estados deben informar a estos últimos sin demora. En este sentido, se impone el desarrollo de un procedimiento de notificación y cooperación internacionales donde los CERTs (*Computer Emergency Response Team*) o los CSIRTs (*Computer Security Incident Response Team*) podrían desempeñar un papel fundamental en el cumplimiento de esta obligación. Dicha cooperación también podría facilitar la notificación por parte de los Estados víctimas de ciberataques hacia los Estados de los que emanaron estos ciberataques, con el fin de garantizar que los Estados de origen conozcan la situación y puedan, por tanto, tomar las medidas necesarias para detener estos ataques y o prevenir los nuevos ciberataques[244].

La obligación de cesación del acto ilícito que incumbe a los Estados es una obligación clásica del derecho internacional que ha sido reiteradamente recordada por la

---

[242] Según los expertos informáticos, "*una vulnerabilidad de día cero es un agujero o falla en un programa de software para el cual no hay un parche o una solución, generalmente porque el proveedor de software desconoce la vulnerabilidad. El término proviene del hecho de que los desarrolladores tienen cero días desde el momento en que se descubre que la falla protege contra un posible ataque cibernético. En algunos casos, un ataque en sí mismo es la primera indicación de que existe un problema de seguridad. Una vez que un proveedor de software descubre una vulnerabilidad de tipo 0 Day, los programadores se apresuran a corregir la falla y lanzan una actualización que contiene el parche necesario*". Si la vulnerabilidad es explotada por los delincuentes antes de que se pueda corregir, el ataque resultante se denomina "exploit" de día cero o ataque de día cero. Recuperado de: https://protecciondatos-lopd.com/empresas/ataques-dia-cero/.

[243] Fidler, M. (2015) *Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis*, I/S: A Journal of Law and Policy for the Information Society, Vol. 11, No. 2/2015, pp. 405-482.

[244] Stytz, M. R. y Bank, S. B. (2014) *Cyber Warfare Simulation to Prepare to Control Cyber Space*. National Cybersecurity Institute Journal, vol 1, nº2.

jurisprudencia internacional. Así, en su Informe de 2015, el GEG mencionó que "*los Estados deben responder a las solicitudes de asistencia adecuadas de otro Estado cuya infraestructura crítica esté sujeta a actos informáticos maliciosos. Los Estados también deben responder a las solicitudes apropiadas para mitigar la actividad maliciosa de las tecnologías de información y comunicación que emana de su territorio y está dirigida en contra de la infraestructura crítica de otro Estado, teniendo en cuenta el debido respeto por la soberanía"*[245].

Finalmente, junto con las medidas técnicas que podrían tomar los Estados para finiquitar estos ataques, también deben investigar y buscar identificar, enjuiciar y condenar a los autores de los ataques. En el caso del Canal de Corfú, la Corte criticó a Albania diciendo que mientras que el gobierno griego había nombrado inmediatamente una comisión para investigar los hechos del 22 de octubre, el gobierno albanés no ha tomado ninguna decisión de tal naturaleza, ni ha empezado una investigación judicial sobre el asunto.

La obligación de prevención constituye, una obligación de medios razonable, lo que significa que los Estados no pueden ser automáticamente responsables en caso de que no lo hagan. En todos los casos antes mencionados, la Corte asumió la responsabilidad internacional de un Estado sólo cuando consideró que el Estado en cuestión no había tomado todas las medidas razonables a su alcance para evitar daños, mientras tenía, o debería tener, conocimiento de los riesgos[246]. Como ya se mencionó, la obligación es proporcional a la capacidad de cada Estado. También es evidente que un fallo de un Estado, especialmente en la protección de su infraestructura digital, implicará su responsabilidad internacional solo si es realmente explotado por agentes no estatales para lanzar ciberataques[247].

Nuestro análisis de estos dos capítulos demostró que en caso de un ciberataque el derecho internacional ya incluye muchas reglas que pueden gobernar las relaciones entre los Estados y también entre los Estados y los actores privados. Se demostró la utilidad del concepto de ciber diligencia no solo para prevenir los ciberataques, sino también para actuar rápidamente y poner fin a ellos. El deber de diligencia debida que los Estados deben ejercer con respecto a los actores no estatales que operan desde su territorio

[245] Grupo de Expertos Gubernamentales (2015) idem.
[246] Ibidem.
[247] Kanuck, S. (2010) *Sovereign Discourse on Cyber Conflict Under International Law*. Texas Law Review, vol. 88, pp. 1571 y ss.

(ya sean grupos terroristas, delincuentes cibernéticos, empresas o simples piratas informáticos) deriva directamente de la obligación de cualquier Estado de "*no permitir que su territorio sea conscientemente utilizado para actos contrarios a los derechos de otros Estados*".

También se examinó el régimen legal aplicable a los ciberataques clasificando las posibles reacciones. se distinguió entre reacciones que siempre están permitidas y otras reacciones que están permitidas solo si se puede establecer que un Estado ha cometido un "*acto internacionalmente ilícito*" por acción u omisión. Destacamos la necesidad de cooperación internacional en esta área, comenzando con la notificación por parte del Estado víctima al Estado donde se originó el ciberataque, solicitando su intervención contra los autores de los actos maliciosos en cuestión.

También se advirtió contra cualquier trivialización de las respuestas que son, en principio, violaciones del derecho internacional pero que están "excusadas" como circunstancias que impiden la ilicitud o la responsabilidad. Esto se aplica tanto al "estado de necesidad", cuya invocación rara vez es aceptada en la práctica por las cortes y tribunales internacionales, como a las contramedidas. Estos últimos, sin duda, están autorizados por el derecho internacional como respuesta a un ciberataque que viola el derecho internacional y se le atribuye a un Estado, pero sigue en uso por falta de una mejor solución.

En diferentes áreas, los procesos de "justicia privada" han dado paso a procedimientos institucionales para la solución judicial de disputas y mecanismos de aplicación centralizados[248]. Si bien las contramedidas siguen siendo una importante solución para que los Estados (pero no para los actores privados) respondan a los ciberataques, cualquier trivialización o proliferación de estos procesos de justicia privada que impliquen riesgos para el orden internacional y, por definición, aprovechen al máximo potente, debe evitarse en la mayor medida posible.

Por último, se llevó a cabo un estudio detallado de los problemas de la "defensa cibernética activa" y la "represión" desde el punto de vista del derecho internacional. Se demostró los numerosos obstáculos y riesgos legales involucrados en una operación de hack-back iniciada unilateralmente por actores no estatales. Por lo cual, los actores privados estarían mejor invirtiendo en higiene cibernética y la implementación de buenas prácticas de seguridad, en lugar de tratar de adquirir herramientas ofensivas. Aunque, si

[248] Deibert, R. y Rohozinski, R. (2012) Contesting Cyberspace and the Coming Crisis of Authority, recuperado de: https://citizenlab.ca/cybernorms2012/DeibertRohozinski2011.pdf.

son víctimas de un ciberataque, en lugar de lanzar un hack-back peligroso, sería mejor si notificaran el ataque a las autoridades estatales y les pidieran que actuaran, y también ejercitaran sus derechos legales contra el autor del ciberataque, suponiendo que el autor pueda ser identificado.

Los Estados deberían actuar en el marco del derecho internacional (y especialmente del derecho de los derechos humanos) para mejorar sus capacidades proactivas y reactivas a fin de evitar dar la impresión de que las formas legales adecuadas de reacción son inexistentes o insuficientes. Los Estados podrían, si fuera necesario, depender de actores privados para llevar a cabo contraataques bajo ciertas circunstancias, pero esto debería hacerse bajo el atento control de las autoridades y existe el riesgo de desencadenar su responsabilidad internacional.

Apoyar que el derecho positivo brinde soluciones a diferentes problemas relacionados con la prevención de los ciberataques y las reacciones a los mismos, no significa de ninguna manera que los Estados deban retirarse. Como hemos visto a lo largo de este análisis, a medida que surgen nuevas preguntas, en el derecho internacional permanecen muchas áreas grises sobre cuestiones fundamentales. Por ende, es imperativo que la comunidad internacional coopere estrechamente para encontrar respuestas a estas preguntas utilizando todos los medios apropiados disponibles en virtud del derecho internacional[249] a la luz de las circunstancias: la adopción de nuevos instrumentos obligatorios; adopción de textos de soft law; una interpretación dinámica y evolutiva de las reglas existentes, etc.

Después de un período de relativa inacción, en los últimos años los Estados han estado explorando mucho más activamente el problema de la seguridad del mundo digital en general y el tema de los ciberataques, en particular. Negocian y cooperan en diferentes foros aumentando sus iniciativas en varias instituciones internacionales: organizaciones con vocación universal, principalmente la ONU y la Unión Internacional de Telecomunicaciones; u organizaciones regionales o cerradas, como la Unión Europea, el Consejo de Europa, la OSCE, la OCDE, la Unión Africana, la Organización de Cooperación de Shanghái, la OTAN, el G20 y más. El problema es que la proliferación de estas iniciativas en foros muy diversos no necesariamente refleja el buen gobierno de la seguridad cibernética. Algunos Estados han propuesto la creación de una nueva

[249] Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy, recuperado de: https://eeas.europa.eu/top_stories/pdf/eugs_review_web.pdf

organización internacional, única, centralizada especializada en ciberseguridad, como remedio para esta dispersión.

Aun cuando, internacionalmente es posible que la perspectiva común ya no se basa en la adopción de estructuras pesadas que nacen de las largas negociaciones de nuevos tratados constitutivos que probablemente nunca podrían ser ratificados por ciertos Estados. Tampoco parece que la nueva perspectiva se fundamenta en la creación de nuevas organizaciones internacionales con una vocación universal dotada de poderes normativos. Al contrario, hay un aumento en el número de "foros", "redes", "grupos", "agencias", "comités" y otras instituciones informales que quizás no corresponden a la definición clásica de una organización internacional, pero que realizan sus funciones de manera eficiente. Como destacó un autor: "*Las alternativas al derecho internacional se crean a través de diversas acciones coordinadas intergubernamentales que no implican la creación de organizaciones internacionales que son sujetos de derecho internacional*"[250].

Estas observaciones parecen ser particularmente relevantes en el área de la seguridad cibernética. Tal como están las cosas, es difícil ver cómo los Estados podrían participar en la creación de una organización internacional especializada en este campo.

También es difícil ver cómo podrían transferir a una institución internacional tales poderes en el campo de la seguridad cibernética, ampliamente percibida como perteneciente al dominio de la "seguridad nacional" y de la seguridad "humana" de sus poblaciones, en resumen, de sus funciones gubernamentales por excelencia.

Sin embargo, se siente la necesidad de una mejor cooperación y racionalización de las iniciativas, al igual que la necesidad de fortalecer las medidas de fomento de la confianza y asistencia para los muchos países que están rezagados en materia de ciberseguridad. Parece indispensable la creación de un organismo capaz de combinar estas acciones, monitorear los compromisos, pero también iniciar estudios o incluso brindar operatividad y promover buenas prácticas de seguridad junto con una cultura de higiene cibernética. Sin embargo, dicho organismo podría ser efectivo solo si fuera flexible, abierto y sin poderes normativos que pudieran aumentar los temores de muchos Estados.

Tal organismo debería, por supuesto, dar gran importancia a los actores privados al proporcionar una composición de múltiples partes interesadas o, al menos, la creación

[250] Benvenisti, E. (2006) *Substituting International Law*, en *The Move from Institutions?,* American Society of International Law Proceedings, Vol. 100/2006, p. 289-290.

de un mecanismo formal para la integración del sector privado, como una "Junta de Asociación Corporativa".

En este sentido, vale la pena recordar la reciente propuesta realizada por Microsoft[251] de crear un organismo tan informal agregando al G20 un ICT20 (formado por las veinte más grandes compañías de tecnología de la información y las comunicaciones):

> *"Una tercera opción podría ser aprovechar los marcos existentes, como el G20, y extenderlos a 20 proveedores líderes de TIC (ICT20). El G20 + ICT20 tendría la ventaja de ser de naturaleza global pero manejable en términos de tamaño. Un conjunto de normas aceptadas por todas estas partes interesadas podría representar una poderosa contribución a una primera carta de normas de ciberseguridad. También permitiría que las 20 economías más desarrolladas se responsabilicen a sí mismas y a otros de los comportamientos en el ciberespacio. El inconveniente de tal grupo es su falta de representación verdaderamente global y su contribución limitada de la sociedad civil. Sin embargo, la creación de un G20 + ICT20 y las 20 principales organizaciones no gubernamentales (NGO20) podría mejorar la colaboración y mejorar los resultados en las normas. No será fácil establecer criterios para la selección de ICT20 y NGO20, pero vale la pena el esfuerzo para abordar este desafío".*

Al mismo tiempo, podría ser más eficaz (y más coherente con la lógica interestatal del derecho internacional, especialmente en áreas que afectan directamente a la seguridad nacional de los Estados) crear en su lugar un organismo intergubernamental flexible que permita la participación de grandes empresas de TIC y de otras empresas, incluidas las Pymes. Dicha institución internacional de múltiples partes interesadas podría permitir a los gobiernos formular políticas y a las empresas trabajar juntos para encontrar soluciones efectivas a los muchos desafíos actuales y futuros de la seguridad cibernética.

[251] McKay, A., Neutze, J., Nicholas, P. y Sullivan K. (2015) *Microsoft. International Cybersecurity Norms. Reducing conflict in an Internet-dependent world.* Recuperado de: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVroA

CAPITULO III. La política europea en materia de ciberseguridad

3.1. Consideraciones previas

Ciudadanos, empresas y los gobiernos de la UE son beneficiarios del mundo digital interconectado que ofrece Internet, pero existe una conciencia cada vez mayor de las amenazas que conlleva dicha interconexión. En el campo de la ciberseguridad, la Unión Europea (UE) es un actor en escena relativamente nuevo. Si bien ha estado involucrada durante mucho tiempo en áreas de gobernanza y regulación de Internet, en cuestiones de ciberseguridad[252] la Unión ha sido más reactiva a los eventos y desarrollos, y todavía continua en el proceso de desarrollar una política de ciberseguridad coherente.

A medida que los desafíos de la ciberseguridad se vuelven más prominentes, la UE y los Estados miembros han tratado de ponerse al día fortaleciendo la resiliencia a las amenazas que emana del ciberespacio. Este capítulo examina esos pasos y evalúa hasta qué punto la Unión se ha convertido en un actor eficaz de la ciberseguridad. Si bien la UE ha dado pasos para abordar la ciberdelincuencia y mejorar la resiliencia de los sistemas de comunicación e información, la Unión solo está comenzando a desarrollar un papel en la ciberdefensa, un campo que se ha dejado en gran medida a los Estados miembros[253].

Uno de los principales instrumentos que contribuyen al logro de este objetivo es el Derecho comunitario, un sistema legal que resultó del proceso de integración no forzado, implementado a través de la asunción voluntaria por cada estado de los valores y principios de la Unión. La Unión Europea no puede considerarse un estado: es una construcción política original que reúne naciones seculares que simplemente quieren mantener su identidad, pero que también quieren trabajar juntas por la paz y la prosperidad de sus pueblos. Este sistema jurídico original no tiene por objeto la desaparición o la atenuación de las diferencias culturales, sino que permite el funcionamiento armonioso de los diferentes sistemas jurídicos, basándose en objetivos comunes.

---

[252] The Cybersecurity Strategy of the European Union. *An Open, Safe and Secure Cyberspace*, recuperado de: https://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.

[253] Sánchez de Rojas, E. (2010) *La ciberseguridad: retos, riesgos y amenazas*. Revista Ejército, 837: 136-143.

Nuestra comunidad es, sobre todo y especialmente una "comunidad de derecho". En este capítulo presentaremos también los principios sobre la aplicabilidad directa de los Reglamentos Europeos en el ordenamiento jurídico de los Estados miembros, desde la idea básica de la comunidad jurídica. Continuaremos con la identificación y explicación de las fuentes del derecho comunitario, seguidas por la presentación de los ámbitos de actividad en los que se requiere un enfoque integrado del marco reglamentario, de modo que se pueda evitar la fragmentación del mercado comunitario. La presentación de la evolución del marco legislativo comunitario en la materia de la ciberseguridad seguirá la línea cronológica de los actos normativos redactados e implementados por las instituciones europeas, un nuevo ámbito de interés para todos los agentes de la economía comunitaria que requiere la coordinación de las intenciones normativas bajo un único ente institucional: la Agencia de la Unión Europea para la Ciberseguridad (ENISA).

Para comprender el sistema legal europeo es necesario analizar el concepto de comunidad de derecho. Este término fue utilizado por primera vez por el profesor de derecho Walter Hallstein, uno de los padres fundadores de la Unión Europea. Según el primer presidente de la Comisión Europea, solamente un fortalecimiento de la legislación europea seguido por la importancia del papel del Parlamento y de la Comisión puede conducir a la creación de una Europa Unida. Por lo cual, esta expresión no es sólo una reiteración del principio rector de las democracias occidentales conocido como el *estado de derecho*, sino que representa la idea de un proyecto jurídico y político original y mucho más fascinante, una materialización de la esencia de la sociedad europea, tal como se desprende de la relación interestatal comunitaria de tipo Comunitas Orbis[254].

La idea de crear una comunidad que comparte los mismos objetivos económicos, sociales y políticos es un espejo detrás de cual se esconde la verdadera intención de esta construcción política: hacer de la Comunidad Europea un instrumento de paz en nuestro continente, sin precedentes en la historia, que sólo se podría lograr a través y en cumplimiento de la ley como único instrumento.

El sistema de derecho de la Comunidad Europea se basa en un conjunto de normas jurídicas organizadas y estructuradas jerárquicamente, con fuentes legislativas propias, protegido por órganos y procedimientos capaces de crear, interpretar e incluso

[254] Noción introducida por el filósofo español Francisco de Vitoria, considerado el padre del derecho internacional. En su trabajo "Una lección sobre los indios", habla de los principios de una ley natural que funciona en las relaciones entre las naciones.

tener facultades para sancionar el incumplimiento. Según el Tribunal de Justicia de las Comunidades Europeas:

> *"La Comunidad constituye un nuevo ordenamiento jurídico del derecho internacional, en favor del cual los estados han limitado sus derechos soberanos, aunque en un número limitado de ámbitos, y cuyas temas no son sólo los estados miembros, sino también sus residentes; que, por lo tanto, con independencia de las legislaciones de los estados miembros, el derecho comunitario no sólo crea obligaciones a los particulares, sino que también tiene por objeto conferir derechos comprendidos en su patrimonio jurídico"*[255].

El ordenamiento jurídico comunitario se caracteriza por el hecho de que los estados acordaron voluntariamente ejercer conjuntamente determinados derechos soberanos, renunciando al enfoque individualista y fragmentado. Sin embargo, no se trata de renunciar a la soberanía, tal como la definen y explican los filósofos del siglo XIX. Al referirse a la limitación de la soberanía, el Tribunal de Justicia de las Comunidades Europeas propone un nuevo concepto de la noción, presentándolo como un atributo divisible del estado, diferente conceptualmente desde el punto de vista de la división o limitación del territorio del estado y más cercano como sentido a una delegación parcial de las competencias estatales hacia la Comunidad Europea.

Este sistema jurídico se rige por el principio de distribución equilibrada de los poderes y se construye alrededor del principio de la aplicación directa y prioritaria de las normas de derecho comunitario en relación con las reglamentaciones internas proprias de cada estado. Los estados transfieren parte de su soberanía a las instituciones comunitarias, a las que confieren competencias legislativas. Dichas instituciones comunitarias constituyen la columna vertebral de la estructura jurídica comunitaria, actuando, en algunas situaciones, como verdaderos órganos constitucionales de la comunidad europea. Esta fue la brillante idea de Jean Monnet: "la creación gradual entre los europeos de un

[255] Sentencia del Tribunal de Justicia no. 5/1963 en el asunto 26/6 - Petición de decisión prejudicial con sentencia previa a base del artículo 177 del Tratado CEE presentada por la Tariefcommissie de Amsterdam el 16 de agosto de 1962 en la disputa entre Nv Algemene Transport- En Expeditie Onderneming Van Gend & Loos y Nederlandse Administratie der Belastingen (Administración Tributaria Holandesa), disponible en:https://curia.europa.eu/jcms/upload/docs/application/pdf/2009-05/tra-doc-ro-arret-c-0026-1962-200802142-05_00.pdf

amplio interés común, servido las instituciones democráticas comunes, a las que se delega la soberanía necesaria"[256].

Los Tratados de la Unión Europea concedieron la obligación de alcanzar los objetivos comunitarios a las cinco instituciones comunitarias [257] de fuerza, el principal motivo por lo cual fueron dotados de todas las facultades decisionales necesarias para materializar esta misión.

El surgimiento del Internet y de las nuevas tecnologías determinaron una reconfiguración de las prioridades legislativas europeas. La migración de la economía en el espacio electrónico, el número creciente de los usuarios de aplicaciones informáticas y de los miembros de comunidades virtuales causaron un mundo nuevo, un mundo virtual, sin fronteras, sin limitaciones en el espacio y el tiempo. Al ser un territorio recientemente conquistado por las personas, requiere reglas y sistemas de gobernanza, por lo que puede convertirse en una jungla digital donde los derechos individuales quedan sin protección. Desde esta perspectiva, la seguridad cibernética y la protección de los derechos fundamentales en el espacio virtual se convirtieron en los temas del momento para todos los actores involucrados en este proceso de digitalización de la vida cotidiana.[258].

Las nuevas nociones jurídicas que nacen de la transición a la economía digital mundial están esperando la realización de un consenso entre los juristas teóricos para conceptualizarse, definirse y explicarse al beneficiario final. La velocidad con la que los informáticos y los programadores están desarrollando territorios nuevos en el ciberespacio es tan acelerada que los teóricos del derecho apenas pueden mantenerse al día en sus esfuerzos por interpretar el derecho clásico y para adaptar las normas legales al entorno electrónico. Crear un ordenamiento jurídico virtual es el desafío del momento, y la integración del ordenamiento físico en el ciberespacio será sin duda uno de los mayores logros de la próxima generación de juristas, abogados y jueces[259].

---

[256] Monnet, J. (1978) *Memoirs*, Editorial Doubleday & Company, INC. Garden City, New York, recuperado de:https://archive.org/stream/MonnetJeanMemoirs/Monnet%2C%20Jean%20-%20Memoirs_djvu.txt.

[257] el Parlamento Europeo, el Consejo, la Comisión, el Tribunal de Justicia y el Tribunal de Cuentas.

[258] Sandru, D.M. (2019) *Răspunderea administratorului unei pagini găzduite de o rețea socială. Calitatea de operator în sensul reglementărilor privind protecția datelor* (La responsabilidad del administrador de una página alojada en una red social. La calidad del operador en el sentido de las normas de protección de datos), Revista Dreptul 07: 160-174. 2019.

[259] Pana, A (2020) Aplicarea regulamentelor europene în domeniul securității cibernetice. Rolul Agenției Uniunii Europene pentru securitate cibernetică *(La aplicacion de los reglamentos europeos en el ambito de*

3.2. Las fuentes del derecho europeo

La comunidad legal europea, además de estar basada en el estado de derecho (rule of law), debe al mismo tiempo estar estrictamente sujeta a sus principios. Estos principios fueron enmarcados por los fundadores de la Unión en las fuentes primarias de derecho. Las principales fuentes de derecho o la legislación primaria de la Unión Europea son los tratados.

El Tratado de Funcionamiento de la Unión Europea (TFUE) [260] y el Tratado de la Unión Europea (TUE) [261] son los tratados en los que se basa la Unión Europea. Estos dos tratados, que tienen el mismo valor jurídico, se encuentran en la literatura de especialidad bajo la denominación de "tratados". Estos definen la división de las competencias entre la Unión y los estados miembros y fundamentan el poder de las instituciones, estableciendo así el marco jurídico en el que las instituciones comunitarias implementan las políticas europeas.

Las normas de derecho contenidas en los tratados constitutivos de la Unión Europea están en la parte superior del ordenamiento jurídico comunitario y prevalecen sobre el resto del derecho comunitario, ya sean actos convencionales o actos unilaterales. La única excepción son los tratados celebrados por los estados miembros con terceros países antes de la entrada en vigor de los Tratados, pero de conformidad con las disposiciones del artículo 351 del TFUE. Además de los Tratados, se consideran fuentes principales de derecho comunitario también los Tratados de adhesión de los estados miembros a la Unión, los Tratados modificativos de la Unión Europea y los Protocolos anexos a los Tratados constitutivos y los Tratados de modificación.

Las fuentes secundarias del derecho comunitario están representadas por los actos unilaterales y los actos convencionales emitidos por las instituciones europeas. Según el artículo 288 TFUE, las instituciones comunitarias pueden adoptar "reglamentos, directivas, decisiones, recomendaciones y dictámenes. El reglamento tendrá un alcance general. Será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.La directiva obligará al Estado miembro destinatario en cuanto al resultado que

la seguridad cibernetila. El papel de la Agencia de Seguridad Cibernética de la Unión Europea). Revista Pandectele Romane no. 3/2020, Editorial Wolters Kluwer România, p. 71-88.

[260] El texto del Tratado está disponible en: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex:12012E/TXT

[261] El texto del Tratado está disponible en: https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0001.02/DOC_1&format=PDF

deba conseguirse, dejando, sin embargo, a las autoridades nacionales la elección de la forma y de los medios. La decisión será obligatoria en todos sus elementos. Cuando designe destinatarios, sólo será obligatoria para éstos. Las recomendaciones y los dictámenes no serán vinculantes". Estos actos enumerados en el artículo 288 son actos unilaterales. A estos se añaden otras normas, como las comunicaciones, las recomendaciones, los libros blancos y los libros verdes, a los que se hace referencia en la literatura jurídica como actos unilaterales atípicos.

Los actos convencionales se consideran acuerdos internacionales firmados entre la Unión Europea, por un lado, y un tercer país u organización, por el otro; los acuerdos celebrados entre las instituciones europeas o los acuerdos celebrados entre los estados miembros.

En la categoría de las fuentes de derecho complementarias están incluidas la jurisprudencia del Tribunal de Justicia de la Unión Europea, las normas del derecho internacional y los principios generales del derecho. Los principios del derecho internacional público son una fuente limitada de derecho comunitario y esto se debe a la naturaleza sui generis del Tratado según lo declarado por el Tribunal de Justicia de la Unión Europea: "El Tratado no se limita a la creación de obligaciones recíprocas solamente entre los sujetos cuyos se aplica, sino que establece un nuevo ordenamiento jurídico; [...] la economía del tratado presupone una prohibición para que los estados signatarios de hacerse justicia a sí mismos"[262]. En consecuencia, el Tribunal de Justicia se refiere sólo excepcionalmente a los principios del derecho internacional.

Además de los principios generales de derecho, el Tribunal declaró que "*el respeto de los derechos fundamentales es una parte integrante de los principios generales de derecho, cuya efectividad está garantizada por el Tribunal de Justicia [...] la protección de estos derechos, inspirada en las tradiciones constitucionales comunes de los estados miembros, debe garantizarse en el marco de la estructura y los objetivos de la Comunidad"* [263].

[262] Sentencia del Tribunal de 13 de noviembre de 1964, Comisión de la Comunidad Económica Europea contra el Gran Ducado de Luxemburgo y el Reino de Bélgica. Asuntos conexos 90/63 y 91/63. Disponible en https://eur-lex.europa.eu/legal-content/RO/ALL/?uri=CELEX:61963CJ0090

[263] Sentencia del Tribunal de Justicia de 17 de diciembre de 1970 - Internationale Handelsgesellschaft mbH contra Einfuhr- und Vorratsstelle für Getreide und Futtermittel, Asunto 11/70, disponible en http://ier.gov.ro/wp-content/uploads/rezumate-cjue/61970J0011.pdf.

Al mismo tiempo, debe tenerse en cuenta que todos los actos de derecho comunitario derivado están sujetos al principio de la legalidad, lo que significa que solo aquellos actos que fueron adoptados por la institución europea con la competencia legal para emitirlo se consideran válidos. Según lo dispuesto en el artículo 296 TFUE, los actos normativos emitidos por las instituciones europeas deben ser motivados, la fecha de su entrada en vigor es la de su publicación en el Diario Oficial de la Unión Europea o la fecha expresamente prevista en su contenido. Ellos siguen el mismo régimen de no retroactividad de la ley, derogación y nulidad similar al régimen previsto por nuestro derecho interno/nacional.

La Comisión Europea, como vigilante de los Tratados, tiene la tarea de garantizar que se respeten el cumplimiento, el desarrollo y la protección del marco jurídico comunitario, sin imponer una legislación excesiva o aumentar artificialmente los poderes delegados por los estados miembros a las instituciones comunitarias[264].

Naturalmente, la competencia legislativa atribuida a las instituciones europeas garantiza la vocación de la Unión de ser un creador de derechos en el beneficio de los ciudadanos europeos. El efecto directo de determinadas normas de derecho comunitario sobre los ciudadanos de cada estado miembro representa una demonstración de la opinión que los Tratados han introducido en el ordenamiento jurídico comunitario la concepción monista del derecho internacional. La construcción y el funcionamiento del sistema legal europeo representa un modelo único en el contexto jurídico nacional e internacional porque la norma jurídica comunitaria (como por ejemplo el reglamento) se aplica en el ordenamiento jurídico de los estados miembros directo e inmediatamente, sin la necesidad de transponerla o interpretarla mediante un acto reglamentario posterior.

Estas normas directamente aplicables produces efectos directos sobre sus destinatarios sin otra intervención estatal. La capacidad de directa efectividad aparece como una característica propria de la norma comunitaria que le confiere la posibilidad de crear por sí misma derechos y obligaciones para los particulares, ciudadanos europeos, derechos subjetivos reconocidos y protegidos automáticamente por los jueces y los tribunales nacionales de cada estado miembro[265].

---

[264] Weiler, J. H. H., (1985) *Il sistema comunitario europeo. Struttura giuridica e processo politico*, Editorial Il Mulino, Bolonia.
[265] Ibidem.

Por lo tanto, en el asunto C-106/77, relativo a una petición de decisión prejudicial ante el T.J.U.E. en virtud del artículo 177 del Tratado CEE, formulada por Pretore di Susa (Italia), en el litigio principal entre Amministrazione dalle Finanze dello Stato y Simmenthal SA, el Tribunal de Justicia dictó lo siguiente: "*dado que la aplicabilidad directa, analizada desde esta perspectiva, implica que las normas de derecho comunitario deben tener plenos efectos en todos los estados miembros, desde su entrada en vigor y a lo largo de su período de validez [...] estas disposiciones son una fuente inmediata de derechos y obligaciones para todos aquellos a quienes se dirigen, ya sean los estados miembros o las personas que son parte en relaciones jurídicas reguladas por el derecho comunitario [...] este efecto afecta también a cualquier órgano jurisdiccional que, como autoridad de un estado miembro, siendo presente en el marco de su competencia, tiene la misión de proteger los derechos conferidos a los particulares por el derecho comunitario"*[266].

Así, el Tribunal de Justicia de la Unión Europea subraya los efectos de la aplicabilidad inmediata y directa, lo que no sólo crea ventajas para los estados miembros, desde la perspectiva del principio de la aplicación uniforme del derecho comunitario, y, en particular, para las personas físicas. La pregunta que se plantea es la siguiente: ¿cuáles son los requisitos para que una norma comunitaria sea directamente aplicable? Según la jurisprudencia constante de la instancia, los requisitos necesarios para que una norma comunitaria sea directamente aplicable y tenga efectos inmediatos son: sus disposiciones están claramente redactadas, ser suficientemente precisa en la delimitación de su objeto específico, es decir, la imposición de una determinada obligación a un destinatario determinado que conduce, de manera conexa, a la creación de un derecho perfectamente identificable, ser una norma autosuficiente e incondicional (su aplicación no está sujeta a plazos ni reservas)[267].

La aplicabilidad y el efecto directo del derecho comunitario convierten al ciudadano europeo en un sujeto de derechos y obligaciones que pueden ser objeto de un procedimiento judicial: el ciudadano puede invocar las normas comunitarias contra cualquier disposición de derecho nacional que se oponga a sus derechos conferidos por

[266] La sentencia del Tribunal puede consultarse en: https://curia.europa.eu/jcms/upload/docs/application/pdf/2009-05/tra-doc-ro-arret-c-0106-1977-200802153-05_00.pdf

[267] Sandru, D.M.; Banu, C.M. y Calin, D. (2016) *Directiva - act de dreptul Uniunii Europene – si dreptul român,* Editura Universitara, Bucarest.

el derecho comunitario. Cuando existen reservas u opiniones divergentes en cuanto a la aplicabilidad directa de una norma de derecho comunitario, la instancia nacional puede plantear una cuestión previa al Tribunal de Justicia a este respecto[268].

La aplicabilidad directa y la invocación de determinadas disposiciones por parte de los ciudadanos no es más que la manifestación de una característica del derecho comunitario y del derecho en general: el principio de la eficacidad.

3.3. La política de seguridad cibernética en la Unión Europea

La ciberseguridad es un área relativamente nueva[269] que aún no se ha beneficiado de la regulación jurídica internacionalmente aceptada. Aunque en el contexto actual, la seguridad del mundo digital es una prioridad, definir el concepto representa un desafío tanto para el sector privado, como para las instituciones u organizaciones internacionales.

La Unión Europea ha incluido este tema entre sus prioridades. El Documento de reflexión sobre el futuro de la defensa europea[270] establece tres diferentes opciones para avanzar hacia una Unión de seguridad y defensa, ilustrando la importancia central de la ciberdefensa. En cada uno de los tres escenarios descritos en el documento (cooperación en seguridad y defensa, seguridad y defensa compartidas y defensa y seguridad comunes) se concibe la ciberdefensa como un área de mayor cooperación a través del apoyo a nivel de la UE, ya que las amenazas cibernéticas representan un factor de división entre las políticas internas y externas. En los debates dentro de los foros comunitarios, la ciberseguridad no se limita a la seguridad de las redes y los sistemas de información, sino que incluye cualquier actividad ilegal en el ciberespacio que implica el uso de las tecnologías digitales, desde ciberdelitos como el lanzamiento de ataques por virus informáticos, hasta al fraude por medios electrónicos de pago, sino también otros delitos relacionados más con el contenido digital que con los sistemas informáticos, como la

[268] Holland, M. (1995) *El fin del estado nacional: las relaciones institucionales de la Unión Europea*, Revista de Ciencias Políticas Polis No. 3/1995, p. 22-46.

[269] Según los datos proporcionados por la Organización del Tratado del Atlántico Norte, el primer ciberataque tuvo lugar en 1988: The Morris Worm. Este es el momento en que las instituciones con responsabilidades en el campo de la seguridad son conscientes de la necesidad de garantizar la seguridad del ciberespacio. La evolución de los ciberataques y sus efectos se pueden consultar en: (https://www.nato.int/docu/review/2013/Cyber/timeline/RO/index.htm)

[270] Comisión Europea (2017) *Documento de reflexión sobre el futuro de la defensa europea.* Recuperado de: https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_es.pdf

pornografía infantil. En la misma categoría se pueden incluir también las campañas online de desinformación o de influencia sobre la opinión pública y las campañas electorales[271].

El objetivo de la Comisión Europea es aumentar las capacidades de ciberseguridad y de cooperación, reforzar el papel de la Unión en la ciberseguridad e integrarla en todas las políticas de la UE. Las principales direcciones generales responsables de la política de ciberseguridad son la Dirección General de Redes de Comunicación, Contenido y Tecnología y la Dirección General de Migración y Asuntos de Interior, responsables del mercado único digital y de la seguridad comunitaria, respectivamente. La Dirección General de Informática es responsable de la seguridad de los sistemas informáticos de la Comisión[272].

Muchas agencias de la UE apoyan a la Comisión, en particular ENISA[273] (Agencia de Ciberseguridad de la Unión Europea): un órgano consultativo que apoya el desarrollo de las políticas de ciberseguridad, el fortalecimiento de la capacidad de defensa y la publicidad sobre los riesgos en el ciberespacio.

El Centro Europeo de Ciberdelincuencia de Europol (EC3) [274] se creó para reforzar la capacidad de la Unión para luchar contra la ciberdelincuencia y defender la libertad del Internet. La Comisión creó también un equipo de intervención en caso de emergencia (CERT-EU) [275], que apoya a todas las instituciones, todos los organismos y todas agencias de la UE. El Servicio Europeo de Acción Exterior (SEAE) está en la primera línea de la ciberdefensa, de la diplomacia cibernética y de la comunicación estratégica. La Agencia Europea de Defensa[276] (AED) tiene como objetivo desarrollar capacidades de defensa cibernética.

El Parlamento Europeo actúa como colegislador en el ámbito de la ciberseguridad. Las organizaciones del sector privado, como la industria digital, los órganos de gobernanza de Internet y las asociaciones académicas, se implican plenamente en el desarrollo y la aplicación de políticas, incluso a través de asociaciones públicas-

[271] Robinson, N. (2014) *EU cyber-defence: a work in progress. European Union*. Institute for Security Studies. Recuperado de: https://www.files.ethz.ch/isn/182329/Brief_10_Cyber_defence.pdf.
[272] La estructura organizativa y las tareas de las Direcciones Generales de la Comisión Europea se pueden encontrar en: https://ec.europa.eu/info/departments_es
[273]Consultar https://www.enisa.europa.eu/
[274] Consultar https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
[275] Consultar https://cert.europa.eu/cert/plainedition/en/cert_about.html
[276] Consultar https://europa.eu/european-union/about-eu/agencies/eda_ro#ce-face-aea?

privadas. Pero, los Estados miembros son los principales responsables de su propia ciberseguridad y, en el contexto europeo, actúan a través del Consejo, que cuenta con numerosos organismos de coordinación e intercambio de información.

La Estrategia de Ciberseguridad adoptada en el año 2013[277] representa la piedra angular de la política de la UE en este ámbito. El objetivo de la estrategia es "hacer que el entorno digital de la UE sea el más seguro del mundo, manteniendo al mismo tiempo valores y libertades fundamentales". Tiene cinco objetivos principales: "1) aumentar la resiliencia cibernética; 2) reducir la ciberdelincuencia; 3) desarrollar estrategias y capacidades de defensa cibernética; 4) el desarrollo de recursos tecnológicos e industriales de ciberseguridad; y 5) la creación de una política cibernética internacional en consonancia con los valores fundamentales de la UE".

Desde entonces, los esfuerzos de la Unión Europea para regular la seguridad cibernética se intensificaron, con la adopción de nuevas normas obligatorias para los Estados miembros, y el papel de la Agencia de Seguridad Cibernética de la Unión Europea incrementó cada vez más para garantizar una implementación e interpretación uniforme y eficaz de las normas comunitarias sobre la ciberseguridad.

A continuación, presentaremos una serie de puntos de referencia en la historia de la agencia y la evolución de la legislación comunitaria en el campo de la ciberseguridad para resaltar los esfuerzos de las instituciones europeas para uniformizar el marco regulatorio incidental en el campo de la estandarización y certificación de la ciberseguridad, una condición esencial para mantener la estabilidad del mercado comunitario.

3.4. La evolución del marco jurídico en el ámbito de la seguridad cibernética. El papel de la Agencia de Seguridad Cibernética de la Unión Europea (ENISA)

3.4.1. El marco regulatorio

La evolución de las regulaciones sobre la seguridad cibernética tuvo como primer punto de partida la necesidad de resolver los problemas de seguridad de las redes

[277] Comunicación Conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones (2013) *Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro*, disponible en:
https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52013JC0001

de comunicación, problemas que afectan algunos derechos fundamentales de los ciudadanos, así como la actividad de las organizaciones y empresas, incluso de las autoridades.

El segundo punto fue la necesidad de garantizar el funcionamiento de las economías de los Estados miembros, que se basan principalmente en la tecnología de la información, especialmente en sectores clave como la salud, la energía, las finanzas y el transporte[278].

La novedad del tema y la falta de una larga historia de regulación que conduzca a una legislación nacional específica en el campo (como en otras ramas del derecho) permitieron a la Unión Europea pensar en una estrategia de seguridad cibernética y un marco regulatorio uniforme para todos los estados miembros, capaz de garantizar a los usuarios un alto grado de ciberseguridad de las redes y de los sistemas informáticos, de los servicios y de los productos digitales utilizados.

Un paso importante en este campo ha sido la adopción del Marco político de ciberdefensa de la UE[279] por parte del Consejo el 18 de noviembre de 2014, actualizado en el año 2018. El documento fue desarrollado en la base de una propuesta del Alto Representante, en cooperación con la Comisión Europea y la Agencia Europea de Defensa (AED). El Marco político ilustra además la existencia de una serie de actores responsables en este campo, sobre todo los gobiernos y los ejércitos de los Estados miembros de la UE.

Para una gestión eficaz del problema, los foros europeos decidieron crear una agencia europea, especializada en la ciberseguridad (ENISA) [280], cuya principal función consiste en asesorar y coordinar las medidas adoptadas por la Comisión y los estados miembros para garantizar la seguridad de las redes y los sistemas de información.

A continuación, analizaremos brevemente el contexto y las etapas del proceso regulatorio de la Agencia de Seguridad Cibernética de la Unión Europea.

---

[278] Santa, I. (ENISA) (2012) *Informe "Synthesis of the results of the first European Cyber Security Month: BE AWARE. BE SECURE",* disponible en: https://www.enisa.europa.eu/publications/ecsm-results.
[279] El texto es disponible en: https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/es/pdf.
[280] El historial de la Agencia, su misión, sus objetivos y regulaciones específicas se pueden encontrar en el sitio web oficial https://www.enisa.europa.eu/.

3.4.1.1. Primera etapa – la adopción del Reglamento (CE) 460/2004 del Parlamento Europeo y del Consejo de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información[281]

La adopción de este primer reglamento, que sentó las bases de ENISA, fue generada, en el año 2000, por el reconocimiento de la necesidad de fortalecer la capacidad de los Estados miembros e implícitamente de la Comunidad Europea para contrarrestar las amenazas a la seguridad de las redes de información y de comunicación, para abordar y responder a los problemas planteados por los usuarios de las nuevas tecnologías de la información.

Por lo tanto, la Agencia recién creada representaba una institución de apoyo, que brindaba asesoramiento y apoyo a la Comisión Europea y a los estados miembros para resolver los problemas de ciberseguridad relacionados con las redes comunitarias de comunicación y transferencia de datos. La Agencia también tenía el papel de impulsar la cooperación entre actores públicos y privados para identificar y contrarrestar de manera oportuna los riesgos de comprometer la seguridad de las redes en el espacio comunitario[282].

Desde el momento de su creación, la Agencia tiene obligaciones de asegurar la transparencia sobre su actividad y personal, teniendo el deber de proporcionar al público o a cualquier parte interesada información objetiva, confiable y accesible sobre su trabajo y los resultados de su lucha contra las amenazas de seguridad cibernética. También se hicieron públicas todas las declaraciones patrimoniales y de intereses de los jefes de la Agencia, así como las del personal enviado por los estados miembros, de los expertos y de los miembros de grupos de trabajo permanentes o ad-hoc[283]..

[281] El texto del Reglamento es disponible en:
https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:02004R0460-20110625
[282] Garrós Font , I. (2019) *Avances y retos de la Agencia Europea para la Ciberseguridad. El nuevo marco de la certificación*. E.M. no. 62 mayo-agosto 2019.
[283] Ibidem.

3.4.1.2. Segunda etapa – adopción del Reglamento (UE) 526/2013 del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA) y por el que se deroga el Reglamento (CE) 460/2004 [284]

El Reglamento (UE) no. 526/2013 del Parlamento Europeo y del Consejo deroga el Reglamento de 2004 y reorganiza la Agencia Europea de Seguridad de las Redes de Información y Datos, renombrándola *Agencia de Seguridad de las Redes de la Información de la Unión Europea* (ENISA), denominación que todavía tiene. Con esta nueva regulación, el papel de la Agencia se fortalece y adquiere nuevas atribuciones en el desarrollo del campo de la seguridad cibernética en la Unión Europea, con mayor atención al sector de las pequeñas y medianas empresas, consideradas como principal motor económico del mercado común.

3.4.1.3. Tercera etapa – adopción de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión[285]

Conocida como Directiva NIS (*Network and Information Systems*), esta regulación comunitaria tiene como objetivo crear un marco regulatorio incluyendo medidas concretas capaces de garantizar la confianza en el uso seguro de las tecnologías de la información y de la comunicación con el fin de desarrollar las actividades económicas y comerciales de las empresas, respetando eficazmente los derechos fundamentales de los ciudadanos.

La Directiva NIS es el elemento esencial de la estrategia de ciberseguridad de la Unión Europea, que define por primera vez, el concepto del operador de servicios esenciales (en el artículo 4.4) como "*una entidad pública o privada de uno de los tipos que figuran en el anexo II, que reúna los criterios establecidos en el artículo 5, apartado 2*."

[284] El texto completo del Reglamento se puede encontrar en:
https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32013R0526
[285] El texto de la Directiva está disponible en:
https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32016L1148

En particular, la Directiva exige a los estados miembros que elaboren y adopten una estrategia nacional para la seguridad de las redes y sistemas de información, así como la designación de una autoridad nacional competente, puntos de contacto únicos y equipos de respuesta a incidentes de seguridad informática (CSIRT) para garantizar la seguridad de las redes y los sistemas de información.

A base de las disposiciones de la Directiva NIS, se creó un grupo estratégico de cooperación cuya misión es de apoyar y fomentar la cooperación estratégica y el intercambio de información entre los estados miembros. El objetivo final es de fortalecer la confianza en el entorno online y conseguir un alto nivel común de seguridad de las redes y de los sistemas de información en la Unión[286].

Una de las medidas más importantes implementadas tras la adopción de la Directiva NIS es de operacionalizar la red europea de equipos de respuesta a incidentes de seguridad informática (denominada la red CSIRTs), cuya misión es contribuir a fomentar la confianza entre los estados miembros y promover una cooperación operativa rápida y eficaz.

Entre los fundamentos del desarrollo de esta norma comunitaria encontramos también el esfuerzo para establecer una serie de criterios mínimos comunes a la hora de desarrollar capacidades operativas en el ámbito de la planificación, intercambio de información y cooperación. Al mismo tiempo se intenta establecer un conjunto de requisitos comunes de seguridad y notificación de incidentes que deben cumplir todos los operadores de servicios esenciales y proveedores de servicios digitales[287].

La integración jurídica comunitaria y la protección efectiva de los intereses generales de los consumidores europeos se puede lograr solo con la armonización y la uniformización de la legislación nacional de los estados miembros. El desarrollo económico, un comercio correcto, la confianza de las empresas y de los ciudadanos son principios europeos que sólo pueden alcanzarse promoviendo políticas y estrategias públicas eficaces en el ámbito de la ciberseguridad, destinadas a garantizar un marco regulatorio eficaz adaptable a un contexto económico en permanente transformación,

[286] Los resultados de los análisis y las propuestas realizados por los miembros del Grupo de Cooperación Estratégica de NIS están disponibles en: https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

[287] Martínez Martínez, R. (2016) *Directiva de ciberseguridad: un nuevo escenario jurídico y material*. Revista SIC: ciberseguridad, seguridad de la información y privacidad, Vol. 25, Nr. 121, p. 98-100

compatible con los esfuerzos de alcanzar el progreso económico y social del mercado interior[288].

El principal objetivo de la Directiva NIS fue de convencer a todos los estados miembros a desarrollar capacidades proprias y elaborar estrategias nacionales que garanticen un alto nivel de seguridad para las redes y los sistemas informáticos en sus territorios.

Debe señalarse que la Directiva ha establecido un nuevo régimen jurídico inédito en el ámbito de la seguridad de las redes y de los sistemas de información, en particular para los operadores de servicios esenciales[289] y para los proveedores de servicios digitales[290]. Desde esta perspectiva, podemos decir sin reservas que todos deben estar sujetos a los requisitos de seguridad y notificación de los incidentes para fomentar una cultura de gestión de riesgos y garantizar que se informen incidentes graves.

3.4.1.4 Cuarta etapa – elaboración del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) no. 526/2013 («Reglamento sobre la Ciberseguridad»), publicado en el Diario Oficial de la Unión Europea el 7 de junio de 2019 [291].

Las disposiciones del presente Reglamento entraron en vigor el 27 de junio de 2019, con excepción de los artículos 58, 60, 61, 63, 64 y 65, que entrarán en vigor a partir del 28 de junio de 2021. Los artículos 58, 60 y 61 se refieren a la obligación de los estados miembros de designar las autoridades nacionales de certificación de ciberseguridad y los organismos de evaluación de la conformidad y de notificar a la Comisión su designación. Los artículos 63 y 64 establecen el derecho de las personas físicas o jurídicas a presentar una reclamación ante la entidad que haya expedido un certificado europeo de ciberseguridad y a recurrir ante los tribunales si no están satisfechas con la manera de

[288] Ibidem.
[289] El "operador de servicios esenciales" es una entidad pública o privada del tipo enumerado en el anexo II que cumple los criterios establecidos en el artículo 5, apartado 2, y el artículo 4, apartado 4, de la Directiva NIS
[290] "Servicio digital" significa un servicio en el sentido del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo (*"servicio" significa cualquier servicio de la sociedad de la información, es decir, cualquier servicio normalmente a cambio de una remuneración, a distancia, por medios electrónicos y a solicitud individual del destinatario del servicio*), que es de un tipo que figura en el Anexo III - Artículo 4, punto 5 de la Directiva NIS.
[291] El texto completo del Reglamento está disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32019R0881

solución de la reclamación. El artículo 65 obliga a los estados miembros a establecer las normas sobre las sanciones que se aplican en caso de infracción de las disposiciones del Reglamento relativas a los sistemas europeos de certificación de la ciberseguridad y a adoptar todas las medidas necesarias para garantizar su aplicación.

La adopción del Reglamento (UE) 2019/881 (en lo sucesivo denominado el Reglamento) fue determinada por las necesidades normativas inmediatas en el ámbito de la normalización a nivel europeo, con el fin de crear normas claras y aceptadas por unanimidad por los estados miembros, incluso establecer un estándar único europeo en el ámbito de la ciberseguridad capaz de aumentar la resiliencia de las redes informáticas. Dado que el mercado único europeo no puede funcionar sin una interconexión digital segura entre los estados miembros y las empresas, este Reglamento es un primer paso para aumentar la seguridad y la protección de las conexiones digitales.

3.4.2. Las Funciones de la Agencia

El papel y las funciones de ENISA se reforzaron y aumentaron con la adopción del Reglamento (UE) 2019/881, con el objetivo de mejorar su capacidad institucional para contribuir a un alto nivel de seguridad común en toda la Unión y, en particular, para asesorar y sensibilizar a las instituciones, organismos y agencias europeos sobre cuestiones de ciberseguridad, así como a los ciudadanos cuya actividad o intereses profesionales se producen en el ámbito virtual.

Prácticamente, esta organización se convirtió en el principal promotor de la cultura de la seguridad en el entorno online, realizando esfuerzos para implementar las políticas de ciber-higiene y ciber-alfabetización entre los ciudadanos europeos, los consumidores, las empresas y las instituciones europeas. Todas sus acciones tienen como principal objectivo identificar y prevenir las amenazas cibernéticas, consideradas como uno de los problemas más grave que pueda afectar el funcionamiento del mercado interior comunitario y del medio ambiente en el que vivimos y nos desarrollamos como seres humanos[292].

El artículo 4 del Reglamento establece de modo exhaustivo los objetivos de ENISA que además de representar un centro técnico dedicado a asistir y asesorar los

[292] Balboni, P. (2010) "*Data Protection and Data Security Issues Related to Cloud Computing in the EU*"; ISSE 2010 Securing Electronic Business Processes - Highlights of the Information Security Solutions Europe Conference 2010; Tilburg Law School Research Paper No. 022/2010.

estados miembros y las instituciones comunitarias en sus esfuerzos de implementar políticas de seguridad cibernética, será al mismo tiempo un liante entre diferentes actores estatales y privados involucrados en la lucha contra las amenazas cibernéticas buscando soluciones para fomentar la cooperación entre las partes interesadas. Uno de los más importantes objetivos es de uniformizar los sistemas de certificación europea de ciberseguridad para asegurar la interconexión de las infraestructuras criticas nacionales y europeas.

Para alcanzar estos objetivos, ENISA cuenta con una serie de funciones (Capítulo II del Reglamento[293]) necesarias para contribuir a la preparación y aplicación de la política y del derecho de la Unión:

I. Institución reguladora. Además de la asistencia y el asesoramiento técnico y jurídico de los Estados miembros en el proceso de identificación y lucha contra las ciber amenazas, la Agencia participa en los esfuerzos para desarrollar e implementar políticas europeas comunes en el ámbito de la ciberseguridad. Los expertos de la Agencia analizan y emiten opiniones sobre iniciativas legislativas nacionales en el ámbito de referencia.

II. Institución de defensa cibernética. La Agencia se comporta como un liante entre las entidades involucradas en la lucha contra los ataques cibernéticos, apoyando el intercambio de información dentro y entre sectores, en particular en los sectores enumerados en la Directiva NIS, pero también proporciona asistencia especializada a los estados miembros, instituciones u otros organismos europeos, según corresponda, para:

- prevenir, detectar y analizar las amenazas y los incidentes cibernéticos y mejorar la capacidad de defensa frente a ellos, proporcionando los conocimientos y la experiencia necesaria; elaborar e implementar políticas para la divulgación voluntaria de vulnerabilidades;
- desarrollar equipos nacionales tipo CSIRT, a la demanda de los estados miembros, de conformidad con el artículo 9, apartado 5, de la Directiva NIS;
- impulsar los esfuerzos nacionales en el ámbito de la elaboración, la revisión y la promoción de estrategias nacionales para la seguridad cibernética y la difusión de

[293] *ENISA Programming Document 2020–2022* disponible en: https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-202020132022.

estos documentos en toda la Unión con el fin de interconectar las instituciones responsables por la implementación (obligación impuesta por la Directiva NIS).

- analizar e identificar los problemas relacionadas con la capacidad de reacción de los equipos nacionales CSIRT. Para solucionar las discrepancias técnicas e informacionales entre los equipos, ENISA está mandatada a iniciar dialogo e intercambios de experiencia entre estos equipos, asegurándose que, dado el estado actual de la tecnología, cada equipo está en acuerdo con los demás y dispone de las mismas capacidades y procedimientos internos;
- organizar cursos de formación sobre la ciberseguridad, en cooperación con las partes interesadas, incluso ejercicios temáticos al nivel regional cuyos resultados pueden ser utilizados en el proceso de reglamentación;

III. Institución de control, certificación y estandarización en el campo de la ciberseguridad. ENISA está responsable con las actividades de reglamentación e implementación de la política de certificación de ciberseguridad de la Unión para productos, servicios y procesos de tecnología de la información y la comunicación. También compila y publica pautas[294] y desarrolla buenas prácticas sobre requisitos de ciberseguridad, en cooperación con las autoridades nacionales responsables y los representantes de la industria de perfil, en un proceso formal, estandarizado y transparente. Además, tiene la obligación de evaluar los sistemas de certificación de seguridad cibernética vigentes en los estados miembros para identificar las brechas, formular propuestas y proponer reglamentaciones de remedio a la Comisión Europea.

Conforme a la estrategia de trabajo 2020-2022, los expertos de ENISA tiene la tarea de monitorear constantemente los desarrollos en las áreas relacionadas con la estandarización y de formular recomendaciones para especificaciones técnicas apropiadas a ser utilizadas en el desarrollo de sistemas europeos de certificación de seguridad cibernética. Por ejemplo, la Agencia ha recibido una solicitud de realizar un estudio sobre los desafíos relacionados con la seguridad de la inteligencia artificial, teniendo en cuenta los problemas, los riesgos y las soluciones relevantes. Par allegar a un resultado pertinente, ENISA tiene que identificar primero a las partes interesadas y a los expertos

[294] Ver a este respecto "*Good practices in innovation on Cybersecurity under the NCSS*" (19.11.2019) disponible en https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1, "Cyber Insurance: Recent Advances, Good Practices and Challenges" (07.11.2016) disponible en https://www.enisa.europa.eu/publications/cyber-insurance-recent-advances-good-practices-and-challenges;

relevantes. Los primeros resultados serán validados con la comunidad en general y las autoridades estatales competentes a través de talleres conjuntos y consultaciones. Las conclusiones validadas tras la finalización del proceso de consulta serán utilizadas par a orientar y apoyar a la Comisión Europea en las iniciativas políticas futuras y en curso relacionadas con el tema, como el enfoque europeo coordinado sobre inteligencia artificial.

Toda información obtenida y los resultados recompilados serán utilizados para fortalecer las capacidades de evaluación y certificación, para diseñar y adoptar normas y directrices en materia, así como brindando apoyo a los estados miembros que lo soliciten[295].

En la misma línea de actividad ENISA realiza y difunde análisis periódicos[296] sobre las tendencias más importante identificadas en el mercado de perfil, tanto en términos de demanda como de oferta, para estimular el mercado de ciberseguridad en la Unión.

IV. Institución con responsabilidades en el ámbito de la cooperación operacional dentro de la Unión Europea. Básicamente, la misión de la organización es facilitar el intercambio de información y buenas prácticas entre todos los grupos de interés, acercándolos, mediando entre los diversos intereses contrapuestos y dirigiendo los esfuerzos de los demás para mejorar constantemente la capacidad común de prevención, detección y respuesta a los incidentes dentro de la UE. Todos los incidentes cibernéticos con un impacto significativo y sustancial requieren una evaluación por parte de la Agencia para que los resultados se utilicen en esfuerzos futuros para combatir los ataques cibernéticos. El intercambio voluntario de información, entre empresas y CSIRT, entre ENISA y los Estados Miembros, es la forma de identificar las soluciones técnicas adecuadas a este tipo de amenazas. La Agencia también brinda asistencia en relación con las investigaciones técnicas llevadas a cabo después de incidentes con un impacto significativo o sustancial.

[295] ENISA (2019) *Bolstering ENISA in the EU Cybersecurity Certification Framework*, disponible en: https://www.enisa.europa.eu/publications/bolstering-enisa-in-the-eu-cybersecurity-certification-framework

[296] El último informe de análisis publicado por ENISA (26 de marzo de 2020) se refiere al estado del sistema educativo de la seguridad cibernética, la falta de recursos humanos calificados en este campo y las medidas necesarias para combatir este déficit - *Cybersecurity Skills Development in the EU* – disponible en: https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union

V. en el caso de los incidentes cibernéticos importantes o de crisis transfronterizas de seguridad cibernética a gran escala, ENISA contribuye activamente a la preparación de una respuesta común y coordinada, tanto a nivel de la Unión como de los Estados miembros, principalmente por los medios previstos en el artículo 7 (apartado 7) del Reglamento[297].

Los ejercicios temáticos anuales o bianuales organizados por la Agencia[298] junto con las instituciones y autoridades de los estados miembros contienen elementos técnicos, operacionales o estratégicos para la política de seguridad cibernética. Periódicamente, ENISA tiene la responsabilidad de organizar una simulación integral de un ciberataque de gran impacto para testar la capacidad de respuesta en situación de crisis. Al mismo tiempo, la Agencia también contribuye y apoya a la organización de ejercicios sectoriales de ciberseguridad en toda la Unión Europeea[299].

Anualmente, ENISA presenta una descripción general de las amenazas actuales y sus consecuencias. El informe[300] contiene información táctica y estratégica sobre las amenazas cibernéticas. También se refiere a los agentes de amenaza y los vectores de ataque típicos. Por lo tanto, el informe representa una fuente de Inteligencia Cibernética (CTI) genérica mediante objetos de información interrelacionados. El contenido del informe se basa en un ejercicio intensivo de recopilación de información, seguido de un análisis y consolidación de la información disponible públicamente sobre amenazas

---

[297] *"a) agregación y análisis de los informes procedentes de fuentes nacionales que son de dominio público y han sido puestos en común de manera voluntaria, con vistas a contribuir a la creación de una perspectiva común de la situación;*
b) garantía de la eficacia del flujo de información y oferta de mecanismos de intensificación entre la red de CSIRT y los responsables políticos y técnicos a nivel de la Unión;
c) facilitación, previa petición, de la gestión técnica de tales incidentes o crisis, en particular apoyando la puesta en común voluntaria de soluciones técnicas entre los Estados miembros;
d) apoyo a las instituciones, órganos y organismos de la Unión y, previa petición, a los Estados miembros en la comunicación pública en torno a esos incidentes o crisis;
e) prueba de los planes de cooperación para responder a dichos incidentes o crisis a nivel de la Unión y apoyo, previa petición, a los Estados miembros para que prueben dichos planes a escala nacional".
El texto completo es disponible en: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32019R0881#d1e1386-15-1.

[298] Los resultados del último ejercicio se publicaron en diciembre de 2018, *"Cyber Europe 2018 - After Action Report", disponible en:https://www.enisa.europa.eu/publications/cyber-europe-2018-after-action-report*

[299] ENISA (2019) idem.

[300] Los informes de ENISA están disponibles en el sitio web de la Agencia, la última publicación es *Roadmap on the cooperation between CSIRTS and LE*, publicada en diciembre de 2019, disponible en: https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-roadmap-on-csirt-le-cooperation.

cibernéticas, incluidos los informes anuales de incidentes identificados por la Agencia o por el Grupo de cooperación NIS en virtud de la Directiva. El informe proporciona información sobre la reducción de la exposición a amenazas. Esta información consistirá en los controles disponibles que sean adecuados para reducir la exposición y, en consecuencia, mitigar los riesgos resultantes. Además del informe, ENISA pone a disposición del público todos los materiales relevantes recopilados durante el año.

En el ámbito de la protección del derecho a la vida privada y de la seguridad, la Agencia coopera a nivel operacional y establece sinergias con las instituciones, los organismos, las oficinas y las agencias de la Unión, incluido el CERT-UE. La cooperación se materializa a través del intercambio de información, pero también a través del asesoramiento y la orientación de estos colaboradores en cuestiones relacionadas con la seguridad cibernética. ENISA también colabora con los servicios que tienen responsabilidades en el campo de la lucha contra el delito cibernético, pero también con las autoridades responsables a supervisar el procesamiento de datos personales, a fin de abordar cuestiones de interés común[301].

3.5. El marco regulatorio europeo sobre la certificación de la seguridad cibernética

La certificación juega un papel importante en el aumento de la confianza en el uso de las nuevas tecnologías. Por ende, resultó necesario establecer un marco de certificación europeo uniforme en el campo de la ciberseguridad, que establece los principales requisitos y líneas de cooperación, como condiciones necesarias para el desarrollo de sistemas de certificación europeos. Estos sistemas comunes permitirán la emisión de certificados europeos de ciberseguridad y declaraciones de conformidad para que los productos, los servicios o los procesos de ITC deben ser reconocidos y utilizados con confianza en todos los estados miembros. El Marco Europeo de Certificación de Seguridad Cibernética está regulado en el Capítulo III del Reglamento, Artículos 46-65.

Desde el artículo 1 del Reglamento, estamos informados sobre los objetivos perseguidos por la adopción de este acto normativo, a saber, "garantizar el correcto funcionamiento del mercado interior y lograr un alto nivel de seguridad cibernética", estableciendo, al respecto, las atribuciones, las cargas y los aspectos organizativos de

[301] Sandru, D.M. y Alexe, I. (2018) *Legislatia Uniunii Europene privind protectia datelor personale. (Legislación de la Unión Europea sobre la protección de datos personales*), Editorial Universitaria Bucarest.

ENISA, así como un marco común para la creación de esquemas europeos de certificación de la seguridad cibernética en la Unión.

Simultáneamente con el logro de este objetivo, se persigue evitar la fragmentación del mercado interno en lo que concierna los sistemas de certificación de ciberseguridad. Cabe señalar aquí que la adopción del Reglamento no afecta en ningún momento la competencia de los estados miembros en asuntos relacionados con la seguridad pública y la seguridad nacional y otras responsabilidades del estado en el ámbito del derecho penal.

El certificado europeo de ciberseguridad es "un documento emitido por un organismo relevante que certifica que un producto, servicio o proceso de TIC en particular fue evaluado para verificar el cumplimiento de los requisitos específicos de seguridad establecidos en un sistema europeo de certificación de la seguridad cibernética"[302]. Los certificados de seguridad deben indicar el nivel de garantía del producto, servicio o proceso según lo requerido por el Reglamento, es decir, "básico", "sustancial" o "elevado". El nivel de seguro corresponde al nivel de riesgo asociado con el uso previsto, entendido como la probabilidad y el impacto de un incidente.

Un sistema europeo de certificación de seguridad cibernética significa "un conjunto integral de normas, requisitos técnicos, estándares y procedimientos establecidos a nivel de la Unión que se aplican a la certificación o evaluación de la conformidad de ciertos productos, servicios y procesos de TIC"[303]. Observamos que la certificación de la ciberseguridad es voluntaria si no existen algunas provisiones legales europeos o nacionales que requieren esta certificación para ciertas actividades o ciertos productos informáticos. Un sistema europeo de certificación de la ciberseguridad propone a los destinatarios varios niveles de evaluación que resultan de las especificaciones, los criterios y las fórmulas utilizadas en la metodología de evaluación propuesta. Cada uno de los niveles de evaluación corresponde a uno de los niveles de seguridad y está definido por una combinación apropiada de componentes de seguridad.

[302] Como se desprende de la interpretación del artículo 2, punto 11 corroborado con el artículo 52 del Reglamento sobre la seguridad cibernética, https://eur-lex.europa.eu/legal-content/RO/ TXT /? uri = CELEX% 3A32019R0881 # d1e3299-15-1

[303]Según lo dispuesto en el art. 2, el punto 9 del Reglamento corroborado con las disposiciones del art. 49-52.

La misión de ENISA en el marco de la certificación de seguridad cibernética a nivel europeo es de contribuir de manera proactiva a la creación del marco emergente de la UE para la certificación de productos, procesos y servicios de TIC e implementar esquemas de certificación de los candidatos de acuerdo con las disposiciones del Reglamento. A lo largo de su trabajo, ENISA recibió el debido reconocimiento por sus resultados. En este contexto, la Agencia fue considerada la entidad apropiada para elaborar estos esquemas de certificación de candidatos en un marco único de certificación[304] de la ciberseguridad a nivel europeo[305].

Establecido a través de un reglamento, el marco europeo de certificación de la seguridad cibernética es directamente aplicable y obligatorio, lo que significa que se implementará de manera uniforme en todos los estados miembros.

La Comisión publicará un programa de trabajo evolutivo para la implementación de los esquemas de certificación europeos (llamado "programa de trabajo evolutivo de la Unión") que definirá las prioridades estratégicas para los futuros esquemas de certificación de seguridad cibernética europeos (de conformidad con el artículo 47, apartado 1 del Reglamento). Este programa de trabajo incluirá en particular una lista de productos, servicios y procesos de TIC o categorías de estos, que podrían beneficiarse de la inclusión en un sistema europeo de certificación de seguridad.

ENISA mantendrá un sitio web dedicado[306] para proporcionar información sobre los esquemas europeos de certificación de ciberseguridad, sobre los certificados europeos de ciberseguridad y las declaraciones de conformidad de la UE. Esta base de datos se actualizará con el fin de publicar información sobre nuevos documentos y certificaciones

[304] Artículo 46 - Marco europeo de certificación de la ciberseguridad:
"1. Se crea el marco europeo de certificación de la ciberseguridad con el fin de mejorar las condiciones de funcionamiento del mercado interior incrementando el nivel de ciberseguridad dentro de la Unión y haciendo posible un planteamiento armonizado a nivel de la Unión de esquemas europeos de certificación de la ciberseguridad, con el objetivo de crear un mercado único digital para los productos, servicios y procesos de TIC.
2. El marco europeo de certificación de la ciberseguridad define un mecanismo destinado a instaurar esquemas europeos de certificación de la ciberseguridad y a confirmar que los productos, servicios y procesos de TIC que hayan sido evaluados con arreglo a dichos esquemas cumplen los requisitos de seguridad especificados con el objetivo de proteger la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o procesados o las funciones o servicios que ofrecen, o a los que permiten acceder, dichos productos, servicios y procesos durante todo su ciclo de vida".
[305] ENISA (2019) *Bolstering ENISA in the EU cybersecurity certification framework*; disponible en https://www.enisa.europa.eu/publications/bolstering-enisa-in-the-eu-cybersecurity-certification-framework
[306] Disponible en https://www.enisa.europa.eu/topics/standards/adhoc_wg_calls.

emitidos, así como sobre certificaciones y autorizaciones retiradas, para que los consumidores y las partes interesadas estén informados sobre el grado de seguridad que ofrecen los productos, los servicios y procesos de TIC que utilizan. El Reglamento también prevé que esta base de datos indique los esquemas nacionales de certificación de seguridad cibernética que fueron reemplazados por un sistema europeo de certificación de la seguridad.

En lo que concierne a la validación de los sistemas de certificación europeos, el artículo 51 del Reglamento establece un conjunto de objetivos de seguridad que debe cumplir, al menos en parte (al menos uno) con cualquier sistema europeo de certificación de ciberseguridad, para que se considere válido.[307]

De conformidad con las disposiciones contenidas en el artículo 56 del Reglamento, se supone que los productos, servicios y procesos de TIC que fueron certificados de acuerdo con un sistema europeo de certificación de la seguridad cibernética, adoptado de acuerdo con el procedimiento establecido por el Reglamento, cumplen con los requisitos del sistema respectivo. Recordamos que el artículo 49 del Reglamento regula la preparación, adopción y revisión de los sistemas europeos de certificación de la seguridad cibernética, y se invita a los estados miembros a abstenerse de introducir nuevos sistemas nacionales de certificación para productos, servicios y

---

[307] *"Los esquemas europeos de certificación de la ciberseguridad deberán diseñarse para cumplir, según proceda, al menos los siguientes objetivos de seguridad:*
a) proteger los datos almacenados, transmitidos o tratados de otro modo frente al almacenamiento, tratamiento, acceso o revelación accidentales o no autorizados durante todo el ciclo de vida del producto, servicio o proceso de TIC;
b) proteger los datos almacenados, transmitidos o tratados de otro modo frente a la destrucción accidental o no autorizada, la pérdida o la alteración o la falta de disponibilidad durante todo el ciclo de vida del producto, servicio o proceso de TIC;
c) que las personas, programas o máquinas autorizados puedan acceder exclusivamente a los datos, servicios o funciones a que se refiere su derecho de acceso;
d) detectar y documentar las dependencias y vulnerabilidades conocidas;
e) registrar qué datos, servicios o funciones han sido objeto de acceso, de uso o de otro tratamiento, en qué momentos y por quién;
f) que sea posible comprobar qué datos, servicios o funciones han sido objeto de acceso, de uso o de otro tratamiento, en qué momentos y por quién;
g) verificar que los productos, servicios y procesos de TIC no contengan vulnerabilidades conocidas;
h) restaurar la disponibilidad y el acceso a los datos, servicios y funciones de forma rápida en caso de incidente físico o técnico;
i) que los productos, servicios y procesos de TIC sean seguros por defecto y desde el diseño;
j) que los productos, servicios y procesos de TIC se entreguen siempre con un programa y un equipo informáticos actualizados que no contengan vulnerabilidades conocidas públicamente, y dispongan de mecanismos para efectuar actualizaciones de seguridad".
Texto disponible en: https://eur-lex.europa.eu/eli/reg/2019/881/oj?locale=es.

procesos de TIC cubiertos por un sistema europeo válido de seguridad de certificación de seguridad cibernética.

La Comisión es responsable con el proceso de evaluación de la eficacia de los sistemas de certificación adoptadas. Sus informes deben presentar la eficiencia de la utilización paneuropea de estos sistemas de certificación y concluirá si implementar un sistema de certificación de seguridad único al nivel europeo será una medida benéfica para los estados miembros, que puede mejorar el funcionamiento del mercado interior y garantizar un alto nivel de ciberseguridad de los productos, servicios y procesos de TIC en la Unión. El día de 31 de diciembre de 2023 ha sido designado como la primera fecha para una primera de estas evaluaciones y se espera que las evaluaciones posteriores se producirán al menos cada dos años. Según las conclusiones extraídas de la primera actividad de este tipo, la Comisión va a elaborar una lista con los productos, servicios y procesos de TIC evaluados por un esquema de certificación existente que tiene que ser validada por un sistema de certificación obligatorio.

La emisión de certificados europeos de ciberseguridad no puede prorrogar más de la fecha limite prevista por el esquema europeo de certificación y su renovación solo se puede obtener si se cumplen los requisitos pertinentes previstos para su emisión, pero evaluados al momento de la solicitud de renovación.

El Reglamento introduce una presunción de conformidad con los requisitos legales para los certificados de la UE o las declaraciones de conformidad que se emiten bajo un sistema europeo de certificación de la seguridad cibernética.

Para crear una presunción de conformidad en caso de discordancia entre varias disposiciones legales de dos o más estados miembros que intentan cooperar en un asunto determinado, las normas de derecho nacional específicas de un estado miembro también pueden establecer que se puede utilizar un sistema europeo de certificación de la ciberseguridad.

En resumen, la necesidad de desarrollar un nuevo marco regulatorio directamente aplicable *erga omnes* ha surgido en el contexto de rápidos desarrollos tecnológicos de los últimos años. La digitalización de la mayoría de las industrias y sectores ha impuesto nuevas reglas de defensa contra los ciberataques. En este contexto, las instituciones comunitarias están obligadas a inducir a los Estados miembros un

comportamiento preventivo, basado en una permanente cooperación para prevenir y combatir inmediatamente y operativo los ataques, con el fin de proteger la infraestructura crítica europea.

Teniendo en cuenta los crecientes desafíos digitales a los que se enfrenta nuestra comunidad en el ámbito de la ciberseguridad, resultó necesario elaborar un marco común y completo de medidas, inspiradas en las acciones anteriores de los estados miembros y las autoridades, que promueva los objetivos de defensa recíproca mediante mecanismos de cooperación. Este conjunto de reglas está lejos de ser suficiente o de ofrecer soluciones a todos los problemas planteados por el creciente número de ataques cibernéticos y la diversidad de armas digitales.

El objetivo del enfoque normativo es garantizar un alto nivel de seguridad común para las redes y los sistemas de información de la Unión Europea y fomentar la cooperación internacional en este campo. En el campo de la seguridad cibernética, no estamos hablando de *self-defence*, sino de *common-defence*, porque el mundo digital se creó a partir de la interconexión y la interdependencia entre sistemas y redes informáticos.

En conclusión, la integración europea pasará de ser una integración jurídica a una cibernética, en la que los mecanismos de cooperación y confianza mutua serán más importantes que nunca, porque la seguridad ya no se puede pensar de forma individual sino en un sistema compartido. Si hasta ahora no ha sido posible adoptar una Constitución Europea e implementar un sistema legal único para todos los Estados, el sistema de certificación en ciberseguridad y las políticas de defensa común para infraestructura crítica será el paso más importante hacia la plena integración de los Estados en esta construcción política denominada la Unión Europea.

CAPITULO IV– LOS DERECHOS FUNDAMENTALES EN LA ERA DE LAS NUEVAS TECNOLOGÍAS

4.1. Consideraciones generales sobre los derechos fundamentales

"¿Quién, pues, no admirará al hombre? A ese hombre que no erradamente en los sagrados textos mosaicos y cristianos es designado ya con el nombre de todo ser de carne, ya con el de toda criatura, precisamente porque se forja, modela y transforma a sí mismo según el aspecto de todo ser y su ingenio según la naturaleza de toda criatura. Por esta razón el persa Euanthes, allí donde expone la teología caldea, escribe: El hombre no tiene una propia imagen nativa, sino muchas extrañas y adventicias".
(Giovanni Pico della Mirandola - "Discurso sobre la dignidad del hombre")

La historia del pensamiento filosófico y la historia del Derecho han destacado la importancia del ser humano en el universo, su lugar y su papel en una comunidad, como también la conducta social que debe tener. Desde un punto de vista diacrónico, el reconocimiento legal del valor del individuo y su propiedad jurídica sobre las prerrogativas que pueden protegerlo en la relación con el poder político y con los demás miembros de la sociedad se realizó tarde, bastante lento y con sacrificios reales. Pero podemos afirmar que los derechos del individuo han adquirido un estado bien definido no solo dentro de los límites de la legislación nacional, sino también al nivel de las organizaciones supraestatales, después de las dos conflagraciones mundiales con trágicas implicaciones para la humanidad.

Por estas razones, este capítulo de la tesis está dedicado a la evolución histórica de los derechos fundamentales, cronológicamente, así como a las teorías elaboradas en relación con la noción, la naturaleza jurídica y la clasificación de estos derechos. Las conclusiones que sacaremos al final de este capítulo nos ayudarán a continuar el análisis del derecho a la privacidad y el derecho a la seguridad en una determinada categoría de derechos fundamentales.

El ámbito de los derechos fundamentales no podría quedar inmune a la influencia de las nuevas tecnologías. La digitalización del mundo obliga a los conceptos clásico a adaptarse a la nueva forma de la vida humana. Ahora, más que nunca tenemos que estar

despiertos y pendientes al traslado de los valores humanos, culturales, jurídicos y sociales desde lo material a lo virtual.

4.2. La importancia de los derechos fundamentales en la sociedad contemporánea

El Derecho se desarrolla de acuerdo con una serie de factores, como el contexto natural, social y político, y el factor humano; este último debe considerarse el más importante: la ley está escrita por hombres, para los hombres. La quintaesencia de tal concepto fue expresada por un teórico del derecho al referirse al factor humano desde la perspectiva de los derechos del individuo:

"la dimensión humana de la ley concierne, sobre todo, los derechos esenciales del individuo (los derechos fundamentales), derechos que garantizan la igualdad, la plenitud de todos los hombres, su capacidad de manifestarse inquebrantablemente sobre la base de la dignidad y la libertad, porque el hombre, por su naturaleza, es un ser digno y libre"[308].

Reconocidos como valores intrínsecos de los seres humanos, los derechos de la persona humana han sido teorizados y posteriormente regulados legalmente mediante el pacto entre el individuo y el poder público ejecutivo (el establecimiento de las "libertades públicas" y de "las obligaciones públicas"), pero también con el poder legislativo y judicial, en el marco del "contrato social"[309]

Los derechos no fueron aceptados inmediatamente por todos los estados, ni en una configuración idéntica; sin embargo, la aparición de las organizaciones internacionales y los eventos históricos que marcaron el siglo XX determinaron la extrapolación de catálogos nacionales e interestatales de derechos, al sublimar un número limitado de derechos acompañados de salvaguardas específicas.

Una definición de los derechos fundamentales, aceptada por la comunidad científica internacional, es ofrecida por el profesor francés Louis Favoreu, que considera que los derechos fundamentales pueden ser comprendidos como *"el conjunto de los derechos y libertades reconocidos a las personas físicas como a las personas jurídicas (de derecho privado o de derecho público) en virtud de la Constitución pero también de*

[308] Popa, N. (1994) *Teoria generală a dreptului. (La Teoría General del Derecho)*; Editorial Actami Publishing, Bucarest, p. 68.

[309] El contrato social supone una relación política establecida entre el individuo y el Estado, en la que los bienes y las personas asociadas están protegidos, mientras se mantiene la libertad del individuo, en este sentido: Rousseau, J.J. (1996) "*El contrato social",* libro II, cap. I, Edit. Alba, Madrid.

los textos internacionales y protegidos tanto contra el poder ejecutivo como contra el poder legislativo por el juez constitucional o el juez internacional" [310].

Por tanto, la definición y regulación de los derechos en los textos legales, la provisión de una tutela efectiva por las jurisdicciones constitucionales, en oposición al poder público, determina la caracterización de ciertos derechos como fundamentales. Deben ser analizados en un contexto amplio, a la luz de las normas e instituciones que los protegen como un conjunto de garantías legales e institucionales. Derechos como la libertad, la igualdad y la seguridad del ser humano, junto con el derecho a la dignidad, deben ser tratados con carácter prioritario y protegidos por mecanismos judiciales, institucionales a nivel estatal, regional e internacional, cuya efectividad no puede verse afectada por intervención política o militar.

Aparentemente creados por el Estado contra el Estado, los derechos fundamentales desempeñan un papel muy importante para el equilibrio del poder dentro de las democracias auténticas y el Estado de derecho, basado en el respeto de la ley (los conceptos de "rule of law" y "la préeminence de droit" frecuentemente citados en la jurisprudencia del Tribunal Europeo de Derechos Humanos, incluso en casos relativos a la protección del derecho a la vida privada)[311]. Por eso, como opinión nuestra, la afirmación formal de ciertos derechos a través del texto constitucional no es una condición suficiente para admitir el carácter fundamental de los derechos: estados totalitarios o aparentemente democráticos, aunque los hayan declarado de esta manera, han dejado las garantías sin el contenido necesario para proteger esos derechos en la práctica. Como también ha declarado el Tribunal Europeo de Derechos Humanos, los derechos no deben ser "*teóricos e ilusorios, sino concretos y efectivos*".[312]

El art. 16 de la Declaración de Derechos del Hombre y del Ciudadano de 1789 afirma que "*toda Sociedad en la que los derechos fundamentales no están establecidos ni la separación de poderes garantizada carece de Constitución*". De aquí podemos concluir que de una Constitución no puede faltar las normas relativas a los derechos humanos, es decir que una Constitución sin derechos no es tal. Pero, al mismo tiempo los derechos fundamentales no gozan de reconocimiento si no están definidos y regulados por la

[310] Favoreu, L. (1990) "*L'élargissement de la saisine du Conseil constitutionnel aux jurisdictions administratives et judiciaires*", RFDC N°4/1990, pp. 581 y siguientes.
[311] Bîrsan, C. (2010) *Conventia europeana a drepturilor omului. Comentariu pe articole* (*El Convenio Europeo de Derechos Humanos. Comentarios sobre los artículos*), Edición 2, C.H. Beck, Bucarest.
[312] Carrillo Salcedo, J. A. (1991) *Protección de derechos humanos en el Consejo de Europa: hacia la superación de la dualidad entre derechos civiles y políticos y derechos económicos y sociales*, Revista de Instituciones Europeas, Vol. 18, Nº 2, págs. 431-454;

Constitución. Asi que nos encontramos en un círculo sin fin. Un ordenamiento jurídico podrá reconocer cuantos derechos subjetivos estime oportuno, pero sólo se consideran como fundamentales los derechos que se recogen en la norma suprema del país.

Los derechos han evolucionado con la historia y con el mundo, adaptándose a los cambios culturales, económicos, religiosos para proteger el ser humano de todos los riesgos nacidos desde la tormenta tecnológica y digital que caracteriza las últimas décadas de nuestras vidas:

> *"La historia, o mejor la razón situada en la historia, recordémoslo, ya abrió una ventana a la evolución de los derechos, a su carácter de invento moral y a su visión dinámica como concepto proprio del mundo moderno (y por tanto ni estático, ni atemporal, ni teológico, tal y como hemos visto). La realidad abría otra ahora hacia la sociedad y la economía, sin más pretensiones, salvo descriptivas y para apoyar una mirada crítica sobre el estado real de los derechos, evitando un formalismo ético y/o jurídico excesivo"*[313].

Al mismo tiempo, el fenómeno de fusión entre el orden jurídico nacional e internacional manifestado en las últimas décadas (nos referimos, por ejemplo, a los conceptos de "europeización del derecho nacional" o "constitucionalización del derecho europeo") ha determinado un intercambio permanente de nociones, reglas, excepciones, de los regímenes legales, de modo que los derechos individuales hayan transgredido el espacio legal en el que fueron creados, siendo adoptados naturalmente o trasplantados artificialmente a otros sistemas legales. La persona creativa y portadora de derechos ("el titular"), sometida a la globalización legal, se ha convertido en un sujeto de derecho nacional e internacional, pero también en un ciudadano dotado de derechos fundamentales específicos de este estatuto, debido a los lazos políticos y legales establecidos entre las entidades nacionales e internacionales.

A pesar de una serie de instrumentos jurídicos de protección universal o regional de los derechos fundamentales fueron reconocidos como verdaderos modelos para cualquier estado de derecho, debido al fenómeno de la interpenetración mencionado anteriormente. También se nota una atracción para ajustar los modelos internos sobre la revisión constitucional y un apetito por un chapado en oro (inflación legislativa) de los instrumentos de cooperación de reforma dirigido a la seguridad de los derechos

[313] Rodriguez Uribes, J. M. (2015) *Gregorio Peces-Barba – Justicia Y Derecho*, Editorial Aranzadi, p. 164

fundamentales, con el pretexto de adaptarlos a los riesgos y al progreso del mundo moderno[314].

En tal contexto legal, complejo y dinámico, sigue siendo importante preservar la dignidad humana, el valor de la que extraen la savia todos los derechos fundamentales. En consecuencia, la privacidad del individuo a través de medios legales apropiados puede ser el último reducto de defensa de su condición, la persona libre dotada de derechos en las relaciones con las autoridades y otros miembros de la comunidad[315].

4.3. El concepto de derechos fundamentales. Concepto y clasificación

4.3.1. Concepto

Bajo las influencias de las revoluciones políticas y económicas del siglo XIX, los derechos individuales fueron reconocidos y definidos, primero a nivel filosófico, y luego desde un punto de vista legal, de manera bastante lenta y no homogénea, en términos de su aceptación por parte de los Estados[316]. Considerado por algunos como una "nueva religión" y por otros como un "arma contra la tiranía", no se puede negar el papel de los derechos individuales en la afirmación de nuevos órdenes constitucionales, específicos del estado democrático, del estado de derecho, por supuesto, sujeto a su observancia efectiva representantes del estado.

En el contexto de las condiciones políticas, legales, sociales y económicas de una sociedad, en un cierto momento, cada legislador constituyente, también considerando sus tradiciones legales, ha seleccionado un número limitado de derechos entre aquellos (potencialmente) reconocidos en el sistema de derecho consuetudinario y los elevó al estado de los derechos constitucionales[317].

El vocabulario jurídico no abrazó la noción de "derechos fundamentales" desde el principio, ya que su génesis, desde un punto de vista terminológico, se atribuyó principalmente al sistema legal alemán. En el contexto del trasplante legal de la noción

---

[314] Bidart Campos, G. (1994) "*La interpretación de los derechos humanos*", Editorial Ediar, Buenos Aires, pp. 30-31.
[315] Peces-Barba Martínez, G. (2002) *La dignidad de la persona desde la filosofía del derecho*. Madrid: Dykinson.
[316] García Amado, J. A. (2000) "*Los derechos fundamentales y las enseñanzas de la historia: Breve comentario al volumen 1 de la historia de los derechos fundamentales, titulado Tránsito a la modernidad. Siglos XVI y XVII*", en Derechos Y Libertades: Revista Del Instituto Bartolomé De Las Casas, Año 5, N. 8 (en.-jun. 2000).
[317] Mihai G. (2005) *Fundamentele Dreptului* (*Fundamentos del Derecho*), Editorial All Beck, Bucharest.

desde el sistema nacional a internacional (y viceversa)[318], así como el préstamo directo entre diferentes sistemas de legislación nacional, el uso de la noción de "derechos fundamentales" se ha convertido en una práctica común, especialmente en el espacio europeo.

Los derechos fundamentales son principalmente derechos subjetivos[319], sin ser distintos de ellos por su naturaleza específica o por su objeto, los derechos fundamentales se convierten en una categoría distinta del resto de los derechos y representa la base legal del conjunto de derechos subjetivos garantizados por la ley.

Teniendo en cuenta que no todos los derechos subjetivos son considerados al mismo tiempo fundamentales, se observa que la selección de un conjunto limitado de derechos se debe a la importancia que se les otorgan por los órganos representativos (los poderes soberanos delegados por el pueblo) al adoptar o revisar una Constitución o al adoptar o modificar una convención internacional, que los legitima y les otorga una fuerza legal superior sobre otros derechos "ordinarios"[320].

La dinámica de los fenómenos intrínsecos o extrínsecos de un orden jurídico a su vez determina que un catálogo de derechos fundamentales pueda complementarse más. Desde este punto de vista, la jurisprudencia constitucional, que en muchos casos (Alemania, Estados Unidos) ha demostrado ser un legislador, desempeñando un papel importante en este sentido, además del trasplante legal obligatorio (factor externo) determinado por la pertenencia a una determinada organización regional o internacional (factor interno).

En la doctrina francesa del derecho constitucional[321], se estima que el momento en que se inició un debate real sobre esta noción coincide con la fecha del Coloquio de Aix (1981). Recordamos la definición formulada en esta ocasión: "*el conjunto de derechos y libertades reconocidos tanto a los individuos como a las personas jurídicas*

---

[318] Con respecto a las tipologías de trasplante constitucional, ver ROGHINA, R. C. "*Trasplante de Constitución*", en The Journal of Public Law, no. 4/2012, pp. 124-140. El autor formula una definición de este fenómeno: "la situación en la que un sistema legal asume normas, instituciones, conceptos constitucionales e incluso regímenes políticos de otros sistemas jurídicos; El trasplante constitucional también puede entenderse como un proceso mediante el cual los "elementos constitucionales" se están expandiendo y ejerciendo influencias a nivel internacional" (p.124)

[319] El derecho subjetivo se ha definido como la capacidad jurídica individual de una persona u organización que les da la oportunidad, en una relación jurídica, de tener una cierta actitud hacia su derecho, de exigir una actitud adecuada por parte del sujeto obligado y exigiendo la defensa de su derecho por la restricción impuesta por el estado - Venegas Grau, M. (2004) *Derechos fundamentales y derecho privado. Los derechos fundamentales en las relaciones entre particulares y el principio de autonomía privada,* Editorial Marcial Pons Madrid, p. 138.

[320] Prieto Sanchís, L. (1990) *Estudios sobre derechos fundamentales,* Editorial Debate, Madrid, p. 206

[321] Favoreu, L. y otros (2008) *Droit constitutionnel*, 11e édition, Editorial Dalloz, Paris, p. 854.

(derecho privado y público) en virtud de la Constitución, pero también por textos internacionales, y protegidos tanto contra el poder ejecutivo como contra del poder legislativo por el juez constitucional (o por el juez internacional)"[322].

De acuerdo con esta definición, el criterio según el cual un derecho entra en la categoría de los fundamentales depende del modo de su consagración legal (respectivamente en la Constitución o en un texto internacional), o de su protección efectiva en relación con el poder ejecutivo y legislativo, de la garantía de protección otorgada por la revisión judicial de la constitucionalidad. En cuanto a los titulares identificados, creemos que no en todos los casos, las personas jurídicas se convierten en titulares de los derechos fundamentales (derecho a la vida, por ejemplo). Por eso, esta definición parece colocar en su núcleo el criterio formal (el reconocimiento de derechos a través de textos de leyes superiores) y el criterio de protección jurisdiccional constitucional.

En otra opinión[323], la principal característica de los derechos fundamentales (que los distingue de otros derechos subjetivos) es de ser derechos esenciales para los seres humanos, para su vida, libertad, personalidad, así concluimos que el objeto de la protección legal puede considerarse como el elemento central para definirlos.

En el contexto contemporáneo, según la opinión del profesor Gregorio Pesces-Barba, "*el concepto de derechos humanos se reserva generalmente para denominar a los derechos de la persona, reconocidos y garantizados por el Derecho Internacional, sea éste Consuetudinario, Convencional o Ius Cogens (Derecho Internacional de los Derechos Humanos y Derecho Internacional Humanitario)*" [324]. A veces la categoría se extiende también a las nociones y derivaciones jurídicas reguladas en las constituciones ganando la denominación de derechos constitucionales o derechos fundamentales.

Por lo tanto, se observa que la doctrina del derecho constitucional no es unánime al establecer la definición de derechos fundamentales. Sin embargo, según algunas opiniones[325], los derechos fundamentales se definieron así: derechos subjetivos de los ciudadanos, esenciales para su vida, libertad y dignidad, indispensables para el libre desarrollo de la personalidad humana, establecidos por la Constitución y garantizados por

---

[322] Ibidem.

[323] Muraru I. (1995) Reflectarea drepturilor omului în noua Constituţie a României *(Reflexión sobre los derechos humanos en la nueva Constitución de Rumania*), en I. Muraru, M. Constantinescu, *Studii constitutionale* (Estudios constitucionales), Editorial Actami, Bucarest, página 140

[324] Peces-Barba Martínez, G. (1995) *Curso de derechos fundamentales: teoría general*. Madrid: Universidad Carlos III de Madrid: Boletín Oficial del Estado, p. 37.

[325] Maritain, J. (1991) "*Acerca de la filosofía de los derechos del hombre*", Editorial Debate, Madrid.

la Constitución y leyes. El denominador común dentro de las diversas definiciones es el elemento relacionado con el tipo (rango) de la norma legal que consagra un derecho fundamental, de modo que en una opinión cuasi general se admite que el derecho fundamental está dado por su protección mediante instrumentos jurídicos internacionales y constitucionales[326].

También hay opiniones[327] en la doctrina jurídica rumana como que la definición de los derechos fundamentales no puede limitarse a su forma de regulación, sino que también debe incluir el alcance de los titulares de los derechos, así como el sistema de garantías para su ejercicio efectivo. Según estas opiniones, los derechos fundamentales son plenamente reconocidos y protegidos por un determinado sistema legal si el marco normativo cumple cuatro condiciones principales:

1. existe una serie de "facultades" que pertenecen a todas las personas;
2. las normas legales e infra legales que pueden suprimir o limitar excesivo estas facultades son consideradas erróneas;
3. siempre existe un organismo jurisdiccional capacitado a controlar y cancelar las normas que limitan o infringen los derechos fundamentales;
4. los titulares de los derechos fundamentales tienen la posibilidad de solicitar el apoyo de los organismos jurisdiccionales de control en cualquier momento.

Las últimas dos condiciones subrayan la importancia de la protección jurisdiccional de los derechos humanos para su clasificación como fundamentales. Esta posibilidad reconocida al titular de tales derechos a acudir a los tribunales para obtener el respecto de sus derechos erga omnes es específica también para la doctrina alemana relativa a los derechos individuales[328].

En el sistema legal de "*common-law*" se considera que "*en un plan práctico, la existencia de un derecho depende de la existencia de un remedio que puede sancionar su violación*"[329].

De tal forma que es importante no confundir los derechos fundamentales con otros derechos civiles que benefician de protección jurisdiccional. En nuestra opinión, las principales características de los derechos fundamentales, que los distingue de los demás derechos subjetivos, son los siguientes:

---

[326] Fernández, E. (1991) *Teoría de la justicia y derechos humanos,* Editorial Debate, Madrid, p. 113.
[327] Selejan-Guţan, B. (2004) *Drept Constitutional si Institutii Politice* (*Derecho constitucional e instituciones políticas)*, volumen I, Universidad de Sibiu "Lucian Blaga", página 161.
[328] Eckhold-Schmdt, F. (1974) *"Legitimation durch Begründung*", Editorial Dissertation Berlín.
[329] Legrand, P. (2001) *Derecho Comparado*, Editorial Lumina Lex Bucharest, p. 80.

I. los valores que defienden son esenciales por su contenido (vida, libertad, dignidad humana, libre desarrollo de la personalidad humana, participación en actividades sociales, políticas, culturales del estado);
II. las normas legales que los consagran y los protegen tienen carácter imperativo de valor supremo (de naturaleza constitucional o internacional) o existe una jurisprudencia del mismo rango que las reconoce;
III. está garantizado el acceso de los titulares a los mecanismos de control y protección judicial del más alto rango en un sistema legal (litigios constitucionales y tribunales internacionales, tales como T.E.D.H. o Tribunal de Justicia de la Unión Europea)[330].

Además de estas opiniones presentadas más arriba, también se ha formulado una doctrina[331] según la cual los derechos fundamentales pueden percibirse desde otras perspectivas: primero, como reglas en relación con las cuales se realiza la interpretación de las normas, específicas de la última etapa de la evolución la teoría de los derechos individuales; luego, como principios legales que dictan la interpretación de todas las ramas del derecho, de acuerdo con la teoría de los efectos positivos de los derechos fundamentales desarrollada en la jurisprudencia del Tribunal Constitucional Federal Alemán.

Basado en esta teoría, los derechos fundamentales ya no despliega solo un papel defensivo en la relación con el Estado, como propone la teoría liberal clásica, sino que se convierten en reglas objetivas (según la jurisprudencia basada en la decisión Lüth de la Corte Suprema Alemana) que implica la referencia de todo el orden legal a estos valores supremos, transformándose así en reglas implícitas de interpretación y aplicación de la ley para los jueces y otros representantes del poder público.

Estas afirmaciones solo refuerzan la idea de "constitucionalización de los derechos"[332] en términos de reconocer el efecto ascendente y descendente de la supremacía de la Constitución sobre el sistema jurídico, en su totalidad, por una parte, multiplicando las normas constitucionales inferidas de otras normas o principios de rango

[330] Ibidem;
[331] Ossenbühl, F. (2000) *Staatshaftungsrecht (Ley de responsabilidad del estado)*, Editorial C.H.Beck; Auflage.
[332] La constitucionalización ha sido definida como un "fenómeno jurídico complejo que afecta en su conjunto a un sistema jurídico determinado a través de la interacción establecida entre las normas jurídicas de las leyes fundamentales y el resto de las normas jurídicas inferiores a la Constitución" *–Böckenförde E. W. (1991): "State, Society, and Liberty: Studies in Political Theory and Constitutional Law", editorial Berg, New York.*

inferior y, por otro lado, "impregnando" las ramas del derecho con normas constitucionales directamente aplicables por todos los sujetos de derecho.

Como tal, los derechos fundamentales consagrados en el texto constitucional prestan el carácter supremo y los efectos sobre el estado de derecho definidos por la Constitución. Como consecuencia, las garantías legales de la Constitución se transfieren a los derechos fundamentales, de modo que también benefician del control general de su aplicación en el nivel de todas las estructuras estatales y al nivel de los actos jurídicos emitidos por ellos, incluso el control de constitucionalidad que garantiza el cumplimiento de las leyes con las normas y los principios de origen constitucional, a través de una jurisdicción político-judicial.

El papel del juez ordinario debe manifestarse activamente tanto en términos de interpretación directa y aplicación de normas constitucionales (si corresponde) como en la notificación de los elementos de incumplimiento con la Constitución de un acto legislativo, estando obligado a notificar al tribunal constitucional[333].

Incluso en un litigio privado, los participantes en el juicio y el tribunal pueden invocar directamente reglas o principios constitucionales diseñados para garantizar el respeto de los derechos fundamentales, que se asimilan en la doctrina alemana a los efectos horizontales como parte de los efectos positivos de estos derechos[334]. En cuanto a los jueces constitucionales, su activismo judicial (opuesto al fenómeno de la "autolimitación judicial") se considera en la doctrina como necesario "*para desarrollar un ejercicio de interpretación creativa del texto de la ley, más allá de su estrecho sentido, a la protección de los derechos fundamentales y su impregnación en el sistema legal*"[335], contribuyendo así a la constitucionalización de la ley, adaptada a los cambios económicos, sociales, políticos y legales.

La determinación del alcance y del contenido de los derechos fundamentales se basa en textos constitucionales (o convencionales) y detallados (si los hay) por normas jurídicas inferiores, pero también la práctica judicial desempeña un papel importante en la determinación del contenido y los límites de estos derechos.

---

[333] Por ejemplo, el artículo 53, párrafo 2 de la Constitución española expresa que "cualquier ciudadano podrá recabar la tutela de las libertades y derechos reconocidos en el artículo 14 y la Sección primera del Capítulo segundo ante los Tribunales ordinarios por un procedimiento basado en los principios de preferencia y sumariedad y, en su caso, a través del recurso de amparo ante el Tribunal Constitucional. Este último recurso será aplicable a la objeción de conciencia reconocida en el artículo 30".

[334] Böckenförde, E. W. (1991) *State, Society, and Liberty: Studies in Political Theory and Constitutional Law*, Editorial Berg, New York.

[335] Selejan-Guţan, B. (2005) *Excepţia de neconstituţionalitate (Excepción de la inconstitucionalidad)*, Editorial All Beck, Bucarest, p.120.

En conclusión, los derechos fundamentales cumplen tanto el papel de valores supremos garantizados por las normas jurídicas con fuerza legal superior, al mismo tiempo que el papel de principios legales que establecen los criterios básicos para la interpretación de las reglas de un sistema legal.

La definición de los derechos fundamentales es posible siguiendo el criterio formal – según el cual los derechos fundamentales son derechos consagrados en la Constitución y en los tratados internacionales – y siguiendo el criterio sustancial que supone la declaración de un derecho fundamental reportándose a los valores superiores (como la dignidad humana consagrados en ella) que están garantizados por el mismo derecho[336].

Las características de los derechos fundamentales resultan de los elementos que componen su contenido:

- derechos subjetivos, individuales por su titular, indivisibles[337], cuyos titulares pueden ser personas físicas (ciudadanos de un Estado o de una organización) o personas jurídicas;
- derechos que defienden valores esenciales, seleccionados y considerados supremos en un momento histórico dado por cada Estado; la esencia de los derechos fundamentales no puede verse afectada por las restricciones que se les imponen, en las condiciones limitadas de legalidad y proporcionalidad permitidas por la Constitución[338];
- derechos consagrados en las normas imperativas de valor supremo o en las prácticas de los tribunales constitucionales o internacionales, que tienen el potencial de aplicabilidad directa e inmediata legalmente vinculante;
- derechos que limitan los poderes del estado a la hora de tomar medidas legislativas que puedan suspender el ejercicio de tales derechos;

[336] Bon, P. (1992) *La protección constitucional de los derechos fundamentales. Aspectos de Derecho Comparado Europeo*, en *Revista del Centro de Estudios Constitucionales*, N.º 11, Madrid, p. 48.
[337] Deaconu, S. (2011) *Drepturile şi libertăţile fundamentale în sistemul constituţional românesc* (*Derechos y libertades fundamentales en el sistema constitucional rumano*), artículo publicado en "Revista rumana de derecho privado", núm. 4/2011.
[338] El artículo 55.2 de la Constitución Española contiene algunas cautelas en relación con la adopción de medidas de suspensión individual de derechos y libertades: "una ley orgánica podrá determinar la forma y los casos en los que, de forma individual y con la necesaria intervención judicial y el adecuado control parlamentario, los derechos reconocidos en los artículos 17, apartado 2, y 18, apartados 2 y 3, pueden ser suspendidos para personas determinadas, en relación con las investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas. La utilización injustificada o abusiva de las facultades reconocidas en dicha ley orgánica producirá responsabilidad penal, como violación de los derechos y libertades reconocidos por las leyes".

- derechos aplicables directamente[339], bajo "la ley", cuando las normas constitucionales mandan al legislador ordinario a regular en detalle las condiciones de aplicación de ciertos derechos;
- derechos justiciables antes de los tribunales del más alto nivel en un sistema legal;
- derechos componentes de un estatus legal del ciudadano, junto con otros derechos subjetivos y deberes fundamentales[340];
- derechos relativos, en la mayoría de los casos, que pueden ser objeto de restricciones (se consideran derechos absolutos los derechos como el de no ser sometido a torturas ni a tratos inhumanos o degradantes, o la prohibición de la esclavitud).

Los derechos fundamentales limitan los poderes del Estado, aspecto que produce efectos verticales, defendiendo el individuo en relación con los titulares del poder público ejecutivo, legislativo, judicial. Al mismo tiempo, los derechos fundamentales también causan efectos horizontales, ya que protegen al individuo en las relaciones legales con otras personas. Como tal, tanto el Estado (en el sentido puramente legal - conjunto sistemático de órganos estatales) igual que otros sujetos tienen obligaciones principalmente negativas, a abstenerse de conductas que puedan perjudicar al titular del derecho, pero también una obligación positiva, que implica una acción diseñada para garantizar el pleno ejercicio de un derecho fundamental.

Por último, podemos proponer la siguiente definición de los derechos fundamentales: derechos individuales, que protegen valores fundamentales, cuyo carácter supremo es reconocido por las normas legales con una fuerza superior dentro de un sistema normativo o bajo la jurisprudencia de los tribunales de la jurisdicción constitucional o internacional y que están garantizados por la Constitución, por las leyes y por el control de los tribunales.

4.3.2. Clasificación de los Derechos Fundamentales

Así como hemos presentado en la subsección 4.31, la catalogación de los derechos fundamentales en una constitución o en un tratado internacional implica un proceso de selección de los derechos subjetivos considerados más importantes para el Estado o para la organización en cuestión, según los valores que protege y la importancia dada en un cierto momento histórico. Sin embargo, una vez que se ha finalizado tal

[339] Favoreu, L.y otros (2008) *Droit constitutionnel*, Editorial Dalloz, Paris, 11e édition, p. 869 – 870 ;
[340] Schneider, H. P. (1979) *Peculiaridad y función de los Derechos fundamentales de un Estado constitucional democrático* en *Revista de Estudios Políticos*, Nº 7 (Nueva época), Madrid, p. 23.

catálogo, todos estos derechos y libertades son de igual importancia[341], y no se puede alcanzar una jerarquía entre ellos[342] (aunque, por ejemplo, la libertad individual tiene de hecho un significado más importante que el derecho de asociación).

Por otro lado, la ausencia de una jerarquía no implica a priori la imposibilidad de clasificar los derechos fundamentales según ciertos criterios. Así, uno de los criterios identificados en la literatura[343] se refiere a la forma en que se describe el contenido sustantivo de los derechos fundamentales en las Constituciones o en las declaraciones de derechos (el criterio material), según el cual los derechos se clasificaron en:

a) derechos-principios;

b) derechos cuyo contenido material es detallado por el legislador ordinario y

c) derechos fundamentales cuyo contenido material se detalla en la norma constitucional o internacional.

Esta clasificación también es relevante en términos de la aplicación de las reglas que rigen los derechos fundamentales, solo esta última permite la aplicación directa, mientras que, en el caso de las dos primeras categorías, las reglas constitucionales se aplican indirectamente, requiriendo la intervención del legislador ordinario[344].

Otra clasificación sigue el criterio del modo de reconocimiento de los derechos fundamentales (el criterio formal), sobre cuya base los derechos se pueden clasificar en:

1. derechos consagrados en la Constitución de un Estado;

2. derechos enumerados en instrumentos legales internacionales con fuerza legal obligatoria;

3. derechos establecidos por la practica judicial, basados en la jurisprudencia de los tribunales de justicia constitucionales o internacionales[345].

La Constitución española de 1978 ha optado por una clasificación relevante en el plano de la interpretación y aplicación de los derechos fundamentales, no en el cuadro del análisis histórico o conceptual. El Título I de la Constitución, dividido en cinco capítulos, es la principal sede de la regulación de los derechos fundamentales. Los

---

[341] Según otro autor - *Renucci J.F. (2009) Tratado de derecho europeo de derechos humanos,* - los derechos consagrados en la ley positiva no pueden tener el mismo nivel de igualdad y no pueden tener el mismo régimen legal. Sin embargo, se considera que la distinción entre los derechos humanos sería criticada desde el punto de vista del principio de indivisibilidad.

[342] Favoreu, L.y otros (2008) idem, p. 854;

[343] Deaconu, S. (2011) idem.

[344] Pérez-Luño, Antonio, (2007) *Los derechos fundamentales*, Editorial Tecnos Madrid.

[345] Salazar, S. (2013) *Fundamentación y estructura de los derechos sociales*, en Revista de Derecho (Valdivia), Vol. 26, Nº 1, pp. 69-93

primeros tres capítulos definen y regulan los derechos sustantivos. Los dos últimos capítulos tratan sobre el régimen jurídico y las garantías de las libertades y derechos de los ciudadanos. El artículo 53 de la Constitución Española ofrece los criterios de clasificación entre ciertas categorías de derechos y libertades: las fuentes y las garantías. Según el criterio de las fuentes distinguimos entre "*los derechos del capítulo segundo y aquellas libertades o derechos que no se hallan sometidos a esta rigurosa cláusula y que por lo tanto pueden obtener un desarrollo de otra naturaleza*"[346].

Usando el segundo criterio, el de las garantías[347], podemos clasificar los derechos en tres categorías:

a) Derechos subjetivos que gozan de una tutela ordinaria disponible para cualquier derecho en el ordenamiento español.

b) Derechos fundamentales que gozan de la protección del recurso de amparo ante el Tribunal Constitucional y de un recurso preferente y sumario ante los Tribunales ordinarios denominado por la doctrina recurso de amparo judicial.

c) Derechos de naturaleza económica, social o cultural, que no gozan de un alto grado de protección judicial, pero se pueden defender usando las garantías jurisdiccionales comunes.

Sin embargo, observamos que dentro del orden jurídico interno de un estado tipo dualista, los derechos consagrados en los instrumentos jurídicos internacionales adquieren la fuerza legal de los derechos fundamentales tras la adopción de los actos necesarios para su internalización, y pueden tener prioridad sobre los principios constitucionales y las regulaciones internas en la medida en que contengan reglas más favorables (lex mitior).

Dependiendo del tipo de obligación del Estado para garantizar (criterio de límite), los derechos fundamentales también pueden clasificarse en:

a) derechos que requieren principalmente una obligación positiva del estado (derecho a la educación o protección de la salud);

b) derechos que requieren predominantemente una obligación negativa del estado (derecho a la vida, libertad de conciencia)[348].

[346] Alexy, R. (2002) *Teoría de los derechos fundamentales*, Editorial CEPEC Madrid.
[347] Ferrajoli, L. (2010) *Derechos y garantías. La ley del más débil,* Editorial Ariel Barcelona.
[348] Wachmann, P. (1999) *Libertés publiques,* Editorial Dalloz, París.

El profesor Gregorio Peces-Barba[349], ofrece una clasificación que depende del contenido del derecho [350], es decir, del objeto o el valor que protegen y de la finalidad que se persigue con esa protección. En la opinión de este autor importante para la historia de los derechos fundamentales en España, la dignidad ser humano es la razón absoluta de la existencia de los demás derechos humanos. Los valores como la libertad, igualdad, seguridad y solidaridad incorporan los aportes liberales, socialistas y democráticos en una síntesis armoniosa e integral de la construcción de los derechos fundamentales derivados de tales valores.

En nuestra opinión, los derechos fundamentales no pueden distinguirse como derechos que implicarían exclusivamente un determinado tipo de obligación, la mayoría basada tanto en la actitud del estado ante la violación de un derecho como también en una actitud proactiva real de su parte, incluso si tuviéramos que referirnos estrictamente a una "provisión" de legislativa sobre las condiciones concretas en las que se puede ejercer un derecho fundamental. Esta clasificación es similar a la de Georg Jellinek[351], que, basado en el criterio funcional determinado por el estatuto del individuo, dividió los derechos en:

a. derechos que son defensivos para proteger una esfera de libertad en relación con el Estado ("status negativus");

b. derechos que requieren acción positiva, un beneficio estatal ("status positivus");

---

[349] Peces-Barba Martínez, G. (1995) *Curso de derechos fundamentales: teoría general*. Madrid: Universidad Carlos III de Madrid: Boletín Oficial del Estado, pp. 453-458.

[350] Los *derechos personalísimos*, tradicionalísimo denominados como derechos individuales, que protegen a la persona en sí, independiente de su vida social y de sus relaciones con los demás. Aquí se pueden mencionar el derecho a la vida, a la integridad física y moral, a la libertad ideológica y religiosa, al honor, a la propia imagen y el derecho de conciencia, entre otros.

Los *derechos de sociedad, comunicación y participación*, denominados también derechos civiles, derivados del carácter social del ser humano, protegen a la persona en el ámbito de la vida social. Entre estos derechos se encuentran, el derecho a la igualdad y a la no discriminación, la libertad de cultos, la inviolabilidad del domicilio, la libertad de expresión y de información, el derecho de asociación, etc.

Los *derechos políticos*, conocidos también como derechos de participación política, ofrecen al titular la posibilidad de participar en la formación de partidos políticos, en el proceso de gobernanza estatal, participando en las decisiones políticas y en los asuntos público. Estos derechos ofrecen al individuo la posibilidad de acceder en condiciones de igualdad a las funciones y cargos públicos.

Los *derechos de seguridad jurídica* tienen como principal objetivo proteger a la persona frente a las sanciones jurídicas, otorgándole garantías procesales para defender sus intereses y para formular eficazmente su pretensiones o defensas antes los tribunales. Podemos mencionar en esta categoría el derecho a la libertad y a la seguridad, así como los derechos integrantes del debido proceso o de la tutela jurisdiccional efectiva.

Los *derechos económicos, sociales y culturales* son aquellos que permiten crear condiciones para favorecer y hacer posible el libre desarrollo de la personalidad y que protegen determinadas dimensiones de la vida privada del individuo con contenido económico o cultural.

[351] Jellinek, G. (2005) *L'Etat moderne et son droit : Tome 1, Théorie générale de l'Etat*, Editorial Pantheon-Assas, p. 51-54

c. derechos que le permiten al individuo participar activamente en la formación de la voluntad del Estado ("status activus").

En una línea de pensamiento similar, usando el criterio de la relación del individuo con el Estado, los autores franceses[352] hicieron la siguiente clasificación en la que las primeras tres categorías corresponden a las categorías identificadas por Jellinek:

1. derechos-libertades ("status negativus");
2. derechos-participación ("status activus");
3. derechos- créditos ("estado positivo");
4. derechos - garantías;
5. el derecho a la igualdad.

La doctrina constitucional rumana propone las siguientes categorías[353], identificadas de acuerdo con otros criterios que se consideran más adecuadas para la clasificación de los derechos fundamentales:

A. *derechos inviolables/derechos de ámbito personal* que incluyen aquellos derechos destinados a proteger los elementos esenciales para la vida humana y su libre desarrollo (aquí se enmarca, por ejemplo, el derecho a la vida, la libertad individual, la libertad de circulación, el derecho a la privacidad, la familia y la vida privada);

B. *los derechos y las libertades socioeconómicas y culturales* que proporcionan las condiciones para una vida social y material, tales como el derecho a la educación, a la salud, derecho a un medio ambiente sano, el derecho a la propiedad, derecho al trabajo, derecho a un nivel de vida decente;

C. *los derechos políticos* que garantizan la participación ciudadana en el proceso gubernamental, tales como el derecho a votar y de ser elegidos;

D. *los derechos y las libertades sociopolíticos* que puede ser ejercitados de manera voluntaria para expresar la opinión sobre la solución de los problemas espirituales, sociales o políticas, en relación con los derechos como la libertad de conciencia, la libertad de expresión, derecho a la información, derecho de asociación;

E. *los derechos – garantías*, aquellos derechos constitucionales que protegen otros derechos, come es el derecho de petición de una persona afectada por una autoridad.

Desde la perspectiva histórica, los derechos fundamentales han evolucionado, en diferentes etapas la panoplia estos derechos se ha ampliado bajo la influencia de varios

[352] Favoreu, L. y otros (2008) idem., p. 88;
[353] Muraru, I. y Tanasescu, E.S. (2001) *Drept Constitutional si institutii politice (Derecho Constitucional e Instituciones Políticas)*, Volumen I, Edición 14, Editorial C.H. Beck, Bucarest, pp. 157-158.

factores sociales, políticos, económicos o tecnológicos. En este sentido, según el criterio temporal, los derechos fundamentales se pueden dividir en varias generaciones que ilustran la evolución del concepto de derechos humanos, debido a las diversas teorías filosóficas y doctrinas jurídicas[354].

Partiendo las disposiciones de la Declaración Universal de los Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos de 1966, la doctrina del derecho constitucional intentó una clasificación de los derechos fundamentales en tres generaciones de derechos, incluso cuatro (esta cuarta categoría ha aparecido en los últimos años), aunque algunos autores[355] son muy críticos con la numeración de las categorías de derechos, porque puede llevar a pensar en una cierta jerarquía de estos derechos e incluso un desplazamiento del interés hacia los derechos colectivos, que podría ascender a suprimir los derechos individuales.

A continuación, vamos a presentar brevemente a las cuatro categorías de derechos. La primera generación de derechos se refiere a los derechos civiles y políticos que han nacido como "*medidas para proteger al individuo contra la violencia y el arbitrario de los gobernantes absolutos, reclamando posiciones jurídicas iguales ante la ley*"[356]. Estos derechos se llaman "negativos" y son, en realidad, las libertades individuales (el derecho a la vida, la prohibición de la tortura, de la esclavitud y del trabajo forzado, la libertad de conciencia, el derecho a votar ya ser elegido etc.), a las que el Estado no debe tomar medidas concretas, sino solo abstenerse de violarlas; cada persona está naturalmente dotada con estos derechos y disfruta de la autonomía individual en su ejercicio, que debe ser protegida por el Estado con solo la autolimitación de sus acciones[357].

En la segunda generación de derechos mencionamos los derechos económicos, sociales y culturales (por ejemplo: derecho al trabajo, remuneración igual por prestaciones iguales, derecho a la seguridad social, derecho a un nivel de vida adecuado, derecho a la vivienda, el derecho a la educación, el derecho a participar en actividades

[354] Muraru, I. y Tanasescu, E.S. (2001) idem., p. 145;
[355] Bustamente Donas, J. (2001) *"Hacia la cuarta generación de Derechos Humanos: repensando la condición humana en la sociedad tecnológica"*, CTS+I: Revista Iberoamericana de Ciencia, Tecnología, Sociedad e Innovación, Nº.1/2001 (Ejemplar dedicado a: La sociedad de la información), pág. 3
[356] Vasak, K. (1984) "*Las dimensiones internacionales de los derechos humanos*", VOL. III, Editorial Serbal/Unesco Barcelona, p. 86;
[357] Vallespín Pérez, D. (2002) "*El modelo constitucional de juicio justo en el ámbito del proceso civil", Editorial Atelier Barcelona, pp. 31-32;*

culturales y deportivas etc.), que requieren acciones concretas por parte del Estado para garantizarlas, para lo cual también se les han llamado "derechos positivos"[358].

La tercera generación de derechos[359] se ha afirmado desde la segunda mitad del siglo XX y también se llama "derechos de solidaridad", ya que solo pueden ser garantizados mediante la cooperación entre los Estados. La teorización de estos derechos (derecho a la paz, derecho al desarrollo, derecho a un medio ambiente sano etc.) es objeto de disputas doctrinales, dada la naturaleza jurídica de estos derechos, muchos de ellos derivados de los instrumentos jurídicos internacionales en los que los sujetos de derecho son los Estados, no el individuo.

Por lo tanto, se argumenta que algunos de estos derechos deben ser miradas con reservas "*ya sea porque introducen la improvisación en este campo tan delicado y tan bien definido, ya sea porque, en un estudio cuidadoso de sus implicaciones, se descubre que no sirven realmente a la causa en cuyo nombre se proclaman, es decir, la libertad humana y la personalidad*"[360].

En una cuarta generación de derechos[361], cuya aparición está determinada por la influencia de las nuevas tecnologías de la información y la comunicación en la vida humana y, por tanto, de origen muy reciente, se destacan el derecho a la privacidad y el derecho a la protección de los datos personales[362].

Se habla también de otras "creaciones", que gozan del mismo régimen que los derechos humanos, pero que son muy cuestionable en cuanto a sus calificaciones legales (el derecho a ser dejado solo, derecho a la nostalgia, el derecho a no ser asesinado en la guerra, el derecho al turismo etc.). Otro derecho polémico, es el derecho a la libre determinación, que, aunque se encuentra en la mayoría de los instrumentos legales que rigen los derechos humanos, se considerar más bien como un derecho colectivo que no se puede ejercer individualmente. Sin dar una respuesta categórica a la disputa sobre la caracterización de la autodeterminación como un derecho humano y un requisito previo

---

[358] Pérez Luño, A. E. (1991) "*Estado constitucional y derechos de la tercera generación*", Anuario de Filosofía del Derecho, Tomos XIII-XIV, pp. 513.

[359] Morello, A. M. (1994) "*El proceso justo. Del garantismo formal a la tutela judicial efectiva de los derechos*", Editorial Platense/Abeledo-Perrot, La Plata, pp. 88-ss.;

[360] Muraru, I. y Tanasescu, E.S. (2001) *Drept Constitutional si institutii politice (Derecho Constitucional e Instituciones Políticas)*, Volumen I, Edición 14, Editorial C.H. Beck, Bucarest, p. 144;

[361] En relación con la cuarta generación de derechos, Jean-François Renucci afirma que estos derechos están destinados a proteger la dignidad humana, considerada fundamental para todos los demás derechos, de ciertos abusos de la ciencia - Renucci, J.-F. (2009) *Tratado de derecho europeo de derechos humanos*, Hamangiu Publishing House, Bucarest, p. 81.

[362] Warren, S. D. y Brandeis, L. D. (1890). *The Right to Privacy*. Harvard Law Review, Vol. 4, No. 5, pp. 193-220

para todos los derechos humanos, algunos autores incluyen la autodeterminación entre los principios básicos de los derechos humanos, como la igualdad y la no discriminación[363].

Todos los tipos de clasificación presentados anteriormente son importantes para el desarrollo de este trabajo y se considerarán al analizar el derecho a la privacidad y el derecho a la seguridad cibernética, derechos que forman parte de la última generación de derechos identificados por la doctrina. De manera similar, la caracterización legal de estos dos derechos seguirá los criterios generales establecidos en este primer capítulo para verificar su carácter fundamental en diferentes contextos, según las características identificadas anteriormente.

Podemos concluir que los diferentes derechos son solo facetas de la libertad fundamental del individuo. La doctrina admite por unanimidad que existe un núcleo duro o un derecho-causa que determina el desarrollo de los demas derechos fundamentales. Algunos autores consideran que este es el derecho a la vida, otros consideran que la dignidad humana es el núcleo duro, otros anteponen la libertad del individuo. Desde un punto de vista científico, cualquier clasificación, ya sea doctrinal o jurídica, es insuficiente, porque ninguna puede formarse un cuadro claro y completo de los múltiples elementos que conforman el concepto y las formas de ejercicio y protección de cada uno de los derechos.

4.4. El marco jurídico relativo a los derechos fundamentales

4.4.1. El reconocimiento de los derechos fundamentales al nivel estatal

Desde un punto de vista histórico, es difícil estimar el momento original de la afirmación consciente de los derechos humanos, pero se sabe que desde la antigüedad se ha planteado la cuestión del reconocimiento de los derechos individuales. Sin derechos reconocidos, incluso en forma consuetudinaria, no se puede hacer justicia. El más antiguo tratado conocido, concluido entre Ramsés II y el príncipe de Cheta (siglo 13), registró algunas reglas con respecto a la prohibición de asilo y tratamientos crueles. El mismo Aristóteles, hablando de igualdad y equidad, se refiere a los derechos - el derecho a la igualdad: "*porque la igualdad y la desigualdad total son injustas entre individuos que no*

[363] Partsch, K. J. (1978) *Les principes de base des droits de l'homme : l'autodétermination, l'égalité et la non-discrimination,* en "Les dimensions internationales des droits de l'homme", Paris, UNESCO, p. 74

son iguales o desiguales solo en un aspecto, todas las sociedades, en las que la igualdad y desigualdad se basa en tal fundamento, son necesariamente corruptas"[364].

De hecho, en la bien conocida definición de hombre como "ser social" (*zoon politikon*), Aristóteles incluyó el derecho a la igualdad considerado como "*la vocación ilimitada que todos los hombres deben disfrutar para participar en condiciones de plena igualdad en la gestión de los asuntos de la ciudad*"[365].

Sin embargo, en la antigua democracia de Atenas, el individuo no disfrutaba en realidad de todos los derechos reconocidos por el estado como intangibles. También los fundadores de la ley romana, de la que se extrae el derecho civil moderno, distinguen entre ley civil y ley natural, mostrando que la primera es aplicable solo a los miembros de la ciudad considerados como iguales, mientras que la segunda es válida para todos los seres humanos, independientemente de su condición de personas libres o esclavos[366].

Gradualmente, la religión cristiana tuvo un papel beneficioso al afirmar la igualdad de las personas ante la Divinidad y promover la tolerancia mutua, aunque en la Edad Media (Inquisición) la religión se transformó en un instrumento usado para el Poder, el binomio Iglesia-Estado, contra el individuo que quería ejercer por derecho propio la libertad de conciencia y la libertad de expresión. Al mismo tiempo, las monarquías absolutas se caracterizaron por la disposición discrecional del monarca sobre la seguridad personal y la propiedad privada del individuo.

Las ideas renacentistas han influencia las concepciones humanistas que han devuelto al hombre su estatuto dentro de los límites de los valores con los que estaba dotado. A partir de ahí, se originaron y luego desarrollaron las grandes ideas de la Revolución Francesa de 1789, que sentaron las bases para una nueva era en la emancipación del individuo libre de toda restricción y dotado de derechos inalienables e inviolables. Los conceptos legales de los derechos humanos comenzaron a manifestarse en el siglo XVIII, y la Revolución Francesa impulsó e impuso algunos principios fundamentales que rigen las teorías de los derechos humanos que han resistido hasta la hora, debido a su validez universal e intemporal[367].

En este contexto político e histórico, Montesquieu ha demostrado que la libertad es "*el derecho a hacer todo lo que permite la ley, y si un ciudadano puede hacer lo que*

[364] Aristóteles (1988) *Política*, Editorial Gredos Madrid, p. 20
[365] Aristóteles (1988) idem, p.14.
[366] Girard, P.F., (1924) *Manuel élementaire de Droit Romain*, Librairie Arthur Rousseau, Paris, p. 2-3.
[367] Roche, J. (1981) *Libertes publiques,* Editorial Dalloz, 6ª ed. Paris.

prohíbe, ya no tendrá libertad, porque todos los demás podría hacer lo mismo"[368]. Así se ha teorizado el vínculo indisoluble que debe existir entre el mantenimiento del estado de derecho y la garantía de los derechos humanos.

Los derechos de un individuo acaban donde y cuando comienzan los derechos y las libertades de los demás, y es necesario mantener la autolimitación en el ejercicio de los derechos sin los cuales la anarquía podría establecerse en una sociedad humana. Como decía el gran filósofo Gregorio Peces Barba:

> *"Frente a la idea del odio como motor de la vida pública, en la sociedad democrática, la amistad cívica, el respeto al otro, la tolerancia, la participación en empresas comunes, necesitan la concurrencia de ambos"*[369].

Desde el punto de vista de los defensores de la ley natural, la libertad del individuo debe ser respetada, ya que ha nacido con este valor innegable, y sobre esta base la libertad, la igualdad y los derechos de propiedad no pueden transmitirse al Estado. Además, si los líderes de una sociedad no respetan el "pacto fundamental" concertado entre los ciudadanos y sus representantes políticos, a través del cual se fundaron las instituciones políticas y el Estado, se reconoce el derecho de los ciudadanos a eliminarlos, es decir, la ley es legítima a la rebelión.

> *"Lo más necesario y quizás lo más difícil del gobierno es esa severa integridad que busca la justicia para todos y principalmente la protección del pobre contra la tiranía del rico"*[370].

A partir de ideas filosóficas sobre los derechos, algunas de ellas con valor programático, los estados han establecido a través de instrumentos de valor político y legal el reconocimiento y salvaguardia de los derechos individuales, junto con la declaración del estado de derecho y la adopción de constituciones. El primer documento constitucional emitido en Inglaterra es Magna Charta Libertatum en 1215, editado por Juan I de Inglaterra, donde se estipulaba el derecho de las personas libres a ser juzgadas de acuerdo con la ley antes de tomar una medida contra ellas. Inglaterra también adoptó otros actos legales pioneros en Europa que contienen disposiciones de derechos humanos ("Petition of Rights" -1628, "Habeas Corpus Act" -1679, "Bill of Rights" -1689), que se

[368] Charles-Louis de Secondat Baron de La Brède et de Montesquieu (1964) *El Espiritu de las Leyes*, Vol. I, Editorial Científica, Bucarest, 1964, p. 193

[369] Peces-Barba, G. (1993) *El derecho y el amor: sus modelos de relación*, en Derecho y derechos fundamentales, Centro de Estudios Constitucionales, Madrid, p. 237.

[370] Rousseau, J. J. (2005) *Discurso sobre economía política*, Editorial Tecnos Madrid, p. 39

consideran las primeras manifestaciones de la idea de codificar todos los derechos públicos del individuo[371].

Sobre la base de estos actos, se ha reafirmado la libertad de expresión, los debates públicos sobre las leyes, el derecho de los ciudadanos a presentar peticiones al rey, la libertad de la opinión se ha garantizado los derechos de propiedad, el sistema de jurados, todos los derechos individuales que se oponen al Estado. El poder ejecutivo ha proporcionado protección y garantías procesales diseñadas para evitar el daño de estos derechos; sobre la base de estos principios, junto con la separación del poder ejecutivo y legislativo y la organización de una justicia independiente, se establecieron las etapas esenciales para la creación del estado de derecho[372] ("rule of law").

Quizás el documento más conocido, una referencia para muchos actos emitidos posteriormente en otros estados, es la Declaración de los Derechos del Hombre y del Ciudadano ("*Déclaration des droits de l'Homme et du Citoyen*"), de Francia, 1789. Desde el primer párrafo, la Declaración establece que "*los hombres nacen y permanecen libres e iguales en derechos. Las distinciones sociales sólo pueden fundarse en la utilidad común*". El objetivo de cualquier asociación política es "*la protección de los derechos naturales e imprescriptibles del Hombre. Tales derechos son la libertad, la propiedad, la seguridad y la resistencia a la opresión*". Estas ideas han sido valoradas por los teóricos del Derecho natural y han determinado una verdadera revolución en la proyección que los derechos en el valor intrínseco del individuo.

Se trata de derechos que, en términos de I. Kant, "*independientemente de un acto jurídico, son transmitidos a cada individuo por la naturaleza*"[373]. Estos derechos que el hombre puede oponer a la autoridad del Estado, o en contra de los privilegios corporativos y clericales, ayuda al individuo desarrollarse libremente en la sociedad, en la relación con los demás seres humanos, usándolos en contra las prerrogativas económicas y sociales del derecho privado[374].

Trece años antes que se afirmaron en Francia la libertad y la igualdad, en los Estados Unidos de América, a través de la Declaración de Estado de Virginia (1776) y la Declaración de Independencia de los Estados Unidos (1776) se proclamaba:

---

[371] Jellinek, G. (2005) *L'Etat moderne et son droit : Tome 2, Théorie juridique de l'Etat*, Editorial Pantheon-Assas París, p. 42

[372] Draganu, T. (1992) *Introducere în teoria și practica statului de drept* (*Introducción en la teoría y la práctica del estado de derecho*), Editorial Dacia Publishing House, Cluj-Napoca, p.15;

[373] Kant, I. (1873) *Principios Metafísicos del Derecho*, Editorial Kessinger Publishing, pag 96.

[374] Julio Estrada, A. (2000) *La eficacia de los derechos fundamentales entre particulares,* Universidad Externado de Colombia, p. 31.

"que todos los hombres son creados iguales; que son dotados por su Creador de ciertos derechos inalienables; que entre éstos están la vida, la libertad y la búsqueda de la felicidad".

También, la declaración subrayaba la libertad política, que según J. J. Rousseau, representa el derecho de los ciudadanos de cambiar una forma de gobierno que no respeta los derechos de las personas.

Al comparar los sistemas de derecho francés y estadounidense, en comparación con el inglés, notamos que se ha mantenido el vínculo causal inverso entre la consagración de los derechos fundamentales y la adopción de una constitución. A diferencia de los Estados Unidos y los estados europeos, donde las constituciones escritas crearon los derechos y libertades fundamentales de los ciudadanos, en Inglaterra, estos derechos aparecieron por primera vez con la Carta Magna Libertatum en 1215, solo después de haber sido reconocidos por actos legales y consolidado a través de una práctica judicial constante[375].

Basándose en los modelos creados en estos sistemas de derecho, los derechos fundamentales fueron consagrados posteriormente en el orden legal de otros estados, dentro de sus leyes constitucionales, por medio de las reformas políticas, económicas, sociales y legislativas implementadas al nivel de cada estado (la Constitución belga de 1831 proporcionó una lista que fue un modelo para otros estados, la Constitución española de 1812 no incorporó una tabla de derechos y libertades, pero sí recogió algunos derechos dispersos en su articulado, incluyendo Rumania cuando adoptó la Constitución de 1866 - Título II "Sobre los derechos de los rumanos").

Las guerras civiles y las revoluciones modernas del siglo XX que han determinado la reorganización política de algunas regiones y el cambio en los regímenes políticos también han causado la afirmación de los derechos fundamentales como un símbolo de la victoria del individuo ante el poder público. La evolución histórica de los derechos humanos ha llevado a su clasificación en varias categorías determinadas por el momento de su reivindicación y reconocimiento legal, pero también por los objetivos perseguidos, las llamadas "generaciones de derechos", sin darse cuenta de que su heterogeneidad tendría el efecto de negar el principio la indivisibilidad de los derechos como un todo[376].

[375] Draganu, T. (1992) idem. p.98
[376] Muraru, I. y Tanasescu, E.S. (2001) *Drept Constitutional si institutii politice (Derecho Constitucional e Instituciones Políticas)*, Volumen I, Edición 14, Editorial C.H. Beck, Bucarest, p. 143;

Desde esta perspectiva, es interesante observar cómo en algunos sistemas jurídicos los derechos naturales transgredieron con el tiempo esta condición primaria, convirtiéndose en libertades públicas, y luego en derechos fundamentales. El término "libertades públicas", específico al derecho francés, fue consagrado por la Asamblea Nacional Francesa durante la proclamación de la Tercera República y representa el régimen legislativo de los derechos individuales y su clasificación legal de acuerdo con el principio general de que "solo la ley determina las condiciones del ejercicio de la libertad, marcando exclusivamente sus límites"[377].

Basado en la filosofía de los derechos naturales, que protege la existencia de la libertad como fundamento de la autonomía del individuo frente a las autoridades, la consagración de los derechos públicos subjetivos en la legislación alemana es el punto de partida para su estatus constitucional, justificando el recurso judicial de cualquier individuo "*herido por el poder público en sus derechos*"[378].

Bajo la influencia alemana, el sistema legal francés adoptó terminológicamente la noción de "derechos fundamentales" para designar el fenómeno de la constitucionalización de los derechos individuales, duplicado por el control constitucional, como elementos de mayor protección legal.

La noción de "derechos fundamentales" está ahora ampliamente difundida y aceptada por los estados democráticos para caracterizar un conjunto limitado de derechos, generalmente establecidos bajo la influencia de desarrollos internos, pero también para armonizar las regulaciones nacionales con aquellas derivadas de la ley generada por las organizaciones internacionales. Se puede decir que es difícil crear un catálogo completo y definitivo de derechos fundamentales porque la dinámica de los fenómenos puede generar la aparición y consagración de nuevos derechos; tal desarrollo es progresivo, en el sentido de que los derechos ya reconocidos no caen en desuso, y hay siempre un núcleo duro de derechos fundamentales (especialmente de la primera generación) que permanece sin cambios.

[377] Stone, N. (1985) *La Europa transformada, 1878-1919*. Siglo Veintiuno Editores, México.
[378] De acuerdo con la doctrina alemana, la posibilidad de emprender acciones legales es el elemento que respalda la existencia de cualquier categoría de derechos individuales - Draghici S. (2009) *Derechos fundamentales entre la definición y los efectos legales*, en "The New Journal of Human Rights", no. 1/2009, p. 58.

En la doctrina jurídica española[379] como también en la doctrina alemana[380] se han formado dos corrientes de opinión que disputan entre la teoría de la eficacia directa y la teoría de la eficacia indirecta de los derechos fundamentales en las relaciones jurídicas entre particulares.

Los autores que abogan por la teoría de la eficacia directa[381], consideran que la mayor parte de los derechos fundamentales están dotados de eficacia inmediata en las relaciones horizontales (inter privados), porque tienen la capacidad de vincular a los particulares directamente, sin la intervención de los poderes legislativos o judiciales. Se trata del efecto irradiante de los derechos y los impulsos a los poderes públicos.

La doctrina que sostiene la teoría de la eficacia indirecta[382] de los derechos fundamentales consideran que estos sólo vinculan a los titulares de forma mediata o indirecta (interpositio legislatoris o interpositio iudicis). Según esta tesis los derechos fundamentales gozan de efectividad solo si los poderes públicos reconocen, a través de leyes o jurisprudencia, su contenido y su alcance. Entonces podemos decir que, según la tesis mediada, la colaboración entre legislador y juez es vital para la existencia y protección de un derecho fundamental porque el primero define y regula y el segundo interpreta la ley, extendiendo sus efectos sobre el vacío legislativo que puede ser generado por la falta de atención del primer actor. En estas situaciones, el juez resuelve el caso utilizando el principio de proporcionalidad o extrayendo las características y partes análogas de los derechos fundamentales, considerados como valores superiores a la normativa de derecho privado[383].

Es cierto que la Constitución Española no contiene un artículo en el que se reconozca claramente la eficacia horizontal de los derechos fundamentales, de la misma manera que la Constitución Portuguesa[384] en su artículo 18.1 menciona que "*los preceptos relativos a los derechos, libertades y garantías son directamente aplicables a las*

---

[379] Bastida Freijedo, F. J. y otros (2004) *Teoría General de los Derechos Fundamentales en la Constitución Española De 1978*, Editorial Tecnos Madrid; Bilbao Ubillos, J. M. (1997) *La eficacia de los derechos fundamentales frente a particulares. Análisis de la jurisprudencia del Tribunal Constitucional*, Centro de Estudios Políticos y Constitucionales, Madrid, p. 852

[380] Wilhelm Gerber, C. F. (1852) *Über öffentliche Rechte*, Tubingen, Laupp; Schoditsch, T.(2019) *Grundrechte und Privatrecht*, Editorial Verlag Österreich.

[381] Anzures Gurría, J. J. (2010). La eficacia horizontal de los derechos fundamentales. *Cuestiones constitucionales*, (no. 22), pp. 3-51;

[382] Aragón Reyes, M. (1997) *La interpretación por el Tribunal Constitucional de la legalidad constitucional y su fuerza vinculante* en Revista Estudios Jurídicos, Año 2007, Número 2007;

[383] Naranjo de la Cruz, R. (2000) *Los límites de los derechos fundamentales en las relaciones particulares: la buena fe,* Centro de Estudios Políticos y Constitucionales.

[384] El texto es disponible en: https://constituteproject.org/constitution/Portugal_2005.pdf?lang=es.

entidades públicas y privadas y vinculan a éstas". Tampoco no existe una "*acción de tutela"* similar al sistema constitucional colombiano que ofrece una protección efectiva del derecho fundamental en caso de violaciones cometidas por las autoridades o por particulares.

Al mismo tiempo, tal como el profesor Peces-Barba observa, tampoco existe alguna mención en la Constitución Española que niega la *eficacia inmediata* de los derechos fundamentales. En su opinión es necesario interpretar su contenido de modo harmónico y holístico, para sorprender y destacar las provisiones legales que sustenten la eficacia horizontal de los derechos[385].

Algunos autores[386] sostienen que si analizamos con atención podemos encontrar suficientes argumentos para demonstrar que los derechos tienen una eficacia horizontal y pueden ser aplicados de forma inmediata, solo si la interpretación de su proprio significado permite este efecto directo en las relaciones entre particulares o entre el individuo y las autoridades.

En este sentido mencionamos el artículo 1.1. Constitución, que declara como valores superiores de todo ordenamiento jurídico español "*la libertad, la justicia, la igualdad y el pluralismo político*", subrayando la dimensión objetiva de los derechos fundamentales.

En la misma línea de interpretación también podemos mencionar que el artículo 9.1 de la Constitución coloca en la misma categoría de sujetos legales tanto a los poderes públicos como también a los ciudadanos como. La idea de la eficacia directa se sostiene incluso por las provisiones del artículo 9.2 de la Constitución: "*corresponde a los poderes públicos promover las condiciones para que la libertad y la igualdad del individuo y de los grupos en que se integra sean reales y efectivas; remover los obstáculos que impidan o dificulten su plenitud y facilitar la participación de todos los ciudadanos en la vida política, económica, cultural y social*".

Por último, el artículo 10.1 señala que: "*la dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social*", estableciendo que el orden jurídico y social de la comunidad humana no puede existir sin el reconocimiento de ciertos valores inherentes al ser humano.

---

[385] Peces-Barba Martínez, G. (1995) *Curso de derechos fundamentales: teoría general*. Madrid: Universidad Carlos III de Madrid: Boletín Oficial del Estado.
[386] Naranjo de la Cruz, R. (2000) *idem*.

Como conclusión podemos afirmar que la Constitución Española de 1978 contiene disposiciones suficientes para confirmar la teoría de que los derechos fundamentales tienen una eficacia horizontal en el ordenamiento jurídico español. Si bien existen derechos fundamentales con mayor eficacia entre los particulares, como por ejemplo el derecho al honor, a propria imagen, a la intimidad, a igualdad, al mismo tiempo existen derechos constitucionales que necesitan la intervención de las autoridades para su efectiva eficacia.

Esta obligación para el estado de crear y aplicar mecanismos de protección efectiva incluye la implementación de garantías normativas que impiden lesionar los derechos fundamentales por las autoridades estatales o por los particulares (por ejemplo, mediante la previsión de sanciones penales). El objecto del derecho fundamental, su valor intrínseco, debe ser definido jurídicamente con el fin de facilitar su ejercicio. La norma que regula un derecho fundamental debe otorgar a los particulares un derecho de prestación, es decir, un derecho a obtener de los poderes públicos los medios materiales necesarios para poder ejercitarlo[387].

La Constitución rumana de 1991, republicada, está estructurada, en general, de acuerdo con la clasificación de los derechos y libertades fundamentales prevista por los Pactos internacionales sobre derechos civiles y políticos, los derechos económicos, sociales y culturales.

Un análisis general de los derechos fundamentales y los principios que los gobiernan demuestra que su garantía no puede limitarse a su consagración constitucional, sino que es necesario establecer procedimientos concretos para permitir su implementación efectiva. El principio que consagra el acceso igual de las personas a los derechos y libertades fundamentales también implica el establecimiento de garantías constitucionales, de modo que la realización de algunos derechos no sea en detrimento de otros. Desde este punto de vista, resulta la necesidad de una regulación unitaria del sistema de derechos, que también debería considerar un sistema de condicionamiento reciproque. El artículo 16 de la Constitución de 1991, republicada, establece dos principios fundamentales del estado de derecho, a saber: "*Nadie está por encima de la ley*" (Párrafo 2) y "*Los ciudadanos son iguales ante la ley y las autoridades, sin privilegios ni discriminación"* (Párrafo 1). También, el art. 1 párrafo 1 establece con

[387] Bastida Freijedo, F.J. y otros (2004) *Teoría General de los Derechos Fundamentales en la Constitución Española De 1978*, Editorial Tecnos Madrid, p. 188.

carácter general que "cualquier persona puede dirigirse a la justicia en defensa de sus derechos, libertades e intereses legítimos" y que "ninguna ley puede impedir el ejercicio de este derecho" (párrafo 2). Estos dos textos se refieren solo a la posibilidad de igualdad de acceso a la justicia, lo que realmente se puede lograr, siempre que los ciudadanos no se desanimen por los impuestos y tasas demasiado altas en relación con sus posibilidades. En el siguiente párrafo del art. 1, se estipula que "las partes tienen derecho a un juicio justo y a la solución de los casos en un plazo razonable" (párrafo 3). Esta regulación no se beneficia de las garantías apropiadas, considerando que estas normas permanecen al nivel de las decisiones, para numerosos casos que llegan a los tribunales. Es cierto que la disposición constitucional sobre el derecho a un juicio justo se complementa con las disposiciones del art. 124, que menciona que "la justicia es única, imparcial e igual para todos" (párrafo 2) y que "los jueces son independientes y están sujetos solo a la ley" (párrafo 3).

Analizando lo expuesto anteriormente podemos concluir que la Constitución rumana reconoce la eficacia horizontal de los derechos fundamentales en el ordenamiento jurídico interno y ofrece un mínimo conjunto de garantías jurisdiccionales para una protección efectiva del ejercicio de estos derechos y libertades.

4.4.2. Marco regulatorio europeo relativo a los derechos fundamentales

La Unión Europea fue creada y desarrollada principalmente como una organización centrada en proteger los intereses económicos de los Estados miembros con prioridad ante otros objetivos, abordando al individuo más bien desde una perspectiva instrumentalista o funcionalista. En este caso, las cuestiones políticas como aquellas destinadas a defender los derechos fundamentales de los ciudadanos de los estados miembros quedaron en un segundo plan. Además, los tratados constitutivos no contienen disposiciones expresas a tal efecto, siendo el Tribunal de Justicia de Luxemburgo el responsable del enfoque integrador de las Comunidades Económicas Europeas sobre las cuestiones de derechos humanos.

Tras un comienzo más vacilante, el Corte comunitario los incluyó, a falta de disposiciones escritas, en los "principios generales del derecho"[388]. La posición del Corte

[388] En el caso 29-69 (Sentencia del Tribunal de Justicia de 12 de noviembre de 1969, Erich Stauder v. El Municipio de Ulm - Sozialamt, publicado en Rep. 1969 00419, ECLI: EU: C: 1969: 57), el Tribunal se refirió a los derechos humanos fundamentales como parte de los principios generales del derecho comunitario, protegidos por este tribunal, aunque evitó mencionar exactamente a qué derecho fundamental se refería en dicha sentencia.

es una reacción indirecta para declarar la preeminencia del derecho comunitario sobre los tribunales constitucionales de algunos Estados miembros que rechazaban la efectividad de las normas comunitarias porque no ofrecían garantías satisfactorias en el ámbito de los derechos humanos.

El papel creativo de T.J.C.E./T.J.U.E. (forma de "activismo judicial"[389]) no se limitó a reconocer la importancia de los derechos fundamentales en el orden jurídico autónomo de la UE, sino que se demostró al establecer un catálogo de derechos coleccionados de las tradiciones constitucionales de los Estados miembros o del derecho internacional público. En este contexto, el Tribunal de Luxemburgo ha recurrido con frecuencia a referencias en la jurisprudencia del T.E.D.H. y a las disposiciones del Convenio Europeo de Derechos Humanos (C.E.D.H.) reconocidas como un estándar mínimo de protección de los derechos fundamentales[390].

Por otro lado, al momento de expresar su opinión sobre la propuesta de adhesión de la UE. al Convenio, en el período previo al Tratado de Lisboa, T.J.C.E. se opuso. En el aviso no. 2/1994[391] el Tribunal ha demostrado que garantizar la protección de los derechos humanos es una condición para la legalidad de la acción comunitaria, aunque no existen disposiciones expresas en los Tratados que confieran a las instituciones comunitarias el poder general para adoptar normas en el campo de los derechos humanos o para concluir acuerdos internacionales en este ámbito. El Tribunal consideró que la adhesión al Convenio traería consigo un cambio importante en el actual sistema comunitario de protección de los derechos humanos que tendría el efecto de vincular a la Comunidad con un sistema de derecho internacional público totalmente diferente del aquis comunitario. En consecuencia, el T.J.C.E. rechazó la aprobación positiva del proyecto del Consejo, señalando que tal cambio de valor constitucional solo es posible si se cambian las condiciones del Tratado constitutivo de la Comunidad.

La demora en el proceso de negociación del proyecto de tratado de adhesión de UE al Convenio es testigo de la dificultad de asimilar e integrar un sistema legal paralelo

---

[389] Craig, P. y de Búrca, G. (2011) *EU Law: Text, Cases, and Materials*, Editorial OUP Oxford; 5 edicion;
[390] Hay muchas causas en las que T.J.C.E./T.J.U.E. recurso a las disposiciones del Convenio y la jurisprudencia del T.E.D.H., uno de los más recientes y representativos es el asunto C-229/05 P, sentencia del Tribunal de 18 de enero de 2007, Osman Ocalan, en nombre del Partido de los Trabajadores del Kurdistán (PKK) y Serif Vanly en el nombre de Kurdistan National Congress (KNK) contra Consejo de la Unión Europea (publicado en Rep. 2007 I-00439, ECLI: EU: C: 2007: 32).
[391] Disponible en: https://curia.europa.eu/jcms/upload/docs/application/pdf/2010-01/tra-doc-ro-avis-c-0002-1994-200802181-05_00.pdf

al derecho comunitario, con sus propias normas, órganos y especialmente la jurisdicción supranacional (en este caso, supracomunitario).

En su jurisprudencia reciente, el T.J.U.E. reafirmó que, mientras la Unión no se haya adherido al Convenio, esto no es un instrumento jurídico legalmente integrado en el sistema legal de la Unión. Por lo tanto, "la ley de la Unión Europea no puede regir la relación entre el Convenio y los sistemas legales de los Estados miembros, ni puede determinar las consecuencias que debe dictar el tribunal nacional en caso de conflicto entre los derechos garantizados por esa convención y una norma de derecho nacional"[392].

Comenzando con el Acta Única Europea[393], pero especialmente después de los cambios en los tratados de Maastricht[394] y Ámsterdam[395], la entidad recién creada, la Unión Europea, adquirió un componente político democrático muy fuerte, con la afirmación de la ciudadanía europea y los elementos que componen su estatuto. La tercera frase del preámbulo del Acta declara la intención clara de los estados signatarios de reforzar el marco jurídico relativo a los derechos humanos:

---

[392] Causa C-617/10 - Sentencia del Tribunal de Justicia (Gran Sala) de 26 de febrero de 2013; Åklagaren contra Hans Åkerberg Fransson. Petición de decisión prejudicial planteada por el Haparanda tingsrätt. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A62010CJ0617

[393] El Acta Única Europea (AUE) tenía por objetivo "revisar los Tratados de Roma, constitutivos de la Comunidad Económica Europea (CEE) y la Comunidad Europea de la Energía Atómica. Esto se hizo para reactivar la integración europea y completar el mercado interior (un espacio libre de fronteras interiores y donde hay libertad de circulación de mercancías, personas, servicios y capital) hasta el 1 de enero de 1993". El Acta ha modificado el modo de organización de las instituciones europeas y ha cambiado sus funciones en diversos ámbitos políticos. Creando e impulsionado nuevas competencias de la Comunidad y reformando sus instituciones, el AUE ha contribuido efectivamente a la integración política de los estados miembros y a la creación de la unión económica y monetaria, que quedarían instituidas por el Tratado de la Unión Europea (el Tratado de Maastricht). Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:11986U/TXT&from=ES

[394] El Tratado de la Unión Europea (TUE), conocido también como "Tratado de Maastricht" por haber sido firmado el día 7 de febrero 1992, en esa localidad holandesa, constituye "una piedra angular en el proceso de integración europea, pues, al modificar y completar al Tratado de Paris de 1951 que creó la CECA, a los Tratados de Roma de 1957 que instituyeron la CEE y el EURATOM, y al Acta Única Europea de 1986, por primera vez se sobrepasaba el objetivo económico inicial de la Comunidad (construir un mercado común) y se le daba una vocación de unidad política". El Tratado de Maastricht consagra oficialmente el nombre de "Unión Europea" que sustituye al de Comunidad Europea. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:11992M/TXT&from=RO.

[395] El Tratado de Ámsterdam resulto de los debates de la Conferencia Intergubernamental de Turín (Italia) con la intención de revisar el Tratado de la Unión Europea. Aprobado por el Consejo Europeo de Ámsterdam (16 y 17 de junio de 1997) y firmado el 2 de octubre de 1997 por los ministros de Asuntos Exteriores de los quince países miembros de la Unión Europea, el tratado entró en vigor el 1 de mayo de 1999. Como documento jurídico, este tratado modifica ciertas disposiciones del Tratado de la Unión Europea, de los tratados constitutivos de las Comunidades Europeas (Paris y Roma) y de algunos actos relacionados con los mismos. No sustituye a los tratados anteriores, sino que se les añade.
Texto disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:11997D/TXT

"*DECIDIDOS a promover conjuntamente la democracia basándose en los derechos fundamentales reconocidos en las Constituciones y leyes de los Estados miembros en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y en la Carta Social Europea, en particular la libertad, la igualdad y la justicia social*".

También, los dos últimos tratados europeos han declarado en su propio texto el compromiso de la Unión de respetar los derechos fundamentales, como principios generales del derecho de la Unión, adoptando normas de derecho positivo para invertir al Tribunal de Justicia de Luxemburgo con el poder de garantizar la protección de estos derechos, otorgando valor legal a un estado de hecho preexistente. El reconocimiento de un conjunto de derechos fundamentales dentro de este sistema normativo revela la intención de los Estados miembros de otorgar un mayor grado de legitimidad democrática y constitucional a esta organización de integración internacional.

Con la entrada en vigor de la Carta[396] y al invertir el Tratado de Lisboa[397] con la fuerza jurídica de los tratados constitutivos de la Unión, se abre una nueva etapa en la construcción política, jurídica y económica de la comunidad, colocando la protección de los derechos humanos en el núcleo fuerte de la legislación europea. Presenta importancia para nuestro análisis las provisiones del artículo 6 de la Carta: *"Toda persona tiene derecho a la libertad y a la seguridad"*. Es la primera vez cuando el derecho a la seguridad de la persona está reconocido como derecho fundamental del ser humano, al nivel europeo, en un documento con tal fuerza jurídica.

A partir de este momento, la U.E. tiene su propio catálogo escrito de derechos, considerado enriquecido, diversificado y modernizado incluso en referencia al Convenio del Consejo de Europa, pero no abandonado como un instrumento externo de interpretación en el campo de los derechos humanos (las explicaciones a la Carta se refieren directamente al Convenio y la interpretación dado a ellos por el T.E.D.H.). En

[396] La Carta de los Derechos Fundamentales de la Unión Europea es un documento que contiene provisiones de derechos humanos y fue proclamado por el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea el 7 de diciembre de 2000 en Niza.
El texto es disponible en: https://www.europarl.europa.eu/charter/pdf/text_es.pdf

[397] El Parlamento Europeo adoptó el Tratado de Lisboa el 19 de febrero de 2008 (informe Corbett/Méndez de Vigo). El Tratado de Lisboa confiere al Parlamento el derecho a nombrar al presidente de la Comisión a propuesta del Consejo Europeo, que ha de en cuenta los resultados de las elecciones al Parlamento Europeo. La codecisión se amplía a nuevos ámbitos y pasa a denominarse "procedimiento legislativo ordinario". Texto disponible en:
https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=OJ:C:2007:306:FULL&from=ES

la actualidad, incluso se puede afirmar la existencia de una equivalencia de sistemas de protección de derechos, traducida también en la colaboración entre T.E.D.H. y el T.J.U.E., ambos asegurando el cumplimiento del principio de protección judicial efectiva. Cada vez hay menos "voces" que afirman que la protección de los derechos fundamentales socavaría la libertad contractual en las relaciones comerciales de la UE, que ahora se considera parte de la exitosa integración económica y política de los estados miembros de la UE[398].

En el intento unánime de reducir el déficit democrático de la organización, la Carta desempeña un papel clave en el proceso deseado de constitucionalización de la legislación de la UE, al enfatizar el carácter político de la Unión. La adopción de la Carta tenía la intención de acercar a los ciudadanos a la UE, al reconocer derechos importantes, ya sean libertades individuales, derechos políticos o sociales y económicos, que podrían haber determinado o al menos influido en una posible aceptación de una Constitución Europea, en el caso de someter dicho texto a la "prueba" de los referéndums nacionales (aceptación fallida, como es bien sabido). En este proceso, el T.J.U.E. mantiene su papel importante, como "interfaz" entre los mecanismos jurisdiccionales europeos (a veces engorrosos y demasiado burocráticos) y el ciudadano común de un Estado miembro, para demostrar de la manera más plausible el compromiso de la UE de respetar los derechos humanos. El simple ciudadano europeo tiene la posibilidad de introducir acciones directas ante los tribunales de la Unión, siendo el Tratado de Lisboa que aporto cierta flexibilidad en las normas procesales en este ámbito.

Por otro lado, la aplicación de las disposiciones de la Carta se ha restringido al alcance de la legislación de la UE. (de acuerdo con el principio de atribución de competencias), manifestando cierta precaución en relación con el "orgullo" de los Estados miembros, a fin de preservar su identidad nacional[399] (véase el caso de Gran Bretaña, Polonia y, más recientemente, Irlanda, que afirmó la supremacía del derecho interno, respectivamente, de ciertas disposiciones constitucionales en relación con la Carta).

---

[398] Blanke, H.J. (2006) *Protection of Fundamental Rights afforded by the European Court of Justice in Luxembourg en*: Blanke HJ. y Mangiameli S. (eds) *Governing Europe under a Constitution*. Editorial Springer, Berlin, Heidelberg;

[399] Alonso García, R.y Sarmiento, D., (2003) *Los efectos colaterales de la Convención sobre el futuro de Europa en la arquitectura judicial de la Unión: ¿Hacia una jurisdicción auténticamente constitucional europea?*, en Revista de Estudios Políticos, pp. 111-138
Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=496693.

En comparación con las disposiciones actuales de los Tratados, enmendados después de Lisboa (artículo 6 del TUE[400]), se observa que las tradiciones constitucionales comunes de los Estados miembros y las disposiciones del Convenio han seguido siendo principios generales del derecho comunitario, actuando como *normas de interpretación*[401] (como una fuente externa del derecho constitucional en materia de derechos fundamentales), mientras que la Carta constituye *una fuente de derecho primario e independiente*, junto con los tratados.

Además, de esta característica de la Carta, algunos autores[402] han apreciado su valor como documento constitucional, incluso si no está incorporado en los tratados, ella tiene una existencia independiente y puede usarse como referencia general para los derechos fundamentales. Según algunos doctrinarios[403], el hecho de reiterar, mediante varias disposiciones de la Carta, que no se extiende la competencia de la U.E. condujo a una equivalencia de los derechos y libertades estipulados aquí con las llamadas "competencias negativas", de limitar las atribuciones de las instituciones europeas. Por lo tanto, los titulares de la obligación de respetar los derechos previstos en la Carta son las instituciones y organismos de la UE, pero también los Estados miembros (incorporando todos los representantes de los poderes públicos y no solo) al aplicar la legislación europea. Finalmente, el examen de la efectividad de las reglas de la Carta y su correcta aplicación se realiza ante los tribunales nacionales y el T.J.U.E., en particular, en el marco

[400] "Artículo 6 – (1) La Unión reconoce los derechos, libertades y principios enunciados en la Carta de los Derechos Fundamentales de la Unión Europea de 7 de diciembre de 2000, tal como fue adaptada el 12 de diciembre de 2007 en Estrasburgo, la cual tendrá el mismo valor jurídico que los Tratados. Las disposiciones de la Carta no ampliarán en modo alguno las competencias de la Unión tal como se definen en los Tratados. Los derechos, libertades y principios enunciados en la Carta se interpretarán con arreglo a las disposiciones generales del título VII de la Carta por las que se rige su interpretación y aplicación y teniendo debidamente en cuenta las explicaciones a que se hace referencia en la Carta, que indican las fuentes de dichas disposiciones.
(2) La Unión se adherirá al Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Esta adhesión no modificará las competencias de la Unión que se definen en los Tratados.
(3) Los derechos fundamentales que garantiza el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y los que son fruto de las tradiciones constitucionales comunes a los Estados miembros formarán parte del Derecho de la Unión como principios generales".
[401] Blanke, H.J. (2006) idem. p. 164
[402] Salinas Alcega, S. (2001) *Desarrollos recientes en la protección de los derechos humanos en Europa. Nuevos elementos en una vieja controversia: la adhesión de las Comunidades europeas a la Convención europea de salvaguarda de los derechos humanos y las libertades fundamentales*, en *Noticias de la Unión Europea*, núm. 199/2/2001; Gearty, C. A. (ed.) (1997) *European civil liberties and the European Convention on Human Rights,* Editorial Nijhoff, La Haya-Boston-Londres; Alonso García, R.y Sarmiento, D., (2003) idem.
[403] Pernice, I. (2009) *The Treaty of Lisbon: Multilevel Constitutionalism in Action*, en The Columbia, Journal of European Law, Vol. 15, no. 3/2009.

de la cooperación entre ellos (como el procedimiento cuestiones prejudiciales sobre la interpretación de la Carta). También, otras instituciones y organismos de la U.E. como el Parlamento Europeo, el Defensor del Pueblo Europeo[404], la Agencia de los Derechos Fundamentales de la Unión Europea[405] y el Supervisor Europeo de Protección de Datos[406], que están involucrados en garantizar o controlar el respeto de los derechos fundamentales. Creados según el modelo de las instituciones existentes a nivel nacional, también desempeñan un papel de contrapeso ("checks and balances") para la acción de la Unión y sus instituciones, en términos de respeto a los derechos fundamentales de los ciudadanos europeos.

La posición adoptada por el T.J.U.E. en el ámbito de los derechos, se ha convertido en un hito importante para otras instituciones europeas, como el Parlamento Europeo, en particular, porque los derechos fundamentales son una de las razones importantes que se tienen en cuenta en la decisión de rechazar la adopción de un acto.

Por lo tanto, el reconocimiento de los derechos fundamentales a nivel del orden jurídico de la U.E. está estrechamente relacionado con el fenómeno de su constitucionalización, transponiendo en este plan supranacional la relación entre los ciudadanos y las instituciones políticas que ejercen el poder, según el modelo francés del "contrato social". En un sistema de varias capas como el comunitario, donde los poderes supranacionales se establecen de manera complementaria a los de las instituciones nacionales, los derechos fundamentales se han visto como un medio para limitar los primeros, a fin de garantizar aún más la libertad y la autonomía individual de cada ciudadano[407], considerado como el objetivo final de la integración europea después del final de la Segunda Guerra Mundial[408]. Aunque creado sobre la base de las tradiciones

[404] El Defensor del Pueblo Europeo fue instituido por el tratado de Maastricht y su papel consiste en investigar las reclamaciones relativas a una mala gestión por parte de las instituciones y los organismos de la UE. Las reclamaciones pueden proceder de cualquier ciudadano de la UE o de residentes, empresas y organizaciones con domicilio en un Estado miembro. Mas información en: https://europa.eu/european-union/about-eu/institutions-bodies/european-ombudsman_es.

[405] La Agencia de los Derechos Fundamentales de la Unión Europea (FRA) proporciona a los responsables de la toma de decisiones nacionales y de la UE asesoramiento independiente, contribuyendo así a que la creación de debates, políticas y legislación en materia de derechos fundamentales sea mejor informada y más específica.

[406] El papel del Supervisor Europeo de Protección de Datos (SEPD) es defender el cumplimiento de las estrictas normas de protección de la intimidad que regulan esas actividades. Mas información: https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_es

[407] Pernice, I. (2009) idem.

[408] Ruiz-Jarabo, D.y Correa Guimerá, B. (1999) *La protección de los derechos humanos por el Tribunal de Justicia de las Comunidades Europeas* en A. MARZAL (ed.) Derechos humanos del migrante, de la mujer en el Islam, de injerencia internacional y complejidad del sujeto, Editorial Bosch, Barcelona, pp. 137 - 138.

constitucionales comunes de los Estados miembros e inspirado de los instrumentos jurídicos internacionales de valor universal o regional, el sistema de derechos fundamentales de la Unión es específico, autónomo, integrado en el orden jurídico comunitario (a su vez autónomo) y reconocido como tal por los Estados miembros.

En este sentido, la doctrina señaló[409] que lo específico del sistema europeo de protección legal de los derechos fundamentales es su contextualización, dependiendo de los titulares, los beneficiarios o el espacio en el que se manifiestan y se reconocen, un aspecto que merece ser enfatizado en el caso del derecho a la privacidad. El sistema de protección de los derechos fundamentales de la U.E. determina la asunción de obligaciones con efecto vertical y horizontal, oponiéndose tanto a las instituciones y organismos europeos, como a los Estados miembros (cuando transponen las normas derivadas del derecho comunitario, pero también en su calidad de agentes de ejecución del derecho europeo).

En el contexto de la entrada en vigor de la Carta y la realización del procedimiento de adhesión al Convenio, la intención del T.J.U.E.[410] parece estar dirigido no solo a garantizar la autonomía de la protección jurisdiccional de los derechos fundamentales, sino también a consolidarla, en directa relación con la jurisprudencia nacional o del T.E.D.H. Sin negar el aspecto positivo de tal enfoque, aún es necesario "*mantener un equilibrio entre un control demasiado intrusivo y una relajación jurídica demasiado peligrosa en la UE, en lo que concierne los derechos fundamentales*"[411].

Como afirma la catedrática Teresa Freixes Sanjuán:

> "*Un instrumento importante puede ser, si se consigue finalmente recuperarla, la Constitución europea, con sus proclamaciones de derechos y sus instrumentos de garantía. Pero estamos ante un impasse que no sabemos todavía en qué sentido se va a poder desbloquear y si, al hacerlo, podremos mantener todas aquellas regulaciones que hemos visto reforzaban la función de los derechos*

[409] Chueca Sancho, A. G. (1989) *Los derechos fundamentales en la Comunidad Europea*, Editorial Bosch, Barcelona.
[410] En este sentido véase el "Documento de reflexión del Tribunal de Justicia de la Unión Europea sobre determinados aspectos de la adhesión de la Unión Europea al Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.
Disponible en: https://curia.europa.eu/jcms/upload/docs/application/pdf/2010-05/convention_es_2010-05-21_12-10-16_194.pdf
[411] Ibidem.

fundamentales en el seno de la Unión. Este proceso de constitucionalización, esta etapa «constitucional» de la Unión tiene que encontrar su coherencia y su referente de legitimidad a partir de la concreción de los valores que deben identificar a la nueva Europa"[412].

Aunque nacieron juntos con la persona humana, los derechos fundamentales fueron reconocidos jurídicamente en el contexto de la reacción de defensa del individuo ante el poder público del estado, a fin de limitar su acción arbitraria y mantener una esfera de autonomía personal. Observando la multitud y diversidad de los tipos de clasificación de los derechos fundamentales, todavía podemos encontrar una constante en el proceso de su definición en la doctrina del derecho constitucional y en la forma de reconocer su carácter supremo. La definición que proponemos incluye los siguientes elementos: son derechos subjetivos esenciales para la vida, libertad y dignidad de la persona cuyo carácter supremo es reconocido por normas legales con fuerza superior dentro de un sistema normativo o bajo la jurisprudencia de los tribunales contenciosos constitucionales o internacionales y que están garantizados por la Constitución, por leyes y por el control de los tribunales.

El profesor Luis-Carlos Amezúa Amezúa considera que las cuestiones problemáticas no derivan de la falta de un marco procesal concreto sino de la inexistencia de un catálogo europeo escrito de los derechos fundamentales, es decir un problema de sustantividad en la configuración los derechos como principios generales, subrayando que los Tratados constitutivos no mencionan una lista o una jerarquía de estos derechos. Según su opinión: "*en el ordenamiento comunitario, los derechos fundamentales prácticamente no funcionan como derechos subjetivos, pues antes de que en cada caso se pronuncie el propio TJCE no existe derecho fundamental alguno. La situación actual no contribuye a fortalecer la seguridad jurídica, ni tampoco el juez puede evitar la falta de globalidad de su tarea, resultando con ello un panorama de protección parcial*"[413].

[412] Freixes Sanjuán, T. (2005) *Derechos fundamentales en la Unión Europea. Evolución y prospectiva: la construcción de un espacio jurídico europeo de los derechos fundamentales*, Revista de derecho constitucional europeo Nº. 4/2005, pp. 43-86,
disponible en: https://www.ugr.es/~redce/REDCE4/articulos/02freixes.htm.

[413] Amezúa Amezúa, L. C. (2004) *Los derechos fundamentales en la unión europea*, *Revista de derecho (Valdivia)*, *16*, pp. 105-130. https://dx.doi.org/10.4067/S0718-09502004000100005.

4.4.3 El reconocimiento de los derechos fundamentales al nivel internacional

A nivel internacional, la historia de los instrumentos jurídicos en el campo de los derechos humanos comienza después de la creación de las Naciones Unidas (O.N.U.). También se manifestaron algunas preocupaciones en el período anterior para regular las cuestiones interestatales que también incluyan cuestiones de derechos humanos. Por ejemplo, en el siglo XIX, se han adoptado declaraciones o convenciones que prohíben la esclavitud[414].

Después de la Primera Guerra Mundial, el tema de la protección de las minorías empezó a presentar interés para los gobiernos, pero no todos los Estados lo abordaron en la misma manera, dada la disparidad y la falta de homogeneidad de las poblaciones en algunos territorios. Los horrores de las guerras de la primera mitad del siglo XX, las experiencias trágicas de individuos pertenecientes a diversas categorías sociales o étnicas, así como las crisis económicas atravesadas entre las dos guerras mundiales o sus consecuencias, llevaron a los estados a adoptar una nueva actitud, más responsable con la necesidad de proteger los valores importantes para el libre desarrollo de la personalidad humana en la sociedad y la preservación de la paz a nivel mundial o regional[415]. Esta tendencia ha sido más marcada por la creación de organizaciones internacionales o regionales con un rol regulador en las relaciones entre los estados, que han generado una nueva filosofía, la de los derechos humanos.

Aunque, la doctrina considera la noción de "derechos humanos" como "relativamente imprecisa"[416], esta noción se ha definido, en un sentido metodológico, didáctico: "*un conjunto de normas jurídicas internacionales que reconocen los atributos y facultades del individuo que garantizan su dignidad, libertad y desarrollo de su personalidad, y que tienen garantías institucionales adecuadas"*[417], o en un sentido

---

[414] El primer instrumento internacional que condenó esta práctica fue la Declaración de 1815 relativa a la abolición universal de la trata de esclavos. Con el fin de poner término al negocio de esclavos en el Atlántico y liberar a los esclavos en las colonias de los países europeos, en los Estados Unidos de América se inició el movimiento abolicionista. A los principios del siglo XIX se firmaron un gran número de acuerdos multilaterales y bilaterales que contienen disposiciones por las que se prohíben esas prácticas tanto en tiempo de guerra como de paz. Se ha estimado que entre 1815 y 1957 se aplicaron unos 300 acuerdos internacionales relativos a la abolición de la esclavitud, pero ninguno de ellos ha sido totalmente efectivo.
415 Schneider, H. P. (1985) *Derechos fundamentales en el Estado constitucional democrático*, Revista de Estudios Políticos, núm. 7.
[416] Renucci, J.-F. (2009) *Tratado de derecho europeo de derechos humanos*, Hamangiu Publishing House, Bucarest, p. 1.
[417] Bîrsan, C. (2010) *Conventia europeana a drepturilor omului. Comentariu pe articole* (*El Convenio Europeo de Derechos Humanos. Comentarios sobre los artículos*), Edición 2, C.H. Beck, Bucarest, p. 14.

menos abstracto, "privilegios gobernados por las reglas que una persona tiene en sus relaciones con los individuos y con el Estado"[418].

Los instrumentos jurídicos internacionales han generado un sistema internacional de derechos humanos basado en tres ideas: a) reafirmación, desarrollo y codificación de la cuestión de los derechos humanos; b) mecanismos establecidos para la aplicación de reglas convencionales; c) educación de los ciudadanos con el espíritu de respetar las disposiciones vigentes de derechos humanos[419]. El sistema genérico internacional para la protección de los derechos humanos también incluye subsistemas regionales creados sobre la base de convenciones celebradas por los estados en una región geográfica particular del mundo.

Con el establecimiento de las Naciones Unidas, después de la Segunda Guerra Mundial y la aprobación de la Carta de las Naciones Unidas, los derechos humanos fueron plenarios, uno de los objetivos de la organización ha sido la promoción y el desarrollo del respeto de los derechos humanos y de las libertades fundamentales, todo sin distinción de raza, sexo, idioma o religión. Entre los documentos adoptados por O.N.U., especialmente la Declaración Universal de los Derechos Humanos del 10 de diciembre de 1948 (Anexo no. 2), que proclama desde el primer párrafo que considera "*que la libertad, la justicia y la paz en el mundo tienen por base el reconocimiento de la dignidad intrínseca y de los derechos iguales e inalienables de todos los miembros de la familia humana*". Más allá de su valor legal – de soft law, este documento se consideró en primer lugar como una declaración política, siendo un "*hito en el camino hacia el progreso humano", "la base del edificio legal internacional en el campo de las libertades públicas*"[420].

En la práctica de las Naciones Unidas, los derechos humanos se consideraron como derechos inherentes a la naturaleza humana y sin la cual la gente no puede vivir como seres humanos[421]. Los derechos consagrados por la Declaración tienen el valor de principios universales: el derecho a la libertad, la igualdad y la dignidad, el derecho a la vida ya la seguridad personal, la prohibición de la esclavitud, de la tortura y de los tratos inhumanos, el derecho a la ciudadanía, el derecho a la libertad de pensamiento, la

[418] Renucci, J.-F. (2009) idem., p. 2.
[419] Deaconu, S. (2011) *Drepturile şi libertăţile fundamentale în sistemul constituţional românesc (Derechos y libertades fundamentales en el sistema constitucional rumano)*, artículo publicado en la "Revista rumana de derecho privado", núm. 4/2011.
[420] Muraru, I. (1995) *Reflectarea drepturilor omului în noua Constituţie a României (Reflexión de los derechos humanos en la nueva Constitución de Rumania)*, en I. Muraru, M. Constantinescu, "Estudios constitucionales", editorial Actami, Bucarest, 1995, p. 174
[421] Levin, L. (2009) *Human Rights, Questions and answers*, Editorial UNESCO Publishing Paris, 1987, p. 5.

fundación una familia, el derecho al respeto por la vida personal. Por primera vez, la declaración prefigura una serie de derechos económicos, sociales y culturales, como el derecho al trabajo, la libertad de asociación en sindicatos, el derecho al descanso y el esparcimiento, el derecho a una vida digna, el derecho a la educación, el derecho a adoptar parte de la vida cultural de la comunidad.

Las disposiciones de este documento fueron el punto de partida para el desarrollo de los instrumentos legales dentro de O.N.U. y no solo, que han fortalecido la dimensión legal de estos derechos y han sentado las bases para la protección internacional de los derechos humanos. Gradualmente, la declaración que ha reafirmado los principios incorporados en numerosos actos jurídicamente vinculantes muestra que este documento inicialmente considerado como uno esencialmente político, se ha convertido en parte del derecho internacional consuetudinario.

Otro momento importante en la promoción de los derechos humanos por la O.N.U. fue la adopción en 1966 de los dos pactos: el Pacto Internacional de Derechos Económicos, Sociales y Culturales (Anexo 4) y el Pacto Internacional de Derechos Civiles y Políticos que entró en vigor desde 1976 (Anexo 3). La adopción de dos instrumentos distintos por las dos categorías de derechos se debe a la diferencia de opinión entre los estados que han considerado los derechos civiles y políticos como derechos existentes y reconocidos en todos los estados, mientras que los derechos económicos, sociales y culturales serían solo objetivos potenciales para garantizar todavía habría acción legal[422]. Estos documentos adoptados por O.N.U. tienen carácter programático, para impulsar a los Estados a regular la protección de los derechos humanos a nivel nacional[423].

A nivel regional, se identifican tres (sub) sistemas principales de protección de los derechos humanos: el sistema europeo, el sistema interamericano y el sistema africano, más los sistemas asiático e islámico; el primero se considera uno de los más desarrollados, siendo un modelo para los otros sistemas[424].

El sistema europeo se basa en las disposiciones del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales (en adelante el Convenio), adoptado por el Consejo de Europa en 1950, que luego se complementó con varios

[422] Duculescu, V. (1994) *Protecţia juridică a drepturilor omului (Protección jurídica de los derechos humanos),* Lumina Lex Publishing House, Bucarest, página 63;
[423] Bîrsan, C. (2010) idem, p. 665;
[424] Deaconu, S. (2011) idem.

protocolos adicionales y se convirtió en un el estándar generalmente aceptado para garantizar los derechos fundamentales.

El Convenio permite que las personas afectadas en sus derechos por los actos de los Estados signatarios de la convención obtengan satisfacción mediante la concesión de daños o de adopción de medidas para restablecer los derechos violados. En particular, el Tribunal Europeo de Derechos Humanos (en lo sucesivo, "T.E.D.H." o "el Tribunal") es la institución que lleva a cabo dicha revisión judicial en favor de las personas cuyos derechos han sido ignorados internamente. Al reafirmar una serie de derechos que se encuentran reconocidos en la Declaración Universal de los Derechos Humanos, el Convenio los regula de una forma detallada y establece las condiciones bajo las cuales se pueden permitir ciertas excepciones. Por ejemplo, el artículo 8 del Convenio protege el derecho a la privacidad, considerando que la injerencia de una autoridad en la vida privada solo se admite en la medida en que la ley lo establece y es necesaria en una sociedad democrática para la protección de ciertos valores importantes.

La libertad de expresión se refiere a la libertad de opinión y la libertad de recibir o comunicar información o ideas sin la interferencia de las autoridades:

> "*Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de las autoridades y sin consideración de fronteras"*[425].

Otro de los derechos consagrados en el Convenio y en la práctica de T.E.D.H., invocado varias veces en los procedimientos antes del Tribunal es el derecho a un juicio justo, previsto en el art. 6:

> *"Toda persona tiene derecho a que su causa sea oída equitativa, públicamente y dentro de un plazo razonable, por un Tribunal independiente e imparcial, establecido por ley, que decidirá los litigios sobre sus derechos y obligaciones de carácter civil o sobre el fundamento de cualquier acusación en materia penal dirigida contra ella. La sentencia debe ser pronunciada públicamente, pero el acceso a la sala de audiencia puede ser prohibido a la prensa y al público durante la totalidad o parte del proceso en interés de la moralidad, del orden público o de la seguridad nacional en una sociedad democrática, cuando los intereses de los menores o la protección de la vida privada de las partes en el*

[425] Articulo 10 (I) del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

proceso así lo exijan o en la medida en que sea considerado estrictamente necesario por el tribunal, cuando en circunstancias especiales la publicidad pudiera ser perjudicial para los intereses de la justicia".

Según los textos contenidos en el Convenio e interpretados por el T.E.D.H., el principio de libre acceso a la justicia requiere la existencia de tribunales, la independencia de los jueces y su sometimiento a la ley[426], la publicidad de las audiencias, la garantía del derecho a la defensa, la existencia de un control judicial de las sentencias dictadas. Además, proclama el principio de unicidad e igualdad de justicia para todos, el principio de utilizar el idioma oficial y la lengua materna en los tribunales, la presunción de inocencia y el principio de legalidad[427].

Dentro de la Unión Europea, la cuestión de la protección de los derechos humanos mediante textos jurídicamente vinculantes se planteó un poco más tarde, dados los objetivos predominantes de cooperación o integración económica de las Comunidades Europeas. Pero tras la aprobación de la Carta de los Derechos Fundamentales de la Unión Europea (en adelante denominada "la Carta"), se otorgó también valor jurídico a los derechos humanos a nivel de la Unión a través de los derechos estipulados en la Carta tras la revisión del Tratado de la Unión Europea y el Tratado de Funcionamiento de la Unión Europea por el Tratado de Lisboa.

Los instrumentos internacionales para la defensa de los derechos humanos, de valor universal o regional, han sido una fuente de inspiración para los legisladores constitucionales en muchos estados, que han incluido disposiciones expresas en el texto de las leyes fundamentales e incluso han dado prioridad ante las leyes nacionales, en la medida en que contengan disposiciones más favorables[428].

4.5. La relación entre los derechos de la cuarta generación y otros derechos fundamentales

Tradicionalmente, la doctrina del derecho constitucional habla de la existencia de tres generaciones de derechos fundamentales; también hay opiniones[429], según las

---

[426] Pardo Iranzo, V. y Pascual Serrats, R. (2011) *Acceso a la Justicia de los más desfavorecidos y Unión Europea*, Revista Boliviana de Derecho, núm. 12/2011, pp. 172-202, Fundación Iuris Tantum, Santa Cruz, Bolivia.

427 Blanke H.-J. y Mangiameli, S. (2011) *The European Union after Lisbon: Constitutional Basis, Economic Order and External Action*, Editorial Springer Science & Business Media Berlin, p. 165.

[428] Ansuátegui, F. J. (1997) *Derechos fundamentales, poder político, y poderes sociales*, en varios autores, Direitos humanos: a promesa do século XXI, Porto, Editorial ELSA.

[429] Peces-Barba, G. (1993) *Derecho y derechos fundamentales*, Madrid: Centro de Estudios Constitucionales; Rodriguez Uribes, J. M. (2015) *Gregorio Peces-Barba – Justicia y Derecho*, Editorial Aranzadi Madrid; Rodríguez Palop, M. E. (2010) *La nueva generación de derechos humanos. Origen y*

cual surgió una nueva generación de derechos fundamentales, la cuarta, cuya génesis es determinada por la influencia ejercida sobre la vida del individuo de las nuevas tecnologías utilizadas en las comunicaciones y para diseminar la información.

Hablar de varias "olas" o "generaciones" de derechos humanos es un tema común en nuestros días. El primero en hablar de estas generaciones fue Karel Vasak[430], en una conferencia para el Instituto Internacional de Derechos Humanos, dada en Estrasburgo en el año 1979.

Después de este momento, la doctrina jurídica ha intentado identificar otros tipos de derechos de la persona, como el derecho al desarrollo económico y personal, el derecho a la asistencia humanitaria, el derecho a una vida digna, el derecho a la libre determinación de los pueblos, el derecho a guardar silencio, el derecho a ser dejado solo. Sin embargo, no cualquier derecho cuya existencia se trata de justificar puede adoptar una forma jurídica adecuada para el propósito de su creación, es decir para la protección de la libertad y la dignidad humana, por lo que es necesario realizar un filtrado desde este punto de vista.

> *"Estos hechos han abierto la discusión de si verdaderamente se está ante una nueva generación que se distinga de las anteriores. Por un lado, sin nuevos derechos no hay nueva generación. Por otro lado, aunque existan derechos nuevos, no necesariamente estos serán «derechos humanos». No basta tener una nueva lista de derechos a protegerse, por larga que sea, sino que es preciso que estén relacionados con lo nuclear del ser humano y entre todos ellos exista algo común que los muestre como una ola continua que golpea las orillas del siglo"*[431].

En la cuarta generación se pueden incluir derechos tales como el derecho a la intimidad, el derecho a la privacidad (que, por la complejidad de su objeto, se considera que subsuma la casi totalidad de los derechos fundamentales), el derecho a la protección datos personales. No se puede negar la existencia y consistencia legal de estos derechos, especialmente porque algunos estados u organizaciones internacionales los han elevado expresamente al rango de derechos fundamentales[432]. Por otro lado, el tema de la

justificación, Editorial Dykinson, Madrid; Pérez Luño, A. E (1991) *Las generaciones de derechos fundamentales*, Revista del Centro de Estudios Constitucionales, Nº. 10, 1991, pp. 203-217;

[430] Vasak, K. (1984) *Las dimensiones internacionales de los derechos humanos*, Editorial Unesco;

[431] Riofrío Martínez-Villalba, J. C. (2014) *La cuarta ola de derechos humanos: los derechos digitales*, Revista Latinoamericana de Derechos Humanos Volumen 25 (1), I Semestre 2014, disponible en: https://www.revistas.una.ac.cr/index.php/derechoshumanos/article/view/6117

[432] Warren, S. D. y Brandeis, L. D. (1890) *The Right to Privacy*, Harvard Law Review, 5, 4.

protección de estos derechos recientes concierne a la protección de valores esenciales para el ser humano, en principio, sus derechos naturales, libertad y dignidad, y por lo tanto la inviolabilidad específica de la primera generación de derechos, lo que asegura el ámbito de la autonomía individual en la relación con el poder estatal.

Asimismo, la garantía objetiva del ejercicio de los derechos a la privacidad y la protección de los datos personales implica una relación con otros derechos socioeconómicos fundamentales (derechos de segunda generación) que permiten al individuo manifestar su personalidad de manera plenaria en la sociedad, facilitada por una acción positiva del estado. Finalmente, el derecho a la vida privada ha recibido un nuevo componente por la jurisprudencia T.E.D.H., que consiste en el derecho a un medio ambiente sano, que se considera un derecho perteneciente a la tercera generación. Existe una estrecha correlación entre los derechos que pertenecen a diferentes generaciones, esta clasificación no se equipara con su separación en el tiempo y el espacio, pero ilustra la "secuencia de doctrinas y corrientes del pensamiento filosófico que sustentó el surgimiento de diferentes derechos y forma un conjunto indivisible en su totalidad, pero no homogéneo en sus grupos"[433].

Todavía es posible el reconocimiento de nuevos derechos fundamentales, su lista permanece abierta para los legisladores y jueces constitucionales o internacionales, si se demuestra su coherencia legal en el ámbito de la aplicación efectiva de las normas que los garantizan.

4.6. Los derechos de la personalidad: ¿una nueva categoría de derechos fundamentales?

El enfoque de este tema tiene como punto de partida la inclusión del derecho a la vida privada y del derecho a la protección de los datos personales en la categoría de "los derechos de la personalidad". Esta frase es específica a la doctrina alemana que la consagró y se atribuye a una categoría de derechos civiles subjetivos, como el derecho a la protección del nombre, el derecho a la protección de la vida, la salud y la libertad, el derecho a contestar[434].

[433] Muraru, I. y Tanasescu, E.S. (2001) *Drept Constitutional si institutii politice (Derecho Constitucional e Instituciones Políticas)*, Volumen I, Edición 14, Editorial C.H. Beck, Bucarest, p. 145
[434] Whitman, J. Q. (2004) *The Two Western Cultures of Privacy: Dignity versus Liberty*, en *Faculty Scholarship Series* (Yale Law School Legal Scholarship Repository), Paper 649, p. 1186

"Los derechos son un instrumento para alcanzar la igualdad que permite a todos, por su extensión generalizada, participar en la democracia social, disfrutar en condiciones de los derechos clásicos, individuales, civiles y políticos, con la satisfacción de las necesidades básicas, y finalmente, alcanzar ‹‹el desarrollo y la salvaguardia de la libre personalidad, que es un objetivo humanista…"[435]

El concepto de "personalidad" en el derecho alemán se basa en las ideas filosóficas de Kant, Humboldt y Hegel y ha adquirido una importancia jurídica fundamental, especialmente después de la Segunda Guerra Mundial, en el contexto del reconocimiento de la Constitución alemán[436] y la jurisprudencia del Tribunal Constitucional Federal sobre el valor supremo otorgado a la dignidad de la persona humana. De este modo, la ley de la personalidad incluye la ley de la libertad y de la esfera íntima en la que una persona desarrolla libre y responsablemente su propia personalidad. La dignidad de la persona humana tiene el valor de un principio legal y de un derecho subjetivo fundamental que establece el estándar según el cual una determinada conducta (acción o inacción) puede ser reclamada por otros[437].

La persona que se convirtió en sujeto de derecho no es solo una ficción legal, sino un individuo real ("un hecho empírico, una realidad de esencia histórica - social"[438]), por lo tanto, la dignidad le permite al individuo detener el control sobre sí mismo y seguir siendo autónomo en la sociedad. En consecuencia, la dignidad se convierte en un concepto legal sobre cuya base se protege la esencia humana, y todo lo que tiende a deshumanizar al hombre se considerará como un perjuicio para su dignidad[439]. La

---

[435] Peces-Barba Martínez, G. (1999) *Derechos sociales y positivismo jurídico: (escritos de filosofía jurídica y política)*. Madrid: Dykinson: Instituto de Derechos Humanos Bartolomé de las Casas, Universidad Carlos III, p. 45

[436] Artículo 1 de la Ley Fundamental de la República Federal de Alemania - Protección de la dignidad humana, vinculación de los poderes públicos a los derechos fundamentales:
(1) La dignidad humana es intangible. Respetarla y protegerla es obligación de todo poder público.
(2) El pueblo alemán, por ello, reconoce los derechos humanos inviolables e inalienables como fundamento de toda comunidad humana, de la paz y de la justicia en el mundo.
(3) Los siguientes derechos fundamentales vinculan a los poderes legislativo, ejecutivo y judicial como derecho directamente aplicable. Disponible en: https://www.btg-bestellservice.de/pdf/80206000.pdf.

[437] Peces-Barba Martínez, G. (2002) *La dignidad de la persona desde la filosofía del derecho*. Madrid: Dykinson.

[438] Poulain, J. ; Sandkuhler, H. J. y Triki, F. (2009) *La dignité humaine: Perspectives transculturelles* (Philosophie und Transkulturalität / Philosophie et transculturalité) (French Edition), Editorial Peter Lang GmbH, Internationaler Verlag der Wissenschaften, p. 12

[439] Decisión del Tribunal Constitucional Federal Alemán en el caso de Luth, BVerfG, 15.01.1958 - 1 BvR 400/51), de 15 de enero 1958, disponible en:
https://www.utexas.edu/law/academics/centers/transnational/work

dignidad, junto con la libertad de expresión son los límites del poder estatal, según la decisión tomada por el Tribunal Constitucional Federal Alemán en el caso de Luth:

> *"La Ley Fundamental, que no quiere ser un orden neutral de valores ha establecido también en la parte dedicada a los derechos fundamentales un orden objetivo de valores y que precisamente con ello se pone de manifiesto un fortalecimiento por principio de la pretensión de validez de los derechos fundamentales. Este sistema de valores, que encuentra su núcleo en la personalidad humana que se desarrolla libremente en el interior de la comunidad social y en su dignidad, debe regir, en tanto que decisión constitucional básica, en todos los ámbitos del derecho; la legislación, la administración y la jurisprudencia reciben de él directrices e impulso"*[440].

El sistema objetivo de valores establecido por la Constitución de un Estado busca proteger los derechos fundamentales centrándose en el libre desarrollo de la personalidad humana en la sociedad y debe aplicarse como un "axioma constitucional" en todo el sistema de derecho basado en el "efecto radiante" de los derechos fundamentales sobre el Derecho privado que no puede ser contrario a ellos y que se interpretará en relación con los derechos fundamentales. Los derechos de la personalidad se desarrollaron aún más sobre la base de la práctica creativa del tribunal constitucional alemán, particularmente en el ámbito del derecho a la vida privada, expuesto a los riesgos nacidos en la nueva era de la información.

Principalmente establecidos en el ámbito del derecho privado, los derechos de la personalidad son derechos subjetivos extrapatrimoniales (no patrimoniales) "que se refieren principalmente a la protección de las características físicas y morales del ser humano, a su individualidad o personalidad"[441]. En una definición que pertenece la doctrina francesa, estos derechos se definieron como "derechos inherentes a la calidad de la persona humana y pertenecen a cualquier individuo por el hecho de que él es un ser humano", siendo llamados "bienes innatos"[442].

---

[440] Ibidem.

[441] Albaladejo, M. (1985) *Derecho civil,* Tomo. I, vol. 2, Editorial Bosch Barcelona, p. 231.

[442] Colin, A.; Capitant, H. y Morandière, J. (1940) *Curso de Derecho Civil*, traducción por V. G. Falls, I. Miloaie, volumen I, 7ª edición, Bucarest, Central Printing, página 127. En la perspectiva de los autores, los derechos civiles tienen tres subdivisiones: derechos inherentes a la personalidad, derechos familiares y derechos patrimoniales.

Citando a la autora rumana Calina Jugastru[443], los derechos de la personalidad definen como "prerrogativas extrapatrimoniales íntimas unidos a la persona que expresa ser intrínseca a ella la humana por excelencia". La autora ha clasificado los derechos de la personalidad en las siguientes categorías:

i) derechos de personalidad que definen al ser humano como una entidad biopsíquica (el derecho a la vida, el derecho a la integridad física y mental, el derecho a la propia voz);

ii) derechos de la personalidad que definen al ser humano como sujeto de los estados y las relaciones emocionales o afectivos (derecho al honor, derecho a la reputación, a la dignidad, el derecho a respetar los sentimientos de una persona afectada de un evento familiar como la muerte de un cercano);

iii) los derechos que protegen al hombre como ser social (derechos que pertenecen a la persona física: el derecho a un nombre, derecho al domicilio, derecho a la intimidad, derecho a la imagen, los derechos de propiedad intelectual).

Por otro lado, una enumeración exhaustiva de los derechos de la personalidad no es posible debido a la evolución dinámica de su esfera como resultado del cambio en las diversas etapas históricas de la perspectiva sobre el individuo y sus atributos, así como el impacto de las tecnologías modernas en los valores considerados importantes en la vida de cualquier persona. Entre los derechos de la personalidad identificados por la doctrina, el derecho a la imagen[444] y el derecho a la privacidad fueron apreciados como los más importantes.

La autora Calina Jugastru identifica las siguientes características de los derechos de la personalidad, que derivan de su esencia no patrimonial:

i) son derechos absolutos y oponibles erga omnes (expresamos la reserva a esta característica, el carácter relativo, condicionado es más específico a estos derechos);

ii) son derechos inalienables e imprecisos, no pueden estar sujetos a disposiciones, adquisiciones o extinciones;

(iii) son derechos puramente personales que pueden ser ejercidos en principio solo por el titular (las reglas de representación siguen siendo aplicables).

Partiendo de las características expuestas, se han definido a los derechos de la personalidad como aquellas prerrogativas extrapatrimoniales, oponibles *erga omnes,* de

[443] Jugastru, C. (2007) *Reflexiones sobre la noción y la evolución de los derechos de la personalidad*, Instituto de Historia "George Bariţiu" de Cluj-Napoca, Serie Humanistica, tomo V, p 326.

[444] El derecho a la imagen es, de hecho, uno de los primeros derechos legalmente reconocido, véase el caso Bismarck: la publicación no autorizada de fotografías con el canciller en el momento de la muerte en 1898.

carácter inalienable y perpetuo, que pertenecen a todo ser humano por su propia condición desde su nacimiento y hasta su muerte; las cuales no pueden ser desconocidas por los poderes públicos ni por los particulares, pues ello traería consigo la vulneración de la personalidad[445].

En el derecho comparado, como regla, los derechos de la personalidad se encuentran regulados en los códigos civiles, bajo un régimen jurídico propio o por medio del reconocimiento genérico de la personalidad. En la mayoría de los Estados, la persona que viola un derecho de otro individuo será responsable de la reparación o el resarcimiento. El *codice civile* italiano de 1942, el código portugués de 1966 y el código peruano de 1984, por ejemplo, han regulado especialmente los derechos de la personalidad.

En Rumania, los derechos de la personalidad fueron expresamente regulados en la legislación ordinaria por las disposiciones del nuevo Código Civil. Hasta la entrada en vigor de estas disposiciones (1 de octubre de 2011), algunos autores afirman que la institución de los derechos de la personalidad se basa en las disposiciones de la Constitución Rumana que definen el marco general para la protección de la privacidad de la persona.

Según la Constitución Española (el artículo 10):

"(1) La dignidad de la persona, los derechos inviolables que le son inherentes, el libre ***desarrollo de la personalidad****, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social.*

(2) *Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España".*

En España, la regulación de los derechos de la personalidad no es una pura opción del legislador, sino una exigencia constitucional, y se encuentra en la Ley Orgánica 1/1982, de 5 de mayo, de protección civil de los derechos al honor, a la intimidad personal y familiar y a la propia imagen, la cual supone un mínimo de protección irrenunciable en orden a garantizar la efectividad de dichos derechos fundamentales en las relaciones sociales y jurídicas entre particulares. Con anterioridad al reconocimiento constitucional de los derechos al honor, a la intimidad y a propia

[445] Rivera, J. C. (2004) *Instituciones de derecho civil,* Editorial Abeledo Perrot Buenos Aires, p. 7.

imagen y a la promulgación de la Ley Orgánica 1/1982, existieron en la doctrina española notables construcciones teóricas de los derechos de la personalidad, en la que se debatió la configuración dogmática de la figura, en particular, si podía, o no, encuadrarse en el molde clásico del derecho subjetivo.

El primer desarrollo jurisprudencial español sobre el contenido objetivo de los derechos fundamentales también hace referencia al libre desarrollo de la personalidad:

> "*En primer lugar, los derechos fundamentales son derechos subjetivos, derechos de los individuos no sólo en cuanto derechos de los ciudadanos en sentido estricto, sino en cuanto garantizan un status jurídico o la libertad en un ámbito de la existencia. Pero al propio tiempo, son elementos esenciales de un ordenamiento objetivo de la comunidad nacional, en cuanto ésta se configura como marco de una convivencia humana justa y pacífica, plasmada históricamente en el Estado de Derecho y, más tarde, en el Estado social de Derecho o el Estado social y democrático de Derecho, según la fórmula de nuestra Constitución (art. 1.1). Esta doble naturaleza de los derechos fundamentales, desarrollada por la doctrina, se recoge en el art. 10.1 de la Constitución, a tenor del cual «la dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamentos del orden político y de la paz social». Se encuentran afirmaciones parecidas en el derecho comparado, y, en el plano internacional, la misma idea se expresa en la Declaración universal de derechos humanos (preámbulo, párrafo primero) y en el Convenio europeo para la protección de los derechos humanos y de las libertades fundamentales del Consejo de Europa (preámbulo, párrafo cuarto). En el segundo aspecto, en cuanto elemento fundamental de un ordenamiento objetivo, los derechos fundamentales dan sus contenidos básicos a dicho ordenamiento, en nuestro caso al del Estado social y democrático de Derecho, y atañen al conjunto estatal. En esta función, los derechos fundamentales no están afectados por la estructura federal, regional o autonómica del Estado*"[446].

En luz de las consideraciones anteriores, se plantea la cuestión de si los derechos de la personalidad pueden considerarse una categoría separada de derechos fundamentales. Como hemos visto, estos derechos defienden valores esenciales, algunos

[446] Tribunal Constitucional de España, STC 25/1981, 14 de julio 981, disponible en: https://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/25

de los cuales se encuentran en las disposiciones constitucionales y son derechos justiciables, que también pueden defenderse ante los tribunales constitucionales. Nacidos por primera vez en el ámbito del derecho privado, los derechos de la personalidad (algunos de ellos) se elevaron más tarde al rango de derechos fundamentales sobre la base de la dignidad humana como principio general, ejerciendo así una influencia decisiva en todas las ramas del derecho.

La naturaleza mixta de estos derechos, como derechos civiles y fundamentales de la persona tiene la ventaja de beneficiarse de todas las garantías legales y jurisdiccionales, como la jurisdicción constitucional, penal y civil - patrimonial (para la recuperación de los daños). Sin embargo, los derechos de la personalidad no suelen estar sujetos a un estudio autónomo del derecho constitucional, como parte de los derechos fundamentales; por otro lado, dada la complejidad de este concepto y la ampliación de su alcance, los derechos generalmente incluidos en esta categoría se tratan por separado como elementos de otros tipos de clasificaciones ya discutidos en una sección previa. El derecho a la privacidad y el derecho a la protección de los datos personales forman parte de la categoría de derechos de la personalidad, y nuestro análisis también abordará este aspecto para caracterizar su naturaleza legal.

4.7. Opiniones teóricas sobre el carácter fundamental de algunos derechos

El lenguaje jurídico relativo a los derechos es bastante variable, al hablar de los "derechos humanos" en general, pero en relación con los aquellos derechos consagrados en los instrumentos internacionales universales, de las "libertades públicas" frente al poder ejecutivo, que es un concepto propio del Derecho francés, o del "derecho fundamental" al referirse, en particular, a los derechos que se otorgan en las constituciones de los estados.

La caracterización de un derecho como "fundamental" también depende de la teoría adoptada para este propósito. En lo que concierne el reconocimiento y la naturaleza jurídica de los derechos fundamentales, entre las teorías más importantes para nuestro análisis mencionamos dos de ellas: *la teoría de los derechos naturales* y la *teoría de los derechos reflejos*, según las cuales vamos a analizar en qué medida el derecho a la vida privada y los derechos derivados del derecho a la privacidad, pueden ser considerados o no derechos fundamentales.

De acuerdo con *la teoría de los derechos naturales*, el hombre es reconocido como el titular de los derechos naturales, que absolutamente le pertenecen, desde el

momento de su nacimiento. Los autores de esta teoría (John Locke, Jean-Jacques Rousseau, Thomas Hobbes, David Hume) han declarado que la justicia natural ("jus naturale") consiste en la libertad que tiene cada individuo a usar de su propio poder para defender su vida, siendo natural la libertad perfecta para ordenar sus acciones, disponer de bienes y personas según su propia voluntad, dentro de los límites de la ley natural, sin pedir permiso o depender de la voluntad de los demás. J. Locke[447] considera que el estado natural es el estado de igualdad donde el poder y la jurisdicción son recíprocas, ya que todas las personas nacen con las mismas ventajas naturales y usan las mismas facultades.

La igualdad natural y la independencia de las personas imponen al mismo tiempo una serie de limitaciones, de modo que nadie debe dañar la vida, la salud, la libertad o la propiedad de los demás y debe abstenerse de dañar o invadir los derechos de los demás. De esta manera, las teorías liberales definieron como derechos naturales los derechos a la vida, la libertad individual, la igualdad, la propiedad, así como se contemplarán más adelante en la "Declaración de los Derechos del Hombre y del Ciudadano" de 1789, adoptada después de la revolución francesa. En la elaboración de estos conceptos, se trata de delimitar los derechos del ser humano visto como persona nacida con estos derechos (derechos naturales), de los derechos humanos reconocidos al individuo como miembro de la sociedad, en la base del contrato social.

Al establecer esta delimitación, J.-J. Rousseau consideró la situación en la que cada individuo cede parte de su poder natural en la medida necesaria para lograr el bien de la comunidad, sin embargo, sin limitar la libertad de la persona de forma incompatible con la naturaleza humana[448] (en este sentido, la teoría de los derechos naturales debe interpretarse en estrecha relación con la teoría del contrato social).

En los Estados Unidos, desde la perspectiva de Thomas Jefferson sobre los derechos humanos establecidos por la Declaración de Independencia, se consideraban como derechos naturales el derecho a la vida, la libertad y la búsqueda de la felicidad. Desde la posición de Jefferson, en la interpretación de un autor estadounidense[449], los derechos naturales son derechos que las personas tienen antes e independientemente de cualquier gobierno, porque estos derechos no conciernen a los gobiernos, sino que son derechos que las personas tienen en relación con otras. Solo cuando se constituye un

[447] Locke, J. (2012) *Segundo Tratado sobre el Gobierno Civil. Un ensayo acerca del verdadero origen, alcance y fin del Gobierno Civil*, Editorial Alianza Madrid.
[448] Rousseau, J.J. (1996) *El contrato social,* libro II, cap. I, Edit. Alba, Madrid, p. 175
[449] Boyd, J.P. (1950) *The Papers of Thomas Jefferson*. Vol. 1. Princeton, NJ: Princeton University Press, pp. 243–247.

gobierno, que representa una amenaza potencial para los derechos, debido a su fuerza coercitiva y organizada, se puede hablar de una nueva clase de derechos universales, donde el estado es el propietario de las obligaciones relacionadas: el derecho civil para proteger los derechos naturales "por" el estado y el derecho a la protección "frente" el estado. Estas relaciones nacen y se racionalizan sobre la base del "contrato social" y se expresan con mayor frecuencia en un contexto constitucional.

Partiendo de este tipo de teorización de los derechos naturales, podemos ver cómo los derechos naturales ganan un valor fundamental constitucionalizándolos. Sin embargo, el intento más fructífero de lograr esta indisponibilidad sería mediante la constitucionalización de derechos. La positivización de los derechos y su fundamentación al definirlos e incluirlos en las normas constitucionales consagra su debido respeto en relación con otras categorías. La mención de los derechos fundamentales en la norma suprema de un Estado les otorga estabilidad, no necesariamente rigidez, los protege y obliga a los demás poderes estatales a respetar su contenido y alcance. De esta forma los derechos sólo pueden modificarse a través del poder constituyente-constituido[450].

En cuanto al derecho a la privacidad y de la protección de datos personales, estos nacieron en medio de la evolución dinámica de la sociedad moderna, sometida a transformaciones tecnológicas, teniendo como base común la dignidad del hombre y el libre desarrollo de la personalidad humana. En cualquier caso, el derecho del individuo a ejercer un control cuasi autónomo sobre la propia persona y sobre los datos personales que lo caracterizan y unifican en relación con otros miembros de la sociedad no es un derecho absoluto, ya que está limitado por la necesidad de defender otros valores considerados más importantes en las relaciones jurídicas, como el orden público o los derechos de los demás. Desde esta perspectiva, el derecho a la privacidad y a la protección de los datos personales podrían considerarse derechos naturales modernos que la persona humana ha recibido desde su nacimiento, pero cuyo reconocimiento y ejercicio está sujeto a los límites del "contrato social".

De acuerdo con *la teoría de los derechos reflejos*, una ley que establece reglas para la protección de algunos intereses no confiere automáticamente derechos, sino que solo constituye una acción legal refleja del estado. El filósofo Rudolf von Jhering[451] ha

[450] Bastida, F.J.; Villaverde, I.; Requejo, P.; Presno, M. A.; Benito Aláez y Sarasola I. F. (2004) *Teoría General de los Derechos Fundamentales en la Constitución española de 1978*, Editorial Tecnos Madrid, p. 21;

[451] Von Jhering, R. (2011) *El espíritu del Derecho romano en sus diferentes etapas de desarrollo*, Editorial Comares.

sido uno de los partidarios de la teoría de los derechos reflejos. Al otorgar estos derechos, el estado se autolimita, pero al mismo tiempo se beneficia de su ejercicio (es por eso por lo que esta teoría también se denomina teoría de la autolimitación del estado).

En una interpretación doctrinal[452] las libertades de los seres humanos representan una autolimitación del Estado o una "vinculación negativa general". El Estado ofrece a sus ciudadanos la posibilidad legal de autodeterminación o de elegir su conducta. esta libertad del ciudadano implica una autolimitando del poder estatal, es decir la imposibilidad del Estado a intervenir o infringir algunas esferas de la persona. Pero, renunciar a la capacidad de regular legalmente algunos amitos de la libertad individual humana no significa que el Estado renuncie a garantizar la esencia de la libertad que es la autodeterminación, según la opinión del autor Bastida Freijedo:

> *"allí donde no interviene el Estado existe un derecho que él mismo se encarga de garantizar; y es esa garantía – esa presencia del poder público – la que permite identificar la existencia de un derecho, y no de una mera capacidad natural".*

En una concepción concebida de manera similar, León Duguit[453] y Philippe Braud[454] argumentan que el estado tiene la obligación de definir claramente los límites de su competencia y los límites entre los cuales los individuos pueden ejercer sus derechos para no ofender a los demás. Para Duguit, "*todo se transforma, por consiguiente, también el Derecho obedece a una evolución, cuyo sentido está determinado por el postulado de la maximización de la solidaridad entre los hombres, solidaridad, a la vez que es un hecho, es un motivo de la conducta individual y social, y es un criterio de la justicia del Derecho"*[455].

A base de la característica social del ser humano, los individuos tienen una necesidad natural de pertenecer a un grupo, a una sociedad, y de aquí la solidaridad se transforma en un hecho común, en una fuerza que hace el hombre sentirse parte de un conjunto social. En plan psicológico, esta fuerza determina al hombre a renunciar a una parte de sus libertades y acomodarse a las conductas y las normas de los demás para sentirse parte de la sociedad, parte de un estado que lo protege. En un cierto momento

---

[452] Bastida, F.J.; Villaverde, I.; Requejo, P.; Presno, M. A.; Benito Aláez y Sarasola I. F. (2004) idem. p. 20;
[453] Duguit, L. (2003) *L´Etat, le droit objectif et la loi positive*. Réimpression de l'édition de 1901 (Études de droit public I), Editorial Dalloz Paris.
[454] Braud, Ph. (2015) *La notion de liberté publique en Droit français*, Editorial LGDJ, París;
[455] Duguit, L. (2003) idem, p. 26.

histórico, la convergencia de los comportamientos solidarios de los miembros decide el futuro de la sociedad, al regular un tipo de conducta como norma de convivencia social. La suma de convicciones de los miembros de una sociedad garantiza el interés común de la decisión adoptada tras una reacción colectiva, formalizada en una norma de derecho objectivo que coincide en cada país con la ley positiva. De aquí la conclusión que el Derecho objetivo es una norma de conducta social que adquiere carácter imperativo porque se impone bajo una sanción con carácter social. Para Duguit "*la regla de derecho nace inevitablemente vinculada a la realidad de la época histórica*"[456].

En la opinión de Braud "*los derechos-obligaciones positivas… no son normas jurídicas, pues carecen de una condición indispensable: la aptitud para la afectividad*" y, siendo así, "*se sitúan fuera del Derecho*"[457].

Es el Estado el que debe proporcionar las condiciones necesarias para el libre desarrollo de la personalidad de cada individuo desde un punto de vista físico, intelectual y moral, teniendo en cuenta la necesidad de armonizar las posiciones de los miembros de la sociedad para no interferir con los derechos garantizados a todos. Por lo cual, "*las libertades públicas pueden considerarse como obligaciones por parte del estado, es decir, limitaciones a su competencia, dejando una esfera de autonomía individual*"[458]. Por lo tanto, el estado está obligado a limitar su acción teniendo en cuenta la autonomía individual de los ciudadanos.

Desde el punto de vista de estas teorías, el derecho a la privacidad y la protección de los datos personales se puede considerar como una medida de protección legal garantizada por el estado, al limitar su derecho a intervenir en la esfera privada del individuo, dejándole una cierta libertad de acción y control sobre su vida y su información personal, pero sin permitirle cruzar las limitaciones impuestas por la ley. Esta perspectiva permite la preservación de la autonomía de la acción estatal como el mantenimiento de la igualdad de derechos entre los miembros de la sociedad.

Más allá de la adopción de cualquiera de las teorías analizadas anteriormente, creemos que un elemento importante de análisis para la caracterización de un derecho como la observación fundamental es su grado de positividad o reglamentación, respectivamente el carácter de las normas legales que lo consagra expresamente. Por supuesto, en esta "ecuación" no debemos descuidar el papel de la jurisprudencia de los

[456] Duguit, L. (2003) idem, p. 31.
[457] Braud, Ph. (2015) idem, p. 152.
[458] Braud, Ph. (2015) idem, p. 13.

tribunales constitucionales o supranacionales, a los que el legislador o la doctrina de un estado pueden referirse en la apreciación de la naturaleza legal de un derecho[459].

Así, se recuerda que la actual definición de literatura sobre los derechos fundamentales abarca las características de los derechos subjetivos de los ciudadanos, esenciales para su vida, libertad y dignidad, indispensables para el libre desarrollo de la personalidad humana, establecidos por la Constitución y garantizados por la Constitución y las leyes[460]. Específicamente, el concepto de "bloque constitucional", un concepto utilizado en estados como Francia o España no solo establece que las leyes constitucionales otorgan fuerza legal fundamental a ciertos derechos, sino también la interpretación dada por los tribunales constitucionales para garantizar la supremacía de las disposiciones constitucionales.

Por otro lado, como un autor ha señalado[461], las declaraciones internacionales de los derechos, aunque su título revela el contenido de los derechos y libertades fundamentales, las disposiciones reales se refieren a aquellos derechos que se reconocen como tales ("fundamentales") por las constituciones y leyes de los estados signatarios[462], sin asignar este adjetivo a cada tipo de derecho o libertad enumerados en el reglamento.

Del mismo modo fueron elaboradas las primeras regulaciones de la Unión Europea que tratan los derechos fundamentales. La situación fue modificada después de la adopción de la Carta en el año 2000 y la adquisición de fuerza legal por la entrada en vigor del Tratado de Lisboa, que hizo una clara clasificación de los derechos y las libertades consideradas fundamentales.

La conclusión a la que el autor desea llegar es la observación de que, al menos en el caso de las declaraciones internacionales de derechos, los derechos se considerarían fundamentales sobre la base de textos externos. Como tal[463], la naturaleza fundamental de un derecho no depende únicamente del valor supralegal del texto que lo regula. En esa opinión, solo los derechos relacionados con la dignidad humana merecen ser calificados como derechos fundamentales, y la apreciación de quienes los invocan para

---

[459] Díez-Picazo, L. M. (2003) *Sistema de Derechos fundamentales*, Editorial Civitas Madrid;
[460] Solozábal Echeverría, J.J. (1991) *Algunas cuestiones básicas de la teoría de los derechos fundamentales*, En: Revista de Estudios Políticos, Centro de Estudios Constitucionales, Madrid, Nº 71 enero-marzo de1991.
[461] Dreyer, E. (2006*) Du caractère fondamental de certains droits*, en "Revue de la Recherche Juridique, Droit Prospectif", nr. 113/2006, p. 1-2
[462] En el caso específico de Francia, el uso del atributo "fundamental" en el caso de los derechos se encuentra en la jurisprudencia del Consejo Constitucional, pero también en una serie de textos legales que exigen el respeto de los "derechos fundamentales" en relación con el procesamiento de datos personales.
[463] Dreyer, E. (2006) idem., p. 13

este propósito coincide con la apreciación de la asamblea constituyente o de los estados que los han reconocido oficialmente.

En consecuencia, el mismo autor determina dos elementos esenciales para la caracterización de un derecho fundamental: el propósito del derecho es proteger la dignidad humana (valor invocado en la mayoría de las declaraciones de derechos constitucionales internacionales y nacionales) y su reconocimiento oficial a través de un texto supralegal, sin el cual el derecho no se podría lograr en su totalidad. La noción filosófica de dignidad adopta una forma legal al incorporar otros valores intrínsecos, como la libertad, la igualdad, la solidaridad, que llevan al reconocimiento del ser humano en relación con uno mismo y con los demás, y distingue a este respecto los derechos fundamentales reconocidos a las personas físicas de otros derechos invocados por personas jurídicas.

La configuración textual de estos valores en normas supra legislativas tiene el efecto de conferir protección legal al individuo frente a las autoridades, ya sean ejecutivas o legislativas.

Por otro lado, es necesario tener un cierto grado de responsabilidad en la clasificación de algunos derechos como fundamentales. Así, en opinión del autor, algunos de los derechos previstos como fundamentales en las disposiciones de la Carta, como el derecho a la protección de datos personales, son consecuencia de la "fragmentación" de otros derechos fundamentales, como el derecho a la vida privada, sin que los nuevos derechos regulados ("desmembramientos") implican la protección de valores verdaderamente fundamentales (esenciales).

Según la tesis que defendía Peces Barba en su obra de 1976[464], el sistema de los derechos está organizado de una forma dualista: por un lado, los derechos fundamentales, considerados objeto de estudio para la filosofía del derecho, son valores situados en la parte superior de la jerarquía normativa; por otro lado, esos mismos derechos deben integrarse en el sistema del derecho positivo como normas jurídicas concretas y como derechos públicos subjetivos. Los derechos fundamentales tienen carácter histórico, pero no pueden ser arbitrarios. El papel de la filosofía del derecho consiste en demonstrar la objetividad y el fundamento racional de estos derechos, para separar las categorías y evitar que cualquier conjunto de normas serán catalogadas como derechos fundamentales.

[464] Peces-Barba Martínez, G. (1976) *Derechos fundamentales*. Madrid: Guadiana de publicaciones, D.L.

En conclusión, sobre la base de los elementos esenciales separados de los conceptos teóricos analizados anteriormente, en nuestra opinión, la calificación de un derecho como fundamental puede abordarse desde dos perspectivas: vista como valor intrínseco y natural, cualquier derecho que proteja la dignidad humana es fundamental, en el sentido básico de este atributo - "esencial", "importante") para el individuo en sus relaciones consigo mismo, con los demás, con el estado; vistos desde una perspectiva extrínseca, no cualquier derecho fundamental como valor natural adquiere la fuerza legal específica de tal derecho, sino solo aquellos derechos que se benefician del positivismo por su reconocimiento oficial sobre la base de normas supra legislativas (generalmente constitucionales), que otorgan a los derechos efectos legales, como el de ser invocados y opuestos a terceros (efectos verticales - efectos horizontales)[465].

Desde este punto de vista, el poder público (el Estado) tiene al mismo tiempo obligaciones negativas de abstenerse a violar estos derechos, como también obligaciones positivas, por ejemplo, el deber de tomar todas las medidas necesarias para garantizar el ejercicio efectivo de los derechos por parte de todos los destinatarios de la norma legal. Estas consideraciones se tendrán en cuenta durante nuestro trabajo para analizar la naturaleza fundamental del derecho a la privacidad y el derecho a la seguridad de la persona.

[465] Tal concepción también es específica de la ley alemana, donde los derechos fundamentales se entienden como derechos negativos de defensa, que pueden invocarse como derechos subjetivos ante el juez (constitucional), contra cualquier acto administrativo o legislativo del poder público que trata anularlo.

CAPÍTULO V - LOS NUEVOS "DERECHOS DIGITALES" FUNDAMENTALES

No todos los derechos fundamentales de las personas existen de forma pura en el entorno cibernético. Algunos derechos han sufrido cambio de contenido y de límites para adaptarse al nuevo medio de vida de la persona digital[466]. Partiendo desde los derechos clásicos podemos afirmar que en el entorno online se manifiestan y deben quedar protegidos por lo menos los siguientes derechos del usuario.

Estos derechos, enunciados por primera vez por el autor Riofrío Martínez-Villalba en su artículo "La cuarta ola de derechos humanos: los derechos digitales" publicado en diciembre 2014 en la Revista Latinoamericana de Derechos Humanos 15, presentan un contenido propio, desarrollado como consecuencia de las nuevas tecnologías sobre las primeras 3 generaciones de derechos fundamentales. Seguidamente vamos a presentar el contenido de estos derechos, así como se manifiestan en el entorno online.

5.1. El derecho a la vida digital o el derecho a existir digitalmente

Una persona, un ser humano, recibe el derecho a la vida desde el momento de su concepción sin poder elegir sobre su contenido, sobre el ejerció del derecho o sin ser capaz de comprender la noción. Simplemente recibe este derecho y todos los demás están obligados a respetarlo. Después de madurar, el ser humano comprende el valor de este derecho y requiere el mismo a los demás el respeto de su derecho fundamental.

Pues, el derecho a la vida digital está directamente relacionado con la voluntad del individuo. El derecho a la vida digital nace al mismo tiempo que el derecho a la vida, pero el ser humano puede elegir si lo va a gozar o no. También una persona puede elegir a vivir o a morir, pero la naturaleza a dotado el ser humano con un instinto para sobrevivir y perpetuar la especie, de tal forma que en la sociedad el normal es desear vivir, el suicidio siendo considerado un trastorno mental.

> *"La máxima metafísica aplica tanto al mundo físico, como al mundo virtual. Desde cierto punto de vista, el primero de todos los derechos es el derecho a existir, a la vida; sin vida no hay derecho que se pueda reclamar. Lo mismo en*

[466] Autores como David Vallespín Pérez, Franz Matcher, Antonio Pérez Luño, Augusto Mario Morello, Robert B. Gelman, Javier Bustamante Donas y Juan Carlos Riofrío Martínez-Villalba afirman que está surgiendo una cuarta generación de derechos humanos, los derechos digitales.

el campo digital: quien no tiene derecho a existir en el ciberespacio, en la práctica no tiene ningún derecho digital. Por eso este es el primero de los derechos digitales"[467].

Dependiendo de sus capacidades cognitivas y más que este dependiendo de los recursos informáticos efectivos, el ser humano elige el momento de iniciar su vida digital. Aunque en su vida real una persona tiene diferentes características impuestas por sus códigos genéticos, en la vida digital él puede elegir libremente sus características, incluso reinventase de una forma única, totalmente distinta de su personalidad real.

Esta personalidad virtual representa según Chinchilla Sandí, "*el desdoblamiento del ser humano en su materialidad física y su desmaterialización virtual de información (principio de ubicuidad), donde esta personalidad virtual conformada en forma absoluta de información se encuentra regulada por cada persona y será considerada como centro de atribución o imputación de efectos jurídicos*"[468]

La vida digital nace en un momento deseado, elegido y depende exclusivamente de la voluntad del individuo sobre el nivel de exposición que elige tener en el ciberespacio.

El derecho a la existencia virtual es diferente a otros derechos, como por ejemplo el derecho a la identidad digital o el derecho al domicilio digital. Una cosa es simplemente "existir", otra "existir de un modo determinado" y otra "actuar de un modo determinado".

El derecho a la existencia digital se puede definir como la capacidad del individuo a conectarse, a estar presente y manifestarse en la red virtual global de una manera que el libremente la elige[469].

Existir digitalmente o manifestarse virtual puede tener varias formas: publicando "cosas del yo" en una plataforma, red o aplicación informática (contenido multimedia, textos proprios) o simplemente crear una cuenta para visualizar el contenido agregado por los demás usuarios y navegar, sin añadir un contenido digital proprio.

El derecho a la existencia digital no es idéntico con el derecho a conectarse a Internet por un período determinado y sin utilizar una cuenta propria. Es el caso de la plataforma Google que permite navegar en Internet de forma incognito. El derecho a existir digitalmente implica obligaciones del "ser digital" como por ejemplo el de

[467] Riofrío Martínez-Villalba, Juan Carlos (2014) *La cuarta ola de derechos humanos: los derechos digitales.* Revista Latinoamericana de Derechos Humanos no.15, pg. 3.
[468] Chinchilla Sandí, C (2005) *Personalidad virtual: necesidad de una reforma constitucional*. Revista de Derecho Informático, ISSN-e 1681-5726, no. 82/2005, p. 5.
[469] Riofrío Martínez-Villalba, Juan Carlos (2014) idem.

navegar, de una forma abierta y transparente, conectado con una cuenta propia, en ciertos sitios Web por varias razones, la mayoría relacionadas con un fin económico. En este sentido el mundo virtual es parecido al mundo digital, una vez que has nacido existen algunas obligaciones que no puedes rechazar (regístrate, pagar impuestos, tener un domicilio, responder a las encuestas de las autoridades etc.)

Podemos decir que los otros derechos digitales no pueden existir fuera del derecho a la vida digital. Si el individuo no nace de forma digital (no está registrado en algún sitio web), tampoco no puede pedir a tener otros derechos en línea. Por ejemplo, el derecho a una identidad digital, al testamento digital o a la libertad de expresión no se pueden manifestar si no están vinculados estrechamente a un determinado ser digital. El desconocimiento de este primer derecho es el desconocimiento de todos los derechos digitales.

5.2. El derecho a la identidad digital

El derecho a la identidad digital representa la capacidad de una persona a tener un nombre y una identidad dentro de la sociedad o comunidad. Si el derecho a la identidad de la persona está previsto en todas las constituciones, normas internacionales y convenios sobre los derechos humanos, el derecho a la identidad virtual no goza de una consagración legal similar, ni de garantías legales.

Todo usuario registrado en línea tiene derecho a una identidad virtual determinada (nombre, código, *nick-name*). La identidad es el atributo que identifica a alguien dentro de una comunidad, no importa si es virtual o real. Por eso, si la identidad en general se basa en los rasgos, opiniones, comportamiento de la persona, que permiten a identificar a su autor, de modo analógico consideramos la identidad digital está compuesta por aquellas informaciones agregadas al perfil digital (fotos, publicaciones, manifestaciones como *like* o *dislike*, datos personales) que nos ayuda a individualizar a la persona que se manifiesta en el entorno online:

> *"La identidad digital es la expresión electrónica del conjunto de rasgos con los que una persona, física o jurídica, se individualiza frente a los demás. Los cimientos de la identidad digital se hallan tanto en la creación como en la recopilación de dichos atributos identificativos por su titular o por terceros. Así, podemos asumir como identidad digital desde el perfil que un usuario de Facebook se crea a sí mismo en dicha red social, hasta la ficha en la que una entidad bancaria mantiene actualizados en formato electrónico los datos personales de uno de sus clientes. En ambos casos se asimila la identidad digital*

al conjunto de datos que identifican o a través de los cuales se puede llegar a identificar a una persona"[470].

Del mismo modo que la identidad física se forma mezclando rasgos innatos con atributos fabricados durante la vida, también la identidad digital se construye principalmente usando características deseadas, diferentes de los rasgos reales, pero en estrecha conexión con la personalidad real de individuo que elige existir en el mundo virtual.

Al mismo tiempo existen plataformas, redes o sitios web que no permiten al usuario crear una identidad virtual como le apetecería porque ofrecen una paleta limitada de características (pelo, ropa, complementos predefinidos). En este sentido se pueden estudiar las plataformas de Roblox y Minecraft. La voluntad de la persona es la que determina la existencia digital y el derecho a tener una identidad en el mundo virtual pero los rasgos digitales no dependen exclusivamente de la elección del usuario. Las normas que protegen la imagen de las personas en el mundo real se aplican también en el mundo virtual: por ejemplo, no puedes usar las fotos o la identidad de otro usuario para robar sus fanes o porque te gustaría ser aquella persona.

No importa si los rasgos son real o elegidos, al final un usuario elige tener algunas características porque tiene una cierta personalidad, un cierto comportamiento que determina sus elecciones en materia de identidad virtual. De esta forma, la identidad virtual no puede ser muy diferente de la identidad física, por lo menos en el caso de las personas sanas desde un punto de vista mental.

El mundo virtual permite fragmentar y mezclar los rasgos, pero no pueden destruir la identidad real. La fragmentación se produce cuando un usuario navega sin "identificarse", manifestando únicamente alguna característica, atributo o preferencia suya: por ejemplo, visualizar algunas páginas web, algunos artículos en venta online, comprar unos billetes o buscar información sobre alguna cuestión que lo interesa o lo preocupa. En estos casos, la identidad digital se construye a base de los interese del usuario sin añadir rasgos físicos. Actualmente, la tecnología permite unificar la identidad fragmentada de los cibernautas por intermedio de las cookies, sin que el usuario se da

[470] Burgueño P. F. (2012) Aspectos jurídicos de la identidad digital y la reputación online, adComunica. Revista de Estrategias, Tendencias e Innovación en Comunicación, 2012, nº3, p. 127.

cuenta de lo que pasa detrás de las páginas web visitadas. Esta tecnología utiliza sistemas como el OpenID[471].

Los analistas han determinado dos tipos de rasgos digitales que pueden ser identificados: los que pertenecen al core identity (identidad principal o básica) y los que no. Los primeros vinculan la identidad digital con la física, como las informaciones personales de un usuario estrechamente conectados con su existencia real que se pueden digitalizar para crear la identidad digital de la persona (nombre, residencia, IP de ordenador/dirección del lugar de donde se conecta, huellas o rasgos físicos, si se conecta a su equipamiento informático usando el método de reconocimiento facial). Otros datos que son creados por el usuario no permiten la vinculación entre la persona digital y la persona real: el nick-name, el avatar, las búsquedas de información, la adopción de un nombre de usuario y de una clave, los algoritmos de las claves públicas y privadas. Si el usuario no utiliza su nombre, su foto o sus datos biográficos reales, es muy difícil vincular el perfil digital con la identidad real del usuario.

A diferencia del mundo real, donde el derecho a la identidad no goza de mucha atención por ser menos expuesto a las violaciones comparado con otros derechos fundamentales, el derecho a la identidad digital ha adquirido una importancia significante por ser muy expuesto a violaciones como el robo de identidad, infracciones digitales usando perfiles de personas inocentes, ataques informáticos que cambian los datos de los usuarios. En parte, este derecho digital fundamental se ha superado al mundo físico, donde la identidad a veces se confunde con otros derechos aledaños, como el derecho a la imagen, al honor o a la intimidad:

> *"La creciente protección jurídica de la identidad digital de las personas físicas está conformando un nuevo derecho que pretende integrar el elenco de los derechos de la personalidad. De esta forma, el derecho a la identidad digital, esto es, el derecho a existir en Internet, a poder tener un perfil en redes sociales*

[471] Según Rubén De León-Peña y Miguel Vargas-Lombardo, el protocolo "OpenID Connect representa un esfuerzo no sólo hacia la definición de protocolos abiertos, sino hacia la descentralización de la gestión de identidad y de datos personales". Con el OpenID un usuario se puede identificar en una página web a través de una URL (o un XRI en la versión actual) y puede ser verificado por cualquier servidor que soporte el protocolo. "En los sitios que soporten OpenID, los usuarios no tienen que crearse una nueva cuenta de usuario para obtener acceso. En su lugar, solo necesitan disponer de un identificador creado en un servidor que verifique OpenID, llamado proveedor de identidad o IdP. El proveedor de identidad puede confirmar la identificación OpenID del usuario a un sitio que soporte este sistema. Actualmente es bastante natural que cada persona almacene un buen número de login-name y claves, que se acumulan a lo largo de la vida digital". Texto disponible en: https://arxiv.org/pdf/1502.00134.pdf.

y a no ser excluido de éstas, a recibir resultados en búsquedas vanidosas y a poder ejercitar para su perfil online los mismos derechos que tiene para el offline, quiere asimilarse al derecho a tener un nombre y, salvando la enorme distancia, a tener y desarrollar una vida, aunque sea en versión digital. Por otro lado, el respeto a su imagen, su intimidad y su honor, unido al ejercicio del derecho de protección de datos aplicado a la web social, está configurando vías rápidas de defensa de los derechos fundamentales de la personalidad por medio de procesos encuadrados bajo la denominación de derecho al olvido, para permitir que el usuario mantenga el control sobre el tratamiento electrónico de la identidad digital y reputación online de su persona"[472].

5.3. El derecho a la reputación digital

"La identidad es lo que yo soy o pretendo ser o creo que soy. La reputación es la opinión que otros tienen de mí. Se forma con base en lo que yo hago y lo que yo digo, pero también a lo que otros perciben de mis actos o palabras, a cómo lo interpretan y a cómo lo transmiten a terceros"[473].

La reputación es la dimensión objetiva del derecho fundamental al honor, un derecho que goza de suficientes garantías legales y procesales. En los tribunales civiles o penales no faltan los casos determinados por los delitos de las injurias o por las calumnias. La ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen establece el marco legal general aplicable a estos derechos, incluyendo el componente económico del derecho a la propia imagen, pero no formula definiciones claras y comprensivas para ninguno de estos derechos, dejando a los jueces la interpretación y extensión de la norma legal para cubrir las lagunas legislativas identificadas en cada caso. Por estas razones, la jurisprudencia pertinente es abundante y en continua evolución. En este sentido, el Tribunal Constitucional Español ha fallado que:

"*en nuestro ordenamiento no puede encontrarse una definición de tal concepto [del honor], que resulta así jurídicamente indeterminado (...). El denominador común de todos los ataques o intromisiones (...) en el ámbito de protección de este derecho es el desmerecimiento en la consideración ajena como*

[472] Pablo Fernández BURGUEÑO (2012) idem, p. 139.
[473] ALONSO, J. (2011) *Identidad y reputación digital*. En P. Cerezo (Ed.), Cuadernos de comunicación Evoca, 5. Identidad digital y reputación online (págs. 5-10). Madrid, España

consecuencia de expresiones proferidas en descrédito o menosprecio de alguien o que fueren tenidas en el concepto público por afrentosas"[474].

El tema del honor, como derecho humano, ha incitado siempre la doctrina jurídica y también a los filósofos del derecho, pero la nueva realidad social ha aumentado los debates sobre el tema con la aparición de la reputación digital o reputación on-line. Sin embargo, la reputación on-line tiene una serie de diferencias que la desmarcan del concepto de reputación más clásico o físico. En primer lugar, la reputación online es acumulativa en el tiempo porque la memoria de internet es infinita en comparación con la memoria de las comunidades que es limitada en tiempo. Cualquier contenido colgado en Internet o acción en la red de redes dejan un rastro o una huella, difícil de borrar.

Nuestra reputación en el ámbito digital se genera a través de una gran cantidad de datos de carácter personal que pueden ser localizados con extrema facilidad incluso sin que seamos conscientes de dicha situación. En segundo lugar, el alto grado de alcance de la información (una foto o una publicación en las redes puede ser visualizada en unos minutos por millones de personas) y la repercusión puede ser más fuerte que en el mundo real. Cualquier internauta se encuentra capacitado para propagar información y opiniones a través de Internet que a su vez pueden localizarse fácilmente y, peor aún, difundirse rápidamente a través de la red.

El derecho a la reputación debe gozar de la misma protección tanto en el mundo físico como también en el ciberespacio. El Internet es, por su naturaleza, un "mundo de exposición", y por esta razón la reputación está más expuesta, lo que no es siempre una situación mala. Solamente con apretar un icono de *like* o *dislike*, o añadir un comentario a una publicación, se puede influir de modo negativo o positivo la reputación de la persona que expone sus fotos o sus opiniones en el entorno digital. Igual que en la sociedad clásica, a veces la crítica es constructiva y permite la corrección de algunos malos comportamientos. Pero existen situaciones cuando personas mal intencionadas utilizan el entorno digital para destrozar la competencia usando métodos desleales. Por ejemplo, algunos empresarios, usando falsos perfiles, agregan en la página web de la competencia comentarios maliciosos o erróneos sobre los productos comercializados, afectando la reputación de la compañía y el número de clientes. Por otro lado, hay falsos perfiles creados por las empresas que elogia de una manera exagerada los productos o los servicios ofrecidos por estas, para engañar a los consumidores. A diferencia del mundo

[474] Tribunal Constitucional Español, Sentencia 223/1992, de 14 de diciembre (BOE núm. 16, de 19 de enero de 1993) ECLI:ES:TC:1992:223;

físico, en el mundo digital la notoriedad es fácil de cuantificar porque las aplicaciones informáticas permiten visualizar en tiempo real los comentarios de los clientes, los *likes* o *dislikes*, los seguidores de la página, etc. El único problema es como hemos mencionado, los falsos perfiles o el uso de varios IP para comentar en las páginas web que se quieren promover o denigrar.

El derecho a la reputación tiene una característica interesante: no puede relacionarse con los parámetros sociales específicos de la comunidad real del usuario. La jurisprudencia relacionada con las afectaciones del derecho a la reputación demuestra que, al juzgar los casos de violación del derecho a la reputación, los jueces utilizan parámetros específicos a la sociedad o comunidad donde desarrollan su actividad. En el entorno online, tales parámetros se diluyen, porque las comunidades se mezclan. Por ejemplo, un musulmán se puede sentir ofendido por algunas palabras o expresiones que para un europeo no significan nada. En este sentido es elocuente el caso Charlie Hebdo, donde unas caricaturas inofensivas para los franceses han determinado y continúan determinar ataques terroristas sobre personas que se consideran inocentes a publicar en Internet las caricaturas del Profeta. Todos estos ejemplos nos hacen pensar que el derecho a la reputación digital tiene una autonomía propia, aunque se fundamenta en el derecho al honor y a la honra.

5.4. El derecho a la libertad de expresión y a la responsabilidad digital

El Internet, como espacio abierto y atemporal es un campo de batalla entre diversas opiniones, culturas, religiones y no últimamente, derechos fundamentales. Las publicaciones que circulan sin fronteras, frutos de la libertad de expresión, afectan valores, principios y derechos, a veces sin que los autores sean conscientes del daño que pueden producir.

Este conflicto de los derechos puede ser un asunto difícil de tratar para los jueces o los teóricos en el ámbito del Derecho porque la línea de demarcación entre varias libertades del individuo es tan fina que a veces no se puede encontrar el punto de equilibrio entre los intereses legítimos de las personas. Por estas razones, los conflictos entre la libertad de expresión y la protección del honor se deben analizar cada uno en su contexto social y temporal caso por caso, estableciendo si los comentarios, las palabras o los gestos tienen connotación negativa, denigrante o vejatoria con relación a una persona o a un grupo de personas.

La libertad de expresión significa la posibilidad del ser humana a publicar sus ideas y las manifestaciones de su conciencia o de su pensamiento. La Real Academia Española lo define como el "*derecho de manifestar y difundir libremente ideas, opiniones o informaciones*" que, en nuestro caso, se produce a través de las redes sociales. Este nuevo instrumento digital de expresión tiene la capacidad de ilimitado en tiempo y espacio, el más eficiente vehículo de difusión que ofrece garantías de anonimato y no discriminación.

Según varios autores[475]: "*el derecho a la libertad de expresión tiene dos dimensiones: una individual y una colectiva. La dimensión individual faculta a cada persona para expresar sus pensamientos, ideas, opiniones, informaciones o mensajes; la dimensión colectiva faculta a la sociedad a buscar y recibir tales pensamientos, ideas, opiniones, informaciones y mensajes*".

En el entorno online estas dos dimensiones se manifiestan sin límites espaciales y temporales. No existen barreras naturales y si se intenta poner límites digitales al derecho de expresión los activistas se rebelan pidiendo justificación y libertad incondicionada. En Internet está gobernado además por el principio de clausura, según lo cual está permitido todo lo que no está prohibido. Hasta ahora no existe un acuerdo sobre que rama de derecho es más apropiada a regular las relaciones entre los usuarios y si es posible designar algunas autoridades digitales que vigilen las conductas de los internautas.

Las dos dimensiones del derecho tienen igual importancia jurídica, son interdependientes, y deben ser garantizadas y protegidas por el Estado, según han explicado la Corte Interamericana de Derechos Humanos:

> *"Las dos dimensiones mencionadas de la libertad de expresión deben ser garantizadas simultáneamente. No sería lícito invocar el derecho de la sociedad a estar informada verazmente para fundamentar un régimen de censura previa supuestamente destinado a eliminar las informaciones que serían falsas a criterio del censor. Como tampoco sería admisible que, sobre la base del derecho a difundir informaciones e ideas, se constituyeran monopolios públicos*

[475] Botero Marino, C. y otros (2017) *El derecho a la libertad de expresión. Curso avanzado para jueces y operadores jurídicos en las Américas*. Guía curricular y materiales de estudio, Editorial Centro de Estudios de Derecho, Justicia y Sociedad, disponible en: https://www.dejusticia.org/wp-content/uploads/2017/07/El-derecho-a-la-libertad-de-expresi%C3%B3n-PDF-FINAL-Julio-2017-1-1.pdf.

o privados sobre los medios de comunicación para intentar moldear la opinión pública según un solo punto de vista"[476].

Por otro lado, la libertad digital tiene un alcance mayor la libertad de expresión clásica, porque la difusión de ideas es aumentada en el ciberespacio. Las personas pueden publicar, bajo su propria responsabilidad, cualquier idea que tenga en mente. En los medios de comunicación antiguos (es decir justo ante de la aparición de www y social media) no era posible publicar sin obtener la permisión del editor o redactor o sin pagar algunos costes de difusión. En nuestros días, solo con tener acceso al Internet, es posible crear un blog, una página propia en internet, un foro de discusiones donde se puede publicar cualquier idea, sea bien fundamentada o superficial. Esta libertad implica también una grande responsabilidad porque estas publicaciones pueden llegar a cualquier rincón del mundo y pueden producir efectos sobre las personas.

En lo que concierne la responsabilidad sobre el contenido publicado en las redes sociales siempre hay unos debates sin soluciones convergentes. De un lado se encuentran los juristas que atribuyen la responsabilidad a las redes – Facebook, Twitter, Linkedin etc. – y del otro lado existen voces que abogan por la responsabilidad del usuario que ha colgado el contenido ilegal. En nuestra opinión, la responsabilidad debe ser analizada en cada caso de forma individual. Si, por ejemplo, se demuestra que un contenido ilegal (*incitación al odio o a la discriminación en base de religión, etnia, sexo, enfermedades etc; incitación a violencias y manifestaciones ilegales; denigración de una persona con violación de su vida priva*da) podría ser eliminado por la red de host que conocía o debería conocer el carácter ilegal de la publicación (existencia filtros de palabras claves), entonces la red es responsable junto con el usuario que ha publicado el contenido ilegal. Es decir que no existe responsabilidad compartida solo cuando los administradores de la red no conozcan de forma efectiva que se ha producido la vulneración de los derechos fundamentales de una persona y actúan con la diligencia suficiente para minimizar los daños en la víctima.

En este sentido, en el Asunto C-18/18[477], *Eva Glawischnig-Piesczek contra Facebook Ireland Limited*, el Tribunal de Justicia de la Unión Europea resaltó que, si una

[476] Corte Interamericana de Derechos Humanos (1985) Opinión consultiva OC-5/85 del 13 de noviembre de 1985. La colegiación obligatoria de periodistas (arts. 13 y 29 Convención Americana sobre Derechos Humanos), disponible en: http://cdh.defensoria.org.ar/wp-content/uploads/sites/10/2018/03/OPINION-CONSULTIVA-5.pdf.

[477] C-18/18 - Glawischnig-Piesczek; Sentencia del Tribunal de Justicia (Sala Tercera) de 3 de octubre de 2019 (petición de decisión prejudicial planteada por el Oberster Gerichtshof — Austria) — Eva Glawischnig-Piesczek / Facebook Ireland Limited) ECLI:EU:C: 2019:458

red social *"facilita la transmisión rápida entre sus diferentes usuarios de información almacenada por el prestador de servicios de alojamiento de datos, existe un riesgo real de que una información que ha sido declarada ilícita sea reproducida y compartida posteriormente por otro usuario de la red"*.

Como solución, el Tribunal ha decidido imponer una obligación para el administrador de la red de limitar la propagación de la información ilícita que viola los derechos fundamentales de las personas:

> *"Por lo tanto, con el fin de prevenir cualquier infracción futura, puede obligarse a un prestador de servicios de alojamiento de datos, mediante requerimiento judicial, a retirar información ilícita que aún no haya sido difundida en el momento de la adopción de dicho requerimiento, sin necesidad de que la difusión de dicha información se ponga en su conocimiento de nuevo y al margen de la solicitud inicial"*[478].

En una reciente sentencia del Tribunal Supremo[479] se explica que, incluso, ciertas expresiones no se pueden enmarcar dentro de la libertad ideológica o de expresión y sí dentro del llamado discurso del odio:

> *"En efecto, compartimos con el Tribunal de apelación que las expresiones que se propagan por las redes sociales, a cargo de los mensajes elaborados por el recurrente, se refieren claramente a una actividad de alabanza y justificación de los medios violentos y una invitación a la utilización de métodos terroristas, elogiando el asesinato de policías y banqueros como algo necesario. Su potencialidad de riesgo abstracto se desprende de los propios mensajes*".

La resolución del Tribunal demarca claramente la intención de la justicia de combatir actuaciones y comportamientos que ocasionan un grave quebranto en el régimen de libertades y daño en la paz de la comunidad y no trata de criminalizar opiniones críticas o pensamientos individuales.

En términos genéricos, las redes sociales son canal donde se pueden perpetrar los mismos delitos y realizar las mismas conductas que en cualquier otro lugar; por tanto, no tienen una regulación específica, salvo para algunos delitos tecnológicos o informáticos. La diferencia es que proporciona una mayor difusión o publicidad a los actos, por un lado, y el peculiar "lugar del crimen", por otro.

---

[478] Idem, parágrafo 44.
[479] Tribunal Supremo, Sentencia núm. 185/2019, STS 1070/2019 - ECLI: ES:TS:2019:1070.

5.5. La privacidad virtual y el derecho al olvido

El respeto de la vida privada es una de las principales preocupaciones de los usuarios de las nuevas tecnologías porque la gran cantidad de datos personales que se suelen cargar en el entorno online es muy expuesta a los fenómenos como el spam o el phishing que pueden poner en riesgo la información personal de los internautas.

El concepto que existe en Estados Unidos es el de *right to privacy*, que en su traducción al español no se corresponde totalmente con el concepto de derecho a la privacidad, puesto que *privacy* es una noción que tiene más relación con la intimidad o con el derecho a ser dejado en paz (right to be let alone[480]), pero con ciertas diferencias jurídicas con respecto a los derechos protegidos en el ámbito europeo o español.

La actual preocupación jurídica es, si el Internet es compatible con un tal derecho fundamental teniendo en cuenta la apertura y la capacidad de almacenaje que tiene el espacio virtual.

La variedad de niveles de exposición digitales permite la plena manifestación de este derecho incluso en las redes sociales, porque en el mundo virtual el grado de exposición depende de la intención y de la voluntad del usuario que decide publicar en línea la información. Colgar una noticia en la red abierta, que es accesible para todos los usuarios sin restricciones, lleva más riesgos que ponerla en la deep Web, donde solo determinadas personas tienen acceso (los usuarios registrados, los que tienen código de acceso, etc.). Los usuarios que deciden publicar contenido personal en la red abierta están conscientes que su vida privada se transpone en un contexto comunicacional de absoluta exposición. En este contexto el mejor consejo es la célebre frase de Dennis O'Reilly:
"La mejor manera de proteger tu privacidad en la red es asumir que no la tienes y modificar tu comportamiento en línea de acuerdo con ello"[481].

En la práctica se han distinguido dos principios cuya aplicación garantiza un mínimo de protección en un contexto comunicacional diverso. En general, los usuarios deben aplicar el principio del mínimo pedido de información (*least reveling means*), especialmente cuando se le pide información sensible. Incluido la compilación y tratamiento de datos de identidad fragmentada puede determinar violaciones del derecho a la privacidad virtual y el usuario debe ser notificado cuando se le solicita y almacenan estos tipos de datos personales. En otros casos, como el comercio online, es mejor aplicar

[480] Warren, S. D. & Brandeis, L. D. (1890) idem.
[481] O'Reilly, D. (2007). "*Five ways to protect your privacy online*",
disponible en: https://www.cnet.com/news/five-ways-to-protect-your-privacy-online/.

el principio de la información más útil (*most convenient means*) porque los clientes necesitan información para elegir un determinado producto. Aunque están buscando un producto genérico, a la hora de elegir una marca, el usuario será tentado a elegir el producto mejor presentado y descrito. En síntesis, el derecho a la privacidad virtual representa un escudo de protección para el cibernauta de buena fe, impidiendo que su información se desvela más allá de lo prudente y legítimamente previsto.

El derecho a la privacidad virtual está directamente relacionado con el derecho al olvido o al derecho al anonimato. Pero, estos últimos derechos siguen siendo dos temas que separan las opiniones jurídicas en dos campos de debates. Por un lado, existen los juristas que abogan por el derecho a que la gente se olvide de lo que hicimos en la red y por el otro lado hay los juristas que apoyan el derecho a ser informado sobre todos los asuntos relacionados con las personas públicas o los temas de interés público. Al final, la que decide es la red.

El mundo virtual es por su naturaleza, un mundo de exposición, y por esta razón es difícil, cuando no imposible, borrar todo rastro dejado ahí [482]. Borrar todas las huellas dejadas en las páginas web resulta especialmente difícil en Internet[483].

En un caso histórico, Google España contra Costeja[484], el Tribunal Europeo de Justicia (TJUE) dictaminó que un motor de búsqueda de Internet es responsable del tratamiento de los datos personales que lleva a cabo y que aparecen en páginas web publicadas por terceros, aclarando que "*la actividad de un motor de búsqueda, que consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia determinado, debe calificarse como tratamiento de datos personales, en el sentido del artículo 2, letra b) de la Directiva 95/46 /CE, cuando esa información contiene datos personales*" y esta calificación responsabiliza al gestor de un motor de búsqueda para el tratamientos de estos datos

[482] Bowden, J. (2014). *Reasons to explore big data with social media analytics*. Recuperado de: https://www.socialmediatoday.com/content/reasons-explore-big-data-social-media-analytics-videos .

[483] El Internet Archive (Archivo de Internet) es "una biblioteca digital gestionada por una organización sin ánimo de lucro dedicada a la preservación de archivos, capturas de sitios públicos de la Web, recursos multimedia y también software. Creada en 1996, se encontraba desde esa fecha y hasta el año 2009 en el histórico Presidio de San Francisco (California) y, desde ese año, se halla en la calle Funston en San Francisco (California). Para encontrar une versión antigua de una página web, archivada, los usuarios deben escribir una dirección URL y seleccionar las fechas deseadas, y el servicio le abre la versión archivada de la Web a esa fecha". Texto disponible en: https://archive.org/about/.

[484] El caso *Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González*. Identificador Europeo de Jurisprudencia: ECLI:EU:C:2014:317

personales. En este caso, el tratamiento de datos por los motores de búsqueda "*debe diferenciarse y es adicional al que realizan los editores de sitios web de terceros*"[485].

Poco después de Google España, el Parlamento Europeo adoptó el nuevo Reglamento General de Protección de Datos (RGPD), que incluye una disposición sobre el derecho al olvido (también conocido como el derecho al borrado), con pasos específicos para que los responsables del tratamiento borren la información a petición. Además, de acuerdo con el artículo 18 del RGPD, conocido como "derecho de restricción":

> *"El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:*
>
> *a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de estos;*
>
> *b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;*
>
> *c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;*
>
> *d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado".*

Cuando el procesamiento está restringido, los controladores de datos pueden almacenar los datos personales, pero no procesarlos más. El responsable del tratamiento debe hacer que los datos sean inaccesibles, en lugar de eliminarlos por completo como en el caso del derecho al olvido. En cuyo caso, el interesado tiene derecho a ser borrados en varias circunstancias específicas, incluso cuando "los datos personales ya no son necesarios en relación con los fines para los que fueron recopilados o procesados".

5.6. El derecho al domicilio digital

La jurisprudencia internacional abunda en sentencias sobre la inviolabilidad del domicilio, pero en la doctrina no hemos identificado una definición del domicilio digital.

[485] Frosio, G. (2017) Right to Be Forgotten: Much Ado About Nothing , Colorado Technology Law Journal 307 (2017), disponible en SSRN: https://ssrn.com/abstract=2908993.

Según el artículo 40 del Código Civil Español: "*para el ejercicio de los derechos y el cumplimiento de las obligaciones civiles, el domicilio de las personas naturales es el lugar de su residencia habitual, y, en su caso, el que determine la Ley de Enjuiciamiento Civil"*. En lo que concierne el domicilio de las personas jurídicas el articulo 41 estipula que: "*cuando ni la ley que las haya creado o reconocido ni los estatutos o las reglas de fundación fijaren el domicilio de las personas jurídicas, se entenderá que lo tienen en el lugar en que se halle establecida su representación legal, o donde ejerzan las principales funciones de su instituto*".

Conforme al Nuevo Código Civil Rumano, el domicilio de la persona natural, para el ejercicio de sus derechos y libertades civiles, es donde declara que tiene su residencia principal (artículo 87). En caso de un domicilio desconocido la ley considera que el lugar de residencia puede ser considerada domicilio. Si tampoco no se puede establecer el lugar de residencia se considera que la persona esta domiciliada en el lugar donde se halla (artículo 90).

El domicilio de la persona y su inviolabilidad están protegidos en los convenios internacionales, en las constituciones de los estados y en las leyes civiles y penales de la mayoría de los estados.

Como ha señalado el Tribunal Constitucional Español: "*la idea de domicilio que utiliza el art. 18 de la Constitución no coincide plenamente con la que se utiliza en materia de Derecho Privado y en especial en el art. 40 del Código Civil como punto de localización de la persona o lugar de ejercicio por ésta de sus derechos y obligaciones.[…] la protección constitucional del domicilio es una protección de carácter instrumental, que defiende los ámbitos en que se desarrolla la vida privada de la persona. Por ello, existe un nexo de unión indisoluble entre la norma que prohíbe la entrada y el registro en un domicilio (art. 18.2 de la Constitución) y la que impone la defensa y garantía del ámbito de privacidad (artículo 18.1 de la Constitución). Todo ello obliga a mantener, por lo menos prima facie un concepto constitucional de domicilio de mayor amplitud que el concepto jurídico privado o jurídico-administrativo*" [486].

Partiendo de las reglamentaciones sobre el domicilio físico, podemos interpretar las mismas normas en el caso del domicilio digital con el fin de concederle la misma protección y garantías legales. Dentro de unos años es previsible que la protección constitucional se puede abrir al domicilio digital. Por analogía, podemos definir el

[486] Tribunal Constitucional Español, Sentencia 22/1984, de 17 de febrero (BOE núm. 59, de 09 de marzo de 1984) ECLI:ES:TC:1984:22;

domicilio digital como "*aquel lugar donde la persona reside digitalmente; es aquel sitio donde tiene derecho a permanecer virtualmente, a que nadie entre sin su voluntad, e implica el derecho a que no sea destruido su hogar"*[487].

Los internautas suelen almacenar, publicar, compartir información sobre su vida privada en sus páginas o cuentas de Facebook, Twitter Tik Tok, Instagram o MySpace, donde ellos existen virtualmente. Estas aplicaciones informáticas ofrecen a los usuarios la posibilidad de elegir los internautas que pueden visualizar su página. Otro domicilio digital es la "nube" (cloud), donde personas físicas o jurídicas almacenan una gran cantidad de datos personales, comerciales, económicas muy sensibles y, por esta razón tienen el legítimo derecho a la inviolabilidad de su sitio. Podemos decir que las personas naturales o jurídicas que mantienen un nombre de dominio en la red tienen un domicilio digital.

Como conclusión, se afirma que el derecho a la inviolabilidad del domicilio digital es un derecho autónomo, distinto del derecho al secreto de las comunicaciones. Este último no tiene la capacidad para proteger los datos que no circulan, que no se comunican y quedan guardados en una nube, por ejemplo, porque no son comunicaciones, sino bienes digitales que pertenecen a un ser fisio o a un ser digital. Por estas razones es de gran importancia conceptualizar y defender el derecho al domicilio digital y su inviolabilidad.

5.7. El derecho al big-reply

Según el diccionario Cambridge[488], el término "reply" significa contestar, reaccionar a una acción, actitud o estimulo, responder a una carta. En lenguaje informático el "reply" puede también ser sinónimo del "replicar", "repetir", volver a publicar. Con la aparición de las redes sociales los usuarios suelen repetir o volver a publicar contenidos colgados en la línea por otros miembros de las plataformas de interacción. Todo usuario tiene derechos al reply, al re-twitt, al forward, al post, pero en las condiciones impuestas por la red o por la plataforma utilizada.

De esta forma una publicación en Facebook de un usuario puede ser difundida miles de veces hasta que llega a otros continentes si el idioma utilizado permite la

[487] Riofrío Martínez-Villalba, J. C. (2014) *La Cuarta Ola de Derechos Humanos: Los Derechos Digitales,* Revista Latinoamericana de Derechos Humanos 25 15 Volumen 25 (1), I Semestre 2014, disponible en: https://www.corteidh.or.cr/tablas/r33897.pdf.
[488] https://dictionary.cambridge.org/es/diccionario/ingles/reply

comprensión del mensaje. Solo al tocar el "compartir" de Facebook el contenido publicado de un amigo puede llegar en un segundo a otros cientos de amigos que tienes en la lista. El derecho de un usuario a compartir, a repetir un mensaje de otro usuario se presume, porque la persona que cuelga la información en Internet está consciente de que se va a propagar y a veces esto representa su objetivo final.

> *"En este contexto, todo cibernauta tiene derecho al reply, a re-twitt, al forward, a la copia, al post, etc. Desde cierto punto de vista también forma parte de este derecho el que tienen los ISP y los usuarios a guardar copias caché de los datos, a fin de poder difundir el mensaje a más gente, en menos tiempo"*[489].

El derecho al big-reply resulta de la psicología de las redes: la necesidad humana de ser famoso, aceptado, adulado, de crear tendencias en algún ámbito. Cuanto más distribuida es tu publicación, más famoso te conviertes, la obsesión de la popularidad es la tendencia natural que impera el comportamiento en la red. El derecho al big-reply no supone imponer mensajes a los demás usuarios de la red, el mensaje se impone por su mismo contenido y la persona que lo visualiza puede elegir a ignorarlo o también a compartir lo con sus amigos. El derecho al big-reply no goza de protección si esta utilizado para compartir enlaces, textos, fotos que contienen virus añadidos que puedan dañar equipos, cuentas, canales, mail boxes.

> *"Por otro lado, el derecho al big-reply del cibernauta debe cumplir con los principios de autenticidad, integridad, precisión y relevancia. Se debe precautelar que el mensaje repetido sea esencialmente el mismo que el original. Además, en el reply deberán constar claramente las debidas indicaciones de autoría"*[490].

La jurisprudencia y la práctica internacional ha demostrado que el derecho a big-reply conlleva sus responsabilidades. Por ejemplo, países como Alemania y Francia han solicitado a las redes sociales el cierre de ciertas cuentas que se dedicaban a repartir en Internet mensajes con contenidos violentes que incitan a odio, racismo, crímenes en masa. Este es el caso del #unbonjuif, una cuenta Twitter que distribuiría en toda Francia una avalancha de mensajes antisemitas.

El caso Twibel de 2011 (acrónimo de Twitter libel, "tweet difamatorio") es muy conocido en el Reino Unido y representa un ejemplo claro de como el derecho al big-reply puede afectar otros derechos fundamentales como el de la reputación o la imagen.

[489] Riofrío Martínez-Villalba, J. C. (2014) *idem.*
[490] Idem.

En este caso, el político británico y ex alcalde de Caerphilly, Gales, Colin Elsbury, recibió una multa por cometer un delito de difamación contra un oponente. La demanda fue presentada por Eddie Talbot, su oponente político, después de que Talbot afirmó que Elsbury había twitteado que Talbot había sido sacado por la fuerza de un lugar de votación por la policía. Bueno, Elsbury definitivamente tuiteó eso, pero, desafortunadamente para él, la persona no era Eddie Talbot. Aunque Elsbury se corrigió rápido y públicamente, Talbot lo llevó a los tribunales y Elsbury fue condenado a pagar una multa de £ 3,000 más costos de alrededor de £ 50,000.

5.8. El derecho a la técnica, al update, al parche

El número de usuarios de Internet ha ido en aumento desde el nacimiento de Internet en la década de 1960. Internet ha cubierto casi todos los aspectos imaginables de la vida moderna. Su apertura e interactividad hacen posible que las personas obtengan más recursos a un costo mucho menor, mientras intercambian ideas y se expresan. La nueva moda es el gran éxito y expansión de las redes sociales como Facebook y Twitter por fuera y WeChat y Weibo por dentro. Facebook, conocida como una de las redes sociales en línea de fama mundial, ha incrementado sus usuarios de 150 millones a 600 millones según las estadísticas. Por medio de estos sitios sociales de Internet, las personas pueden ejercer su libertad de expresión y de expresión de manera activa, lo que lo convierte en el método más eficiente para ampliar la participación ciudadana en la vida pública, a fin de transparentar la información.

Tal y como ha descrito Hamadoun Toure, secretario general de la Unión International de Telecomunicaciones[491] : "En la historia, Internet constituye la fuente potencial de iluminación más poderosa, y el gobierno debería poner Internet como la infraestructura básica, al igual que el tratamiento del agua y los desechos"[492].

El derecho a la técnica significa la capacidad de cualquier individuo a acceder y utilizar la tecnología, los servicios de comunicación electrónica y otras aplicaciones informáticas, a un costo razonable. La Asamblea General de las Naciones Unidas ha declarado el acceso a Internet como un derecho humano[493]:

---

[491] Véase el sitio web de la organización: https://www.itu.int/en/about/Pages/default.aspx

[492] Touré, H. I. (2014) Speech by ITU Secretary-General, *Digital Economy & E-Government: Towards New Digital Opportunities : Opening Speech*, disponible en: https://www.itu.int/en/osg/speeches/Pages/2014-09-24.aspx.

[493] La Rue, F. (2011*) Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, A/HRC/17/27*, disponible en: https://undocs.org/es/A/HRC/17/27.

"En algunos Estados económicamente desarrollados el acceso a Internet se ha reconocido como un derecho. Por ejemplo, el Parlamento de Estonia aprobó en 2000 legislación que declaraba el acceso a Internet un derecho humano básico. En 2009, el Consejo Constitucional de Francia declaró efectivamente el acceso a Internet derecho fundamental, y la Sala Constitucional de Costa Rica adoptó en 2010 una decisión semejante53. Yendo aún más lejos, Finlandia aprobó en 2009 un decreto por el que se establece que toda conexión a Internet debe tener una velocidad mínima de 1 megabit por segundo (en conexiones de banda ancha). El Relator Especial observa que, según una encuesta llevada a cabo por la BBC en marzo de 2010, el 79% de los entrevistados en 26 países consideran que ***el acceso a Internet es un derecho humano fundamental****".*

Este derecho de "acceso al conocimiento", y al "intercambio y desarrollo tecnológico" esta explicado por la Carta de la Asociación para las Comunicaciones progresistas[494] sobre derechos en internet: "*Internet ofrece una extraordinaria posibilidad de intercambio de información y conocimiento, así como nuevas formas de creación de contenidos, herramientas y aplicaciones. Los proveedores de herramientas, servicios y contenidos de internet no deben prohibir a las personas la utilización de internet para compartir el aprendizaje y la creación de contenidos. La protección de los intereses de los creadores debe hacerse de manera coherente con la participación abierta y libre en el flujo de conocimiento científico y cultural"*[495].

Como componentes del derecho a la técnica podemos mencionar el derecho al update, que representa la posibilidad de un usuario a mejorar su programa o tecnología adquirida cuando el productor u otras empresas sacan al mercado versiones actualizadas del producto informático, de tal forma que le permita la interconexión con los demás usuarios:

"Los estándares técnicos que se usan en internet deben mantenerse abiertos para permitir la interoperabilidad y la innovación. Los nuevos desarrollos tecnológicos deben cubrir las necesidades de todos los sectores de la sociedad, sobre todo los que se ven enfrentados a limitaciones y obstáculos cuando están en línea (como las comunidades que usan escritura no latina o las personas con

[494] Véase el sitio web de la asociación: https://www.apc.org/es/sobre-apc
[495] Carta APC sobre derechos en Internet,
disponible en: https://www.apc.org/sites/default/files/APC_charter_ES_1_2.pdf.

capacidades diferentes, las que usan computadores más antiguos y las que carecen de conexiones de alta velocidad)"[496].

Otro derecho importante relacionado con la tecnología es el derecho al parche o al arreglo del producto informático inadecuado o defectuoso adquirido por el usuario. Este derecho protege el consumidor de productos informáticos ante cualquier tipo de comportamiento abusivo de los productores de software, de forma que obliga al vendedor a adaptar al producto informático según las necesidades del usuario:

> *"Las interfaces, contenidos y aplicaciones deben diseñarse para garantizar el acceso a todos y todas, incluso las personas con discapacidades físicas, sensoriales o cognitivas, las personas analfabetas y las que hablan lenguas minoritarias. Se debe promover y apoyar el principio de diseño inclusivo y el uso de tecnologías de asistencia para ayudar a las personas con capacidades diferentes a tener los mismos beneficios que aquellas que no son discapacitadas"*[497].

Teniendo en cuenta que nuestro mundo se vuelve cada día más virtual es importante pensar en los problemas de las personas discapacitas que deben tener las mismas oportunidades para integrarse en el entorno online. El desarrollo de las nuevas tecnologías debe respetar el principio de igualdad, para proteger los intereses de los menos afortunados. La técnica no es un objetivo en ella misma, sino un instrumento al servicio del ser humano. Su creación tiene como fundamento el desarrollo de la persona y la mejora de la vida humana. Pero el derecho a la técnica no sirve si no viene acompañado por un derecho a saber usar esa técnica. Por esta razón, las autoridades son obligadas a pensar medidas concretas para conectar los ciudadanos con la tecnología y enseñarlos a usarla en su propio beneficio.

5.9. El derecho a la seguridad informática y a la paz cibernética

La "paz cibernética", que también se ha denominado "paz digital", es un término que se utiliza cada vez más, pero también sigue siendo un ámbito de escaso consenso. En 1969, el profesor Johan Galtung[498] abrió un nuevo campo de estudios de la paz, argumentando que la paz digital puede definirse como la "ausencia de violencia" en línea. De manera similar, Galtung argumentó que encontrar definiciones universales de los

[496] Idem.
[497] Idem.
[498] Galtung, J. (1969) *Violence, Peace, and Peace*; Journal of Peace Research, Vol. 6, No. 3, pp. 167-191.

términos "paz" o "violencia" era poco realista, pero el objetivo debería ser, encontrar una definición "subjetivista" adecuada aceptada por la mayoría.

Con ese espíritu, la comunidad internacional y el mundo académico se han enfrentado al significado de la paz cibernética. La Unión Internacional de Telecomunicaciones es una agencia especializada de la ONU que se centra en las tecnologías de la información y la comunicación (TIC) y fue pionera en algunos de los primeros trabajos en el campo de los estudios de la paz cibernética junto con el Vaticano y la Federación Mundial de Científicos. Definieron el término como "un orden universal del ciberespacio" construido sobre un "*estado saludable de tranquilidad, la ausencia de desorden, de disturbios y de violencia*"[499]. Aunque es deseable, tal resultado, como el fin de los ciberataques, es técnicamente improbable, al menos en el próximo futuro. Es por eso, la paz cibernética se define no como la ausencia de conflicto en línea, sino como un estado de cosas que puede llamarse paz cibernética negativa. El derecho no goza de un estatuto jurídico claro y la literatura de especialidad continúa dando vueltas a la noción para definir su contenido.

El término "paz cibernética" no se puede confundir con la seguridad informática o la seguridad cibernética, porque estas nociones corresponden a otras situaciones relacionadas con la estabilidad del funcionamiento del hardware y del software[500] o con la seguridad de los usuarios que se manifiestan en línea. La paz es un principio del derecho internacional y un alto valor de la humanidad y por estas razones debe ser protegido tanto en el entorno real como también el virtual. Las autoridades estatales o supraestatales deben garantizar el derecho a la paz cibernética pensando normas y mecanismos efectivos de protección.

5.10. El derecho al testamento digital

Un "testamento digital" es la cantidad de datos electrónicos que un usuario deja en los medios de datos y en Internet cuando muere. Estos incluyen perfiles en redes sociales, cuentas en línea, bandejas de entrada de correo electrónico, almacenamiento en

[499] Wegener, H. (2011) *Cyber Peace. A concept of Cyber Peace* en The Quest for Cyber Peace (cood. Hamadoun I. Touré), disponible en: https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf.

[500] En concreto, la seguridad informática es una parte de la ciencia informática que se enfoca en la protección de la infraestructura computacional. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas.

la nube, licencias, procesos de chat, medios, moneda criptográfica y más, y todos generalmente están protegidos con contraseña. El legado digital es un tema comparativamente nuevo en la ley de sucesiones y plantea desafíos tanto para los legisladores como para los consumidores y familiares.

Una persona de condición media pasa una parte esencial de su vida en Internet y deja una gran cantidad de información confidencial en forma de documentos, archivos, imágenes, videos y mucho más. Si muere inesperadamente, sus perfiles en línea y otros contenidos en Internet siguen activos y sobreviven. Las contraseñas generalmente solo las conoce la persona fallecida. En este caso, es mucho más difícil para los familiares cuidar adecuadamente el legado digital. Por eso se recomienda administrar el patrimonio digital a lo largo de la vida. Esto es especialmente importante cuando almacena documentos confidenciales en línea (utilizando un servicio en la nube, por ejemplo) o cuando está realizando correspondencia importante por correo electrónico. En el caso de una muerte súbita, a menudo es muy importante que se pueda acceder a los mensajes y archivos privados.

Para la mayoría de los perfiles en línea, por ejemplo, tiene sentido desactivarlos o convertirlos en páginas conmemorativas. En 2012, la red social Facebook registraba más de treinta millones de cuentas de usuarios que habían fallecido. El almacenamiento de datos puede contener documentos y archivos importantes para familiares. Tiene sentido establecer una respuesta automática para las direcciones de correo electrónico de uso frecuente, de modo que las personas de contacto sepan que la persona a la que están tratando de comunicarse ha fallecido y, si es necesario, pueden ser remitidos a otra persona. O la cuenta podría simplemente eliminarse, por supuesto. Varias organizaciones han pensado en soluciones al respecto.

Por ejemplo, la plataforma de Administrador de cuentas inactivas desarrollada por Google permite a los usuarios programar una fecha para ejecutar el conjunto de acciones configuradas para salvaguardar el contenido de la cuenta (emails, documentos archivados, fotos, datos económicos etc.). Una vez terminado el plazo y ejecutadas las acciones configuradas, la cuenta será eliminada automáticamente.

Otras redes tratan el problema de otra manera. Es el caso de Facebook que brinda la opción de mantener la cuenta del usuario fallecido como una piedra funeral, para conmemorar el difunto. En este caso, la familia del fallecido es la que opta para esta forma de conmemoración y para activar la opción debe enviar por e-mail el certificado de defunción. La aplicación Twitter no permite mantener una cuenta conmemorativa. A

cambio permite a los sucesores mandar “tuits” desde la cuenta del fallecido si desean hacer pública la muerte del usuario. Para eliminar la cuenta es necesaria una notificación de la familia que debe mandar los documentos relacionados con la muerte del usuario y una copia de los “tuits” del de cuius será enviada a los familiares.

Cuando se trata datos físicos, el legado digital es comparativamente simple, ya que estos simplemente se transfieren a los herederos como posesiones. En la mayoría de los casos, los discos duros, los dispositivos y las memorias USB no están protegidos por contraseñas o, si lo están, los familiares suelen conocer las contraseñas. Sin embargo, los datos de inicio de sesión y las contraseñas también deben regularse para que los familiares puedan acceder a los datos que contienen. Pueden ser archivos privados como fotos y videos, así como documentos importantes.

El legado digital se vuelve más complicado si la persona fallecida ha estado haciendo negocios en Internet. Si, por ejemplo, tenían un canal de YouTube que continuará generando ingresos publicitarios de manera regular, será necesario administrar el flujo de dinero. Lo mismo se aplica a los perfiles populares de Instagram que contienen publicaciones patrocinadas y a través de los cuales se finalizaron los contratos publicitarios. En resumen, el legado digital es de enorme importancia para las personas influyentes, los productores de contenido y otras personas que ganan dinero en línea.

La moneda digital también debe gestionarse. No existe una política internacional relativa a los activos digitales, como la moneda criptográfica (por ejemplo, Bitcoin) y el crédito de PayPal después de la muerte. Por estas razones el usuario tiene que asegurase que sus herederos podrán acceder estos recursos digitales después de su muerte.

Otro tema complicado son los contratos en línea para los servicios SaaS, los pedidos realizados en línea que aún no se han recibido y las suscripciones en línea para contenido digital (por ejemplo, servicios de transmisión o bibliotecas de libros electrónicos). El sector del juego también se ve afectado, ya que el contenido aquí (por ejemplo, artículos en juegos en línea) puede valer dinero real. En conclusión, el derecho a un testamento digital del usuario impone a los estados de adaptar le legislación sobre las herencias a este nuevo mundo virtual que pueda contener valores digitales importantes para la familia del defunto.

CAPITULO VI. Mecanismos para garantizar los derechos fundamentales

"Uno de los desafíos más importantes de la época en que vivimos consiste en establecer una ecuación exacta, correspondiente a los apremios del tiempo, en las relaciones entre los avances tecnológicos y la tutela de las libertades. El ámbito del mundo, cada vez más planetario, ha apretado decisivamente sus exigencias y reclama un adecuado planteamiento de las garantías de los derechos cívicos ante el desarrollo de las Nuevas Tecnologías"[501].

Empleando las palabras de René Cassin, los derechos humanos se definen "*como una rama particular de las ciencias sociales que tiene como objetivo estudiar las relaciones entre los hombres, desde la perspectiva de la dignidad humana, mediante la determinación del conjunto de los derechos y facultades necesarios para el desarrollo de la personalidad de cada ser humano*".[502].

Es necesario considerar también que para Yves Madiot, "El objeto de los derechos humanos es el estudio de los derechos humanos reconocidos a nivel nacional e internacional y que, en cierto estado de civilización, garantizan la reconciliación entre, por un lado, la afirmación de la dignidad de la persona y su protección y, por otro lado, el mantenimiento del orden público"[503].

Por lo tanto, vemos que los derechos humanos de hoy constituyen una gran preocupación para las comunidades y los científicos internacionales y nacionales. En particular, la cuestión de la protección de los derechos humanos está demostrando ser importante ante sus violaciones masivas y reiteradas. En esta dinámica, el examen de los mecanismos internacionales para la protección de los derechos humanos es de fundamental importancia. De hecho, es a través de estos mecanismos que el derecho

[501] Pérez Luño, A. E. (2011) *Internet y los derechos humanos*, Anuario de Derechos Humanos. Nueva Época. Vol. 12. 2011 (287-330), recuperado de: http://dx.doi.org/10.5209/rev_ANDH.2011.v12.38107.
[502] Cassin, R. (1951) *La déclaration universelle et la mise en œuvre des droits de l'homme*, Paris, Librairie du Recueil Sirey, p. 245.
[503] Becet, J. M. y Colar, D. (1982), Les droits de l'hommes, dimensions nationales et internationales, Paris, Economica, pp. 9-10

internacional de los derechos humanos proporciona una protección más o menos activa e intenta superar el abismo que a menudo existe entre los preceptos y la práctica.

El simple reconocimiento formal de algunos derechos fundamentales en los textos básicos de los Estados o en los instrumentos jurídicos elaborados por las organizaciones internacionales no es suficiente para garantizar el logro de los objetivos perseguidos por su regulación jurídica en la ausencia de garantías adecuadas, con el papel de concretar el contenido de los derechos.

El papel preventivo de los mecanismos de protección de los derechos humanos es esencial, en el sentido de que tienden a proteger a la persona humana, porque como afirma Frédéric Sudre: "*la justiciabilidad de la norma condiciona la efectividad de la garantía y su sanción. No se puede implementar seriamente la protección internacional de los derechos humanos si no se acompaña de mecanismos jurisdiccionales apropiados*".[504]

Además, las regulaciones internacionales imponen la obligación de los estados de tomar medidas efectivas para respetar los derechos. Así, el art. 2 párrafo (3) del Pacto Internacional de Derechos Civiles y Políticos establece que los Estados Contratantes deben:

> *"a. garantizar que cualquier persona cuyos derechos o libertades reconocidos en este Pacto hayan sido violados tendrá un recurso efectivo, incluso cuando la infracción haya sido cometida por personas que actúan en el ejercicio de sus funciones oficiales;*
>
> *b. garantizar que la autoridad competente, judicial, administrativa o legislativa o cualquier otra autoridad competente de acuerdo con la ley del estado, decida sobre los derechos de la persona que utiliza la ruta de apelación y desarrolle las posibilidades de apelación judicial;*
>
> *c. garantizar que las autoridades competentes procederán a cualquier recurso que haya sido reconocido como justificado".*

Según el conocido *dictum* consagrado por el T.E.D.H., los derechos fundamentales no deben ser teóricos e ilusorios, sino concretos y efectivos. Desde este punto de vista, es necesario establecer algunas garantías legales destinadas para defender la esencia de este derecho y proteger a sus beneficiarios, un requisito que forma parte de

[504] Sudre, F. (1989) *Droit international et européen des droits de l'homme*, 3e Edition, Paris, PUF, p. 13.

las obligaciones positivas del estado[505]. La doctrina del derecho constitucional[506] ha identificado dos tipos de garantías para el ejercicio de los derechos fundamentales: algunos externos y otros internos a la Constitución. La efectividad de las garantías se puede lograr a través de mecanismos estatales o supraestatales que a su vez se pueden clasificar en varias categorías: constitucionales (o convencionales), legales, institucionales (administrativas) y jurisdiccionales[507].

A nivel supraestatal, los medios de protección son comunes a todos los estados que se han adherido al respectivo orden legal, por ejemplo, a este respecto, los órganos de la Convención para los estados que se adhirieron a ésta, o los mecanismos utilizados por las instituciones y organismos de la U.E. (El Parlamento Europeo, El Defensor del Pueblo, La Autoridad de Protección de Datos Personales) por el respeto de los derechos fundamentales, ya que se derivan de las tradiciones constitucionales de los Estados miembros y / o de la Carta de los Derechos Fundamentales de la Unión Europea.

A nivel estatal encontramos dos categorías de mecanismos, constitucionales y legales. En adelante vamos a analizar los diferentes mecanismos de garantías previstos por los tratados internacionales, regionales o por las constituciones y leyes de los estados.

6.1. Mecanismos supraestatales universales

Además de proteger la paz universal, no hay causa con la que las Naciones Unidas se identifiquen más que la de los derechos humanos. "*Si los últimos sesenta años se han centrado en el desarrollo de un conjunto de normas destinadas a proteger los derechos humanos que ha producido un marco normativo notable de leyes, normas y mecanismos, empezando por la Declaración Universal de los Derechos Humanos, es la hora de entrar en una nueva era, orientada hacia la implementación efectiva"*[508]; dijo Kofi Annan el 7 de abril de 2005 en la 61ª Sesión de la Comisión de Derechos Humanos en Ginebra.

La preocupación por la dignidad humana está consagrada en la Carta de las Naciones Unidas e incorporada a las estructuras mismas de la Organización. Por lo tanto, la formación de un derecho internacional de los derechos humanos y, sobre todo, la

[505] Idem.
[506] Muraru, I. y Tanasescu, E.S. (2001) *Drept Constitutional si institutii politice (Derecho Constitucional e Instituciones Políticas)*, Volumen I, Edición 14, Editorial C.H. Beck, Bucarest
[507] Idem.
[508] Naciones Unidas, Kofi ANNAN pide una reforma en profundidad del servicio de información de la Comisión de Derechos Humanos, Nueva York, 07 de abril de 2005;

cristalización de su protección será el trabajo de las Naciones Unidas y ciertos organismos especializados, en particular la Organización Internacional del Trabajo y la UNESCO. De hecho, desde el preámbulo de la Carta, las Naciones Unidas declararon su determinación de "*proclamar una vez más su fe en los derechos humanos fundamentales, en la dignidad y el valor de la persona humana, en la igualdad de derechos de los hombres y mujeres*". El artículo 1 establece expresamente que uno de los objetivos de la Organización es lograr la cooperación internacional resolviendo problemas económicos, sociales, intelectuales o humanitarios internacionales, desarrollando o alentando el respeto de los derechos humanos. Derechos humanos y libertades fundamentales para todos, sin discriminación de raza, sexo, idioma o religión. El párrafo (c) del artículo 55 adopta una formulación idéntica[509], lo que lleva a una continuación lógica con el artículo 56 que establece que "*los miembros se comprometen, con el fin de lograr los objetivos establecidos en el artículo 55, actuar, conjuntamente y por separado, en cooperación con la Organización*".

Por lo tanto, esta afirmación de las Naciones Unidas sobre la fe en los derechos fundamentales ha llevado al establecimiento de mecanismos para monitorear y garantizar los derechos humanos, los llamados mecanismos universales. Para comprender mejor estos mecanismos, vamos a analizar su implementación dentro de las Naciones Unidas y a examinar la efectividad de esta implementación.

El análisis de la implementación del control y la garantía de los derechos humanos dentro de las Naciones Unidas debe empezar con la identificación de los organismos competentes de la ONU responsables del asunto. De hecho, como casi todos los problemas humanitarios tienen un aspecto que concierne a los derechos humanos, todos los órganos principales de las Naciones Unidas (a saber, la Asamblea General, el Consejo de Seguridad, el Consejo Económico y Social, el Consejo de Administración Fiduciaria, la Corte Internacional de Justicia, y la Secretaría) abordan de alguna manera el tema de los derechos humanos.

Sin embargo, la Asamblea General es el principal órgano responsable de las cuestiones de derechos humanos. Por el artículo 13 de la Carta de las Naciones Unidas, este órgano está invertido con el poder de realizar estudios y hacer recomendaciones para desarrollar la cooperación internacional en los ámbitos económico, social y cultural, y en

[509] Oumba, F. P. (2004) *La Cour internationale de justice et la problématique des droits de l'homme*. Mémoire de Master droits de l'homme et action humanitaire, UCAC (Cameroun), p. 4.

el de educación y salud pública, con el fin de facilitar el disfrute de los derechos humanos y las libertades fundamentales para todos, independientemente de su raza, sexo, idioma o religión.

Sobre esta base, la Asamblea General tiene poderes de decisión y cumple una función de coordinación que facilitan la elaboración de los textos normativos y la firma de los textos por los Estados miembros. La mayor parte del trabajo de la Asamblea General se lleva a cabo en comisión, y la Tercera Comisión es responsable de los asuntos sociales, humanitarios y culturales, incluso tiene la responsabilidad de ocuparse de los asuntos de derechos humanos. Sin embargo, dado el alcance de las actividades de la Asamblea General, el Artículo 62 de la Carta delegó naturalmente al Consejo Económico y Social el poder de hacer recomendaciones para garantizar el respeto de los derechos humanos y las libertades fundamentales para todos. También puede preparar proyectos de convenios para su presentación a la Asamblea General. Finalmente, según el Artículo 62 de la Carta, tiene la posibilidad de establecer comités en esta área. De esta manera fueron creadas la Comisión de Derechos Humanos y la Comisión de Derechos de la Mujer. Es importante señalar que la Comisión es un órgano político compuesto por representantes de los Estados que actúan bajo instrucciones nacionales. Actualmente tiene 53 estados miembros elegidos por tres años sobre la base de sutiles equilibrios regionales para dar una imagen real de la comunidad internacional.

6.1.a. Garantías de control institucional implementadas por los organismos de las Naciones Unidas.

Los mecanismos de protección contra violaciones de derechos humanos involucran a todos los organismos antes mencionados mediante los procedimientos de investigación y deliberación previstos en las resoluciones adoptadas por la Comisión de Derechos Humanos. A continuación, vamos a presentar los diferentes tipos de procedimientos: el procedimiento confidencial, el procedimiento público y otras prácticas.

• El procedimiento confidencial o el procedimiento 1503

La necesidad de establecer procedimientos apropiados para el examen de presuntos casos de violaciones de los derechos humanos se consideró desde la primera sesión de la Comisión de Derechos Humanos. Mediante la resolución 1503 (XLVIII) del 27 de mayo de 1970, relacionada con las resoluciones 728F, 1235 de 6 de junio de 1967

y 2000/3 de 16 de junio de 2000, el Consejo Económico y Social desarrolló un procedimiento integral para la examinación de todas las comunicaciones individuales, sin discriminación, que denuncian violaciones de derechos humanos, dirigidas a las Naciones Unidas.

El procedimiento 1503 se aplicará plenamente en las actividades del nuevo Consejo de Derechos Humanos que reemplazó a la Comisión de Derechos Humanos. En este contexto, se crearán dos grupos de trabajo separados con el mandato de examinar las comunicaciones y llamar la atención del Consejo de Derechos Humanos sobre toda una serie de violaciones graves y evidentes sobre los derechos humanos y las libertades fundamentales. Los dos grupos de trabajo actuarán, cuando es posible, por consenso. En ausencia de un consenso, las decisiones se tomarán por mayoría simple de votos. Pueden establecer sus propias reglas de procedimiento.

El Comité consultativo del Consejo de Derechos Humanos designará a cinco de sus miembros entre los representantes de cada uno de los grupos regionales, teniendo en cuenta los principios del equilibrio de género, para constituir el Grupo de Trabajo de Comunicaciones. En caso de un puesto vacante, el Comité Consultativo designará un experto independiente y altamente calificado elegido entre los miembros del mismo grupo regional. Como existe la necesidad de experiencia independiente y continuidad en la revisión y evaluación de las comunicaciones, los expertos independientes y altamente calificados que formarán parte del Grupo de Trabajo de Comunicaciones tendrán un mandato de tres años renovable solo una vez.

El presidente del Grupo de Trabajo sobre Comunicaciones deberá realizar, en colaboración con la secretaría, una clasificación inicial de comunicaciones, basada en los criterios de admisibilidad, antes de transmitirlas a los Estados interesados. Las que sean manifiestamente sin fundamento o anónimas serán rechazadas por el presidente y, por lo cual, no serán transmitidas al estado en cuestión. En aras de la rendición de cuentas y transparencia, el presidente del Grupo de Trabajo de Comunicaciones proporcionará a todos los miembros del Grupo de Trabajo una lista de todas las comunicaciones rechazadas después de la revisión inicial. Esta lista debe indicar los motivos de todas las decisiones de rechazo. Todas las demás comunicaciones, que no han sido rechazadas, se transmitirán a los Estados parte implicados para que realicen sus comentarios sobre las presuntas violaciones. Los miembros del Grupo de Trabajo de Comunicaciones decidirán

sobre la admisibilidad de una comunicación, examinarán el fundamento de las alegaciones de violación, incluida la cuestión de si la comunicación, considerada por separado o en conjunto con otras comunicaciones, parece revelar una violación flagrante de los derechos humanos y las libertades fundamentales, evidenciada por elementos creíbles.

El Grupo de Trabajo de Comunicaciones proporcionará al Grupo de Trabajo de Situaciones un archivo que contiene todas las comunicaciones admisibles y las recomendaciones a las que se han dirigido. Si el Grupo de trabajo requiere un examen más detallado o más información, puede mantener el asunto bajo revisión hasta su próxima sesión y solicitar la información del Estado en cuestión. Puede decidir cerrar un caso. Todas las decisiones del Grupo de Trabajo de Comunicaciones se basarán en una aplicación rigurosa de los criterios de admisibilidad y estarán debidamente justificadas.

Los grupos regionales, teniendo debidamente en cuenta los principios de equilibrio de género, designarán cada uno un representante de un Estado miembro del Consejo para el Grupo de trabajo sobre situaciones.

El mandato de los miembros del Grupo de Trabajo será de un año, renovable una vez, si el Estado en cuestión sigue siendo miembro del Consejo. Los miembros del Grupo de Trabajo sobre Situaciones actúan individualmente. En caso de un puesto vacante, el grupo regional al que pertenece el puesto vacante designará un representante de uno de los estados miembros del mismo grupo regional. El Grupo de Trabajo sobre Situaciones presenta al Consejo de Derechos Humanos un informe, sobre la base de la información y las recomendaciones que emanan del Grupo de Trabajo sobre Comunicaciones. El informe debe presentar cualquier violación grave cierta de los derechos humanos y las libertades fundamentales y contiene recomendaciones al Consejo sobre las medidas que deben adoptarse, normalmente en forma de un proyecto de resolución o decisión sobre las situaciones que se le presenten.

Si el Grupo de Trabajo sobre Situaciones requiere un análisis más profundo o más información, sus miembros pueden mantener el asunto bajo revisión hasta la próxima sesión del Grupo. El Grupo de Trabajo de Situaciones también puede decidir cerrar un caso. Todas las decisiones del Grupo de Trabajo de Situaciones estarán debidamente fundamentadas e indicarán la razón por la cual se detuvo la consideración de una situación o la acción recomendada en relación con esta situación. La decisión de terminar el examen

de una situación debe tomarse por consenso o, si esto no es posible, por mayoría simple de votos.

Como el procedimiento de solicitud debe tratarse, entre otras cosas, de manera favorable para las víctimas y realizarse de manera confidencial y oportuna, los dos grupos de trabajo celebrarán al menos dos sesiones por año, de cinco días hábiles cada una, por lo que examinar con prontitud las comunicaciones, incluidas las respuestas a ellas, así como las situaciones que el Consejo ya ha recibido en relación con el procedimiento de solicitud.

El Estado interesado cooperará con el proceso de solicitud y no escatimará esfuerzos para proporcionar respuestas sustantivas, en uno de los idiomas oficiales de las Naciones Unidas, a cualquier solicitud del Grupo de Trabajo o del Consejo de Derechos Humanos. Tampoco escatimará esfuerzos para responder dentro de los tres meses posteriores a la solicitud. Sin embargo, si es necesario, este período puede ampliarse a solicitud del Estado interesado. La secretaría debe comunicar los archivos confidenciales a todos los miembros del Consejo, al menos con dos semanas de anticipación, para que tengan tiempo de revisarlos.

Periódicamente, al menos una vez al año, el Consejo de Derechos Humanos tiene la obligación de revisar todas las violaciones graves de los derechos humanos identificadas y presentadas por el Grupo de Trabajo sobre Situaciones. Los informes del Grupo de Trabajo sobre Situaciones remitidos al Consejo de Derechos Humanos serán tratados de manera confidencial, si no hay una decisión del Consejo que ha establecido lo contrario. Por ejemplo, en caso de falta de cooperación, el Grupo de Trabajo sobre Situaciones puede recomendar al Consejo que examine la situación en público, y el Consejo examinará esta recomendación como una prioridad en su próxima sesión.

Para que el procedimiento de solicitud se aborda de manera amigable, eficiente y oportuna para las víctimas, el período de tiempo entre la transmisión de la solicitud y su consideración por el Consejo de Derechos en principio no debe exceder los veinticuatro meses. Como parte del procedimiento de solicitud, se garantizará que el autor de la solicitud y el Estado en cuestión estén informados sobre el estado del procedimiento en las siguientes etapas clave:

1. Cuando la solicitud sea declarada inadmisible por el Grupo de Trabajo sobre Comunicaciones, cuando sea tratada por el Grupo de Trabajo sobre Situaciones o cuando la comunicación sea suspendida por uno de los grupos de trabajo o por el Consejo;

2. Adopción de las conclusiones. Además, la secretaría informará al solicitante de la grabación de su comunicación sobre el procedimiento de solicitud. Si un solicitante requiere que su identidad se mantenga confidencial, no se divulgará al Estado en cuestión.

De acuerdo con la práctica establecida, la decisión tomada sobre una situación particular será una de las siguientes:

i. Finalizar el análisis de la situación cuando la continuación de su examinación o la adopción de otra medida no esté justificada;
ii. Continuar el procedimiento de examinación de la situación y solicitar al Estado en cuestión que ofrezca más información dentro de un tiempo razonable;
iii. Nombrar a un experto independiente y altamente calificado para continuar monitorear el caso e informar inmediatamente al Consejo;
iv. Concluir la consideración del asunto bajo el procedimiento de petición confidencial para consideración pública;
v. Recomiende que la Oficina del Alto Comisionado brinde cooperación técnica, asistencia para el desarrollo de capacidades o servicios de asesoramiento al Estado interesado.

• El procedimiento público: Resolución 1235

Creado por la resolución 1235 (XLII) del ECOSOC del 6 de junio de 1967, el procedimiento público permite a la Comisión y a su Subcomisión de invertirse con la capacidad para examinar situaciones que revelan violaciones flagrantes y sistemáticas de los derechos humanos.

La decisión se adoptó como consecuencia de la política de apartheid practicada en Sudáfrica y en Rhodesia del Sur (Zimbabue). Se dice que es público porque da lugar a la publicación de un informe. A través de esta resolución, la Comisión y la Subcomisión pueden, en ciertos casos, tomar medidas sobre las denuncias de derechos humanos. La Comisión puede, si es necesario, y después de haber examinado cuidadosamente la información recibida, realizar un estudio en profundidad de las situaciones que revelan

violaciones constantes y sistemáticas de los derechos humanos y presentar al Consejo un informe y recomendaciones al respecto[510].

El propósito de este procedimiento es ejercer presión diplomática sobre el estado en cuestión. De hecho, existen situaciones cuando el país responsable de la violación de los derechos humanos pone fin a sus actos culpable solo porque otros Estados y las ONG han sido informados sobre la situación creada. Por lo tanto, la Comisión ha iniciado un estudio de las modalidades que permiten la recepción de numerosas comunicaciones de particulares u organizaciones no gubernamentales. Puede ser iniciado por un Estado, por un grupo de Estados o por iniciativa de la Subcomisión y cada año da lugar a un intenso lobbying por parte de las ONG y los Estados interesados.

Algunos están trabajando para garantizar que el procedimiento conduzca a una resolución de la Comisión que pronuncie una condena pública del estado en cuestión, este último y sus aliados buscando el resultado contrario[511].

El procedimiento público permite a la Comisión examinar sin restricción cualquier situación que revele violaciones de los derechos humanos en ciertos países en sesiones públicas. La primera situación examinada fue la que reinó en Chile desde el derrocamiento por violencia, en 1973, del gobierno constitucional del presidente Salvador Allende. Posteriormente, la Comisión generalizó sobre la base del ejemplo chileno, el establecimiento de procedimientos relativos a ciertas situaciones.

Numerosos "relatores especiales, grupos de trabajo"[512] y "representantes del Secretario General"[513] serán nombrados gradualmente y desplegarán actividades enérgicas con el objetivo de eliminar las violaciones más obvias de los derechos humanos. Escriben informes utilizando todos los medios a su disposición[514].

---

[510] Melkevik, B. (1997) *ISSE OMANGA BOKATOLA, L'Organisation des Nations Unies et la protection des minorités*. Les Cahiers de droit, 38 (1), 238–239., Editorial Bruylant, Bruxelles.
[511] Ergec, R. (2014) Protection européenne et internationale des droits de l'homme, Tercera Edicion, Editorial Larcier.
[512] Los relatores especiales son expertos independientes con mandatos especiales para investigar los derechos humanos. Cuando se da un mandato a varios expertos, hablamos de un grupo de trabajo.
[513] La comisión puede pedirle al Secretario General que intervenga o envíe un experto para examinar o prevenir una situación de violación de los derechos humanos en el marco de sus buenos oficios y una diplomacia discreta de forma confidencial con los Estados miembros.
[514] Nations Unies, Les Nations Unies et les Droits de l'Homme : 1945-1995, New York, Département de l'information, 1995, p. 70.

Entre los grupos de trabajo establecidos en el marco del "Procedimiento 1235", el profesor Rusen Ergec menciona lo que se creó para Sudáfrica y el Comité Especial, aún activo, para la investigación de las prácticas israelíes que afectan los derechos humanos del pueblo palestino y otros territorios ocupado.

Otro caso importante es el nombramiento del Profesor Ermacora como Relator Especial luego de la invasión de Afganistán por la Unión Soviética, que llevó a cabo una investigación en profundidad en los países vecinos y denunció numerosas violaciones de derechos humanos en su informe.

Otros ejemplos de relatores especiales designados por la Comisión de Derechos Humanos son los de los siguientes países: Burundi, Cuba, Guinea Ecuatorial, Iraq, Myanmar, República Democrática del Congo, Ruanda, Palestina ocupada, Sudán, Bosnia Herzegovina, República de Croacia, República Federal de Yugoslavia. En cuanto a los mandatos encomendados al Secretario General de las Naciones Unidas, cabe mencionar la situación de los derechos humanos en Chipre, Estonia y Letonia (las minorías lingüísticas), Kosovo y el Timor Oriental.

Como a los estados no les gusta ser estigmatizados públicamente como autores de violaciones graves y sistemáticas de los derechos humanos16, la acción de la Comisión de Derechos Humanos bajo el "procedimiento 1235" es beneficiosa porque generalmente conduce a una condena pública, que tiene un alto significado moral[515]. Luego resultó ser muy difícil lograr la implementación de este procedimiento descrito por la mayoría de los Estados como más restrictivo e inconveniente. Por lo tanto, habiendo notado esta dificultad, la Subcomisión preparó un proyecto de resolución sobre las normas relativas al examen de las Comunicaciones recibidas por el Secretario General en virtud de la "Resolución 728 F"[516]. Este es el procedimiento confidencial consagrado en la resolución 1503 (XLVII), cuyo análisis se realiza en las siguientes líneas.

[515] Oumba. P. (2009) La Cour internationale de justice et la problématique des droits de l'homme. Humanité et liberté en Afrique centrale, 2009, Tome 1, pp.147-162.
[516] La Resolución General del ECOSOC 728 (XXVIII) del 30 de julio de 1959 invita al Secretario General a elaborar una lista de Comunicaciones de individuos u ONG que se quejan de violaciones de los derechos humanos. Mantiene el anonimato de su autor, informa al Estado interesado de estas comunicaciones y las somete a un comité especial de la Comisión de Derechos Humanos.

• Otras prácticas

Junto con el procedimiento 1503 y el procedimiento público, la Comisión ha desarrollado progresivamente una práctica que consiste en tratar ocasionalmente ciertas "situaciones".

Se han adoptado varias resoluciones específicas pidiendo al presidente que designe un relator especial, o un representante especial, para estudiarlas en profundidad. Los relatores especiales consideran las comunicaciones de individuos u organizaciones no gubernamentales, y si los gobiernos de los estados involucrados están de acuerdo, viajan al lugar para examinar la supuesta situación y reunirse con las diversas partes involucradas. Además, varias violaciones de los derechos humanos han recibido atención especial debido a su relevancia, impacto y la necesidad de conocer sus manifestaciones donde sea que ocurran, así como las razones que les dieron origen. Por esta razón se han designado los llamados relatores especiales temáticos para examinar, por ejemplo, el problema de las ejecuciones arbitrarias, la tortura, los mercenarios y la intolerancia religiosa.

Otra violación particularmente grave de los derechos humanos, el aumento de las desapariciones inexplicables de personas, a menudo como resultado de excesos cometidos por la policía o por organizaciones paramilitares, ha adquirido una dimensión internacional en los últimos años.

6.1.b. Mecanismos de control legal por el sistema de pactos y convenios.

La elaboración y adopción por las Naciones Unidas de instrumentos internacionales que definan con precisión los derechos reconocidos a las personas y que además prevea procesos de monitoreo constituye, cronológicamente, la segunda etapa en la consolidación de la protección internacional de los derechos humanos.

En el marco de los Pactos, tenemos el Pacto Internacional de Derechos Económicos, Sociales y Culturales[517] y el Pacto Internacional de Derechos Civiles y

[517] Pacto Internacional de Derechos Económicos, Sociales y Culturales, adoptado y abierto a la firma, ratificación y adhesión de la Asamblea General de las Naciones Unidas en su resolución 2200 A (XXI) del 16 de diciembre de 1966. Este Pacto es entró en vigor el 3 de enero de 1976, de conformidad con lo dispuesto en el artículo 27.

Políticos[518]. Mientras que el segundo establece un Comité de Derechos Humanos[519], el primero no menciona ningún órgano similar, siendo el Consejo Económico y Social el responsable de garantizar su implementación. Mediante la resolución 1985/17, de 28 de mayo de 1985, el Consejo creará el Comité de Derechos Económicos, Sociales y Culturales, responsable de supervisar su aplicación.

Como órgano de "asesoramiento y supervisión", la función principal del Comité de Derechos Humanos es examinar los informes presentados por los Estados Parte "sobre las medidas que han adoptado y que dan efecto a los derechos reconocidos en el [...] Pacto y en los progresos realizados en el disfrute de estos derechos". El texto agrega que "los informes deben indicar, cuando corresponda, los factores y dificultades que afectan la implementación de las disposiciones de este Pacto".

Para Marie-Odile Maurize, "*una de las primeras tareas del Comité fue establecer reglas para la presentación y el estudio de estos informes. El procedimiento de examen que tiene lugar en una sesión pública toma la forma de un diálogo entre los miembros del Comité y los de la delegación del Estado en cuestión: el Comité envía una lista de puntos al gobierno, los representantes de este último responden. durante la sesión*".[520]

Algunos de los derechos fundamentales garantizados por los Pactos también son objeto de otros instrumentos funcionales o especializados, ya que ha surgido la necesidad de proteger en particular ciertas categorías de derechos o personas. Por lo tanto, en el marco de los Convenios, conservaremos aquí el Convenio internacional para la represión y el castigo del crimen de apartheid, que entró en vigor el 13 de julio de 1976, y cuya aplicación está garantizada, en virtud de Artículo IX de esta Convención, por tres miembros de la Comisión de Derechos Humanos que son al mismo tiempo representantes de los Estados parte en la Convención.

---

[518] Pacto Internacional de Derechos Civiles y Políticos, adoptado y abierto a la firma, ratificación y adhesión de la Asamblea General de las Naciones Unidas en su resolución 2200 A (XXI) del 16 de diciembre de 1966. Este Pacto entró en vigencia en vigor desde el 23 de marzo de 1976, de conformidad con lo dispuesto en el artículo 49

[519] El Comité de Derechos Humanos es el órgano de la Naciones Unidas formado por expertos independientes que supervisa la aplicación del Pacto Internacional de Derechos Civiles y Políticos por sus Estados parte. El comité examina cada informe presentado anual por los Estados y expresa sus preocupaciones y recomendaciones al Estado Parte en forma de "observaciones finales". más información sobre la actividad del Comité en: https://www.ohchr.org/sp/hrbodies/ccpr/pages/ccprindex.aspx.

[520] Maurize, M.-O. (1992) *Au delà de l'Etat. Le droit international et la défense des droits de l'homme*, Paris, Amnesty International, 1992, p. 86.

A esta Convención, agregaremos la Convención contra la Tortura y Otros Tratos o Penas Crueles, Inhumanos o Degradantes, que entró en vigor el 26 de junio de 1987, que dio origen al Comité contra la Tortura; la Convención internacional contra el apartheid en el deporte, que entró en vigor el 3 de abril de 1988 y que establece el establecimiento de una Comisión contra el apartheid en el deporte; y finalmente el Segundo Protocolo Facultativo relativo al Pacto Internacional de Derechos Civiles y Políticos, adoptado por la Asamblea General el 15 de diciembre de 1989, que busca la abolición de la pena de muerte y cuyo control debe garantizar el Comité de derechos del hombre.

En virtud de los instrumentos que rigen los derechos de las diversas categorías de personas, debe tenerse en cuenta lo siguiente: la Convención internacional sobre la eliminación de todas las formas de discriminación racial, que entró en vigor el 4 de enero de 1969; la Convención sobre la eliminación de todas las formas de discriminación contra la mujer, que entró en vigor el 3 de septiembre de 1981; la Convención sobre los Derechos del Niño del 20 de noviembre de 1989 y finalmente la Convención internacional sobre la protección de los derechos de todos los trabajadores migratorios y sus familias. Los órganos encargados de supervisar la aplicación de estos convenios están integrados, según sea el caso, por 10, 18 o 23 expertos, nacionales de los Estados parte, que deben ser personalidades de alto carácter moral con reconocida competencia en el campo de los derechos humanos. hombre. La característica fundamental de estos expertos es la independencia, ya que son elegidos por votación secreta y sirven a título individual.

El elemento clave del mecanismo de monitoreo es la consideración de los informes presentados por los Estados parte. El alcance de este control depende en última instancia de la efectividad real del sistema. Los Estados parte se comprometen a presentar informes sobre las medidas que han adoptado que dan efecto a los derechos reconocidos en el instrumento en cuestión y sobre los progresos realizados en el disfrute de estos derechos. Los informes deben indicar, cuando corresponda, los factores y dificultades que afectan la implementación de los arreglos planificados. El control realizado sobre la base de informes estatales solo es de interés si se renueva periódicamente. De hecho, el examen del informe inicial presentado por el Estado resulta ser en muchos casos un contacto entre el Comité pertinente y el Estado Parte.

Este primer examen ayuda a desarrollar al nivel general y legal, una imagen única y global sobre la situación de los derechos humanos en un país determinado. Es solo con la consideración de informes periódicos donde se destaca mejor la situación concreta de los derechos humanos que el ejercicio adquiere su pleno significado.

La periodicidad permite comparar y medir la evolución de la situación: lleva al Comité a consultar sus observaciones y preguntas anteriores para considerar cómo las autoridades nacionales las han tenido en cuenta.

Concretamente, la periodicidad aplicada es de cuatro o cinco años según el caso. La revisión en sí se lleva a cabo en sesiones abiertas y toma la forma de un diálogo entre los miembros del Comité y la delegación nacional, ya que el Comité no es un tribunal internacional y los procedimientos no son inquisitorios. El examen de los informes se resume en el informe anual del Comité que se transmite cada año a la Asamblea General o al Consejo Económico y Social.

Algunos comités han desarrollado una práctica de adoptar observaciones generales para permitir que todos los Estados Parte se beneficien de su experiencia, llamar su atención sobre las deficiencias reveladas por una gran cantidad de informes, sugerir ciertas mejoras en sus presentaciones y estimular las actividades de los Estados y las organizaciones internacionales que tienen como objetivo proteger los derechos humanos.

Para mejor garantizar el cumplimiento de los propósitos del Pacto de Derechos Civiles y Políticos, la Convención sobre la Eliminación de la Discriminación Racial y la Convención contra la Tortura, y sus disposiciones, los comités pertinentes han sido facultados para recibir y considerar las comunicaciones de personas que afirman ser víctimas de una violación de uno de los derechos establecidos. Aunque, este procedimiento es opcional y solo vincula a algunos de los Estados parte. No es necesario reiterar la importancia de la posibilidad de que un individuo pueda, después de agotar los recursos internos y bajo ciertas condiciones, referirse a un organismo internacional. El Comité de Derechos Humanos, por ejemplo, ha desarrollado una jurisprudencia particularmente elaborada al emitir más de un centenar de conclusiones sobre el fondo. Estos han tenido un cierto eco dentro de los Estados parte. Los organismos competentes también pueden, bajo ciertas condiciones, considerar comunicaciones en las que un Estado Parte alega que otro Estado Parte no está cumpliendo con sus obligaciones bajo el

instrumento correspondiente. Sin embargo, desde su inicio, ninguno de los cuerpos ha tenido que lidiar con tales comunicaciones.

6.1.c. Los efectos determinados por la activación de los mecanismos de supervisión de los derechos humanos por la ONU

La mayoría de los muchos organismos de derechos humanos de las Naciones Unidas supervisan constantemente la aplicación de las normas internacionales de derechos humanos como parte de un sistema general de revisión periódica de la información recibida de todas las fuentes confiables, incluidos los informes de los Estados Miembros, las organizaciones intergubernamentales y no gubernamentales y las comunicaciones relacionadas con presuntas violaciones de derechos humanos recibidas de o en nombre de las víctimas de tales violaciones. Además, ahora hay una serie de organismos especializados, establecidos de conformidad con las convenciones internacionales que se ocupan de ciertos aspectos de los derechos humanos, que dedican todo su tiempo y atención a supervisar la aplicación de las disposiciones de estos instrumentos.

Los sistemas de control general y el control especializado están estrechamente relacionados, funcionan armoniosamente sin dificultad y son complementarios. Trabajan juntos para garantizar que todas las personas, sin distinción, puedan disfrutar plenamente de sus derechos humanos y libertades fundamentales. Pero no importa, el sistema internacional para la protección de los derechos humanos es en gran medida incapaz de reaccionar rápida y efectivamente ante situaciones críticas como las violaciones graves y sistemáticas de los derechos humanos fundamentales (como la tortura a gran escala, desapariciones, procedimientos sumarísimos y detenciones arbitrarias).

Ante tales situaciones, es urgentemente necesario proporcionar respuestas concretas que reflejen la preocupación de actuar y no se limiten a declaraciones. Los procedimientos requeridos para tratar situaciones críticas no son exactamente los mismos que en el examen de casos individuales, ya sea que se analicen los desafíos políticos que plantean o desde el punto de vista de los métodos requeridos. Muy a menudo, las situaciones críticas de derechos humanos son inseparables de los conflictos armados, internos o internacionales, en los que se aplica el derecho internacional humanitario[521].

[521] Oumba. P. (2008) *La prise en compte de la règle de droit humanitaire dans la jurisprudence de la Cour internationale de justice*. Revue Aspects, pp.69-83.

Por ejemplo, con respecto a los mecanismos no convencionales, uno debe analizar el procedimiento establecido por la Resolución 1503 del ECOSOC, que ha merecido una crítica reflexiva de los círculos de derechos humanos. Una de las formas de aumentar la efectividad de estos mecanismos es, sin duda, disminuir su confidencialidad. Las sanciones que probablemente se impongan en el marco de este procedimiento son esencialmente políticas. La principal de estas sanciones, que es la publicidad, podría modularse según el grado de colaboración y el progreso del estado investigado desde una perspectiva de derechos humanos.

Esta política sobre la publicidad de los procedimientos debe aplicarse más ampliamente a todas las preguntas en las que se ha acordado tratar la información recibida de esta manera: pongamos por caso, la lista de bancos, compañías multinacionales y otras organizaciones que apoyan o financian a los regímenes dictatoriales o incluso a los países que declararon un estado de emergencia para suspender el ejercicio de ciertos derechos, a saber, Birmania y Nepal. Si bien, debe reconocerse que, si la acción procesal de las Naciones Unidas en el campo de los derechos humanos es limitada, es sobre todo porque esta acción es precisamente posible solo dentro del marco de las Naciones Unidas.

Esta evidencia a menudo parece olvidarse siempre que nos centremos en los detalles del procedimiento. Sin embargo, "en el estado actual de las relaciones internacionales, los Estados soberanos siguen siendo los factores principales, ya sea que actúen dentro o fuera del sistema de las Naciones Unidas"[522]. En general se acepta que este estado de las cosas influye en la actividad normativa de las Naciones Unidas. Sería sorprendente si no lo encontramos en la etapa de implementación, multiplicado incluso por el concreto de las situaciones. Debe recordarse que los organismos que en última instancia tienen que ocuparse de las cuestiones de derechos humanos son los organismos políticos. Siendo así, si existe un límite inherente a la acción que se evalúa aquí, se encuentra en el nivel de toma de decisiones.

Por otro lado, en términos de la autoridad de las decisiones como declaraciones y recomendaciones, sabemos el peso de las resoluciones aprobadas con grandes mayorías de pequeños estados[523]. En cuanto a las decisiones vinculantes del Consejo de Seguridad,

[522] Véanse las siguientes resoluciones de la Comisión: resolución 20 (XXXVI) del 29 de febrero de 1980, resolución 1985/33 del 13 de marzo de 1985 y resolución 1982/26 del 11 de marzo de 1982

[523] Charpentier, J. (1997) *Le fondement du pouvoir des organisations internationales*", Revue Le Pouvoir, Paris, Ed. LGDJ, pp. 999-1011.

solo pueden tomarse en el marco de sus poderes regidos por el Capítulo VII de la Carta; Además, ninguno de estos cinco miembros permanentes se opone. Insistir en la importancia de la política en el trabajo de derechos humanos de las Naciones Unidas no significa necesariamente que "el derecho humano internacional es política; cualquier otra opinión es simplemente una locura"[524]. Y esta situación pasa debido a que la mayoría de los cuerpos son políticos.

Asimismo, aunque los Estados están obligados a ejecutar de buena fe y razonablemente las decisiones de los organismos internacionales de protección de los derechos humanos cuya competencia han reconocido oficialmente mediante la ratificación de tratados y de conformidad con el gran principio consuetudinario "*pacta sunt servanda*", las conclusiones de los organismos de protección y control de los derechos humanos no gozan de autoridad vinculante a nivel universal. Esto se justificaría por el hecho de que los mecanismos de protección universal no son jurisdiccionales con el pretexto de no socavar gravemente la soberanía de los Estados al establecer una especie de policía internacional. A nivel regional, por otro lado, especialmente en Europa, donde la garantía está dominada por un mecanismo judicial, las sentencias son vinculantes. La naturaleza jurisdiccional de este último mecanismo de protección tiene un impacto positivo en la justiciabilidad y la efectividad de los derechos humanos[525].

Como un importante cuerpo político en la nueva configuración de la protección internacional de los derechos humanos, el Consejo de Derechos Humanos tiene la intención de simplificar su trabajo al introducir más flexibilidad y fluidez y al hacer la lectura de sus deliberaciones más fácil. Se fortalecerán las actividades de promoción de los derechos humanos y las realizadas en el marco del programa de servicios de asesoramiento. Para hacer esto, la tarea esencial del Consejo de Derechos Humanos es sensibilizar a los Estados, las autoridades gubernamentales, las víctimas y, por supuesto, la opinión pública internacional en la aplicación de las normas internacionales.

Su creación, decidida por la Asamblea General de las Naciones Unidas en su resolución A/RES/60/251 del 15 de marzo de 2006, es parte de la tendencia de reforma de las Naciones Unidas iniciada por el Secretario General durante los años 1997-2005.

---

[524] Hauser, R. (1970) *United Nations Law on Racial Discrimination*, American Journal of International Law, n° 64, p. 115.
[525] Kamwanga, K. D. (2005) *Les mécanismes internationaux de protection et l'effectivité des droits de l'homme*, Mémoire de DEA, Université D'ABOMEY-CALAVI (Bénin).

El Consejo asumió las responsabilidades mantenidas desde 1947 por la Comisión de Derechos Humanos de las Naciones Unidas con cambios significativos en su método de elección y en su funcionamiento. El Consejo es un órgano subsidiario de la Asamblea General y, por eso, tiene un estatus institucional más alto que el de la Comisión, que era un órgano funcional del Consejo Económico y Social. La primera elección tuvo lugar el 9 de mayo de 2006 y la duración del mandato inicial de los miembros fue determinada por sorteo. La primera sesión ordinaria del Consejo se inauguró el 19 de junio de 2006. De conformidad con la resolución 60/251 de la Asamblea General del 15 de marzo de 2006, titulada "Consejo de Derechos Humanos", todos los mandatos, mecanismos y funciones. y los poderes de la Comisión de Derechos Humanos, incluida la Subcomisión de Promoción y Protección de los Derechos Humanos, se han transferido desde el 19 de junio de 2006 al Consejo de Derechos Humanos.

Por ende, debe conservar las características principales que han sido esenciales para los logros de la Comisión de Derechos Humanos, a saber:

- El poder de responder de manera efectiva y pública a las violaciones graves de los derechos humanos, al tiempo que conserva las funciones y responsabilidades adaptadas a sus propias necesidades atribuidas a la Comisión por las resoluciones 1235 y 1503 del Consejo Económico y Social;

- El sistema de expertos independientes especializados en temas o países, conocidos como "procedimientos especiales", pero con mayor coherencia y más apoyo;

- El estado consultivo de las ONG basado en el Artículo 71 de la Carta de las Naciones Unidas y las prácticas de participación de estas ONG con la Comisión. Diseñado para servir oficialmente durante todo el año de forma permanente, el Consejo de Derechos Humanos promoverá y protegerá todos los derechos humanos de cada individuo en el mundo. Para cumplir con este requisito, debe supervisar y promover la implementación de estándares y compromisos relacionados con dichos derechos e identificar las necesidades en términos de acciones de fortalecimiento en el campo de las libertades fundamentales.

De igual modo, este Consejo debe proporcionar una respuesta inicial a situaciones de crisis relacionadas con los derechos humanos, mostrar el camino a seguir y apoyar la integración efectiva de estos derechos en todo el sistema de las Naciones

Unidas como el principal cuerpo político de protección; su otra misión es liderar el desarrollo de nuevos estándares e instrumentos relacionados con estos derechos, así como responder de manera efectiva a las graves violaciones observadas. Sus funciones y atribuciones requieren que los Estados que desean ser miembros de esta, cumplan un cierto número de condiciones para garantizar el disfrute efectivo de los derechos individuales y así corregir las múltiples brechas e insuficiencias de la Comisión de los derechos humanos.

La función principal del Consejo de Derechos Humanos debería ser monitorear y ayudar a mejorar la implementación de los estándares y compromisos internacionales de derechos humanos en todos los países. Este proceso de evaluación objetiva debería servir como base para identificar los obstáculos para la realización de los derechos humanos y las necesidades de desarrollo de capacidades en cada país. El Consejo de Derechos Humanos debería en todo momento poder llamar la atención sobre un deterioro repentino y significativo de la situación de los derechos humanos en un país en particular. Esta función de "hacer sonar las alarmas" constituiría una tarea importante del Consejo. Otra tarea sería garantizar que los derechos humanos sean parte integral de todas las actividades de otros órganos de las Naciones Unidas[526].

La antigua Comisión de Derechos Humanos había establecido varios procedimientos y mecanismos para examinar, monitorear e informar públicamente sobre la situación de los derechos humanos en países específicos o sobre derechos o temas específicos. específico. Todos estos procedimientos constituyen los "procedimientos especiales" de la Comisión. Los procedimientos especiales están en el corazón del sistema de derechos humanos de las Naciones Unidas. Son uno de los principales logros de la Comisión y se encuentran entre "*las herramientas más innovadoras, confiables y flexibles del sistema de derechos humanos*"[527]. Son únicos en su naturaleza porque son independientes, accesibles para las víctimas de violaciones de derechos humanos, abiertos, no selectivos, de alcance universal y porque pueden realizar investigaciones sobre cuestiones o situaciones específicas de los derechos humanos.

[526] Eudes, M. (2006) *De la Commission au Conseil des droits de l'homme : vraie réforme ou faux-semblant?*. Annuaire français de droit international, volume 52, pp. 599-616.
[527] Amnesty international, *Les procédures spéciales des Nations unies : piliers de la protection des droits humains*, p. 5, disponible en: https://www.amnesty.org/download/Documents/84000/ior400172005fr.pdf.

Los procedimientos especiales permiten:

1- Realizar misiones de investigación en los países,

2- Enviar comunicaciones y solicitaciones urgentes a los gobiernos,

3- Publicar declaraciones de prensa o comunicados de prensa,

4- Identificar tendencias o problemas emergentes,

5- Contribuir al desarrollo de estándares de derechos humanos,

6- Presentar informes al Consejo de Seguridad y, a veces, a la Asamblea General.

La Resolución 60/251 de la Asamblea General establece que el Consejo de Derechos Humanos "*asumirá, revisará y, según sea necesario, mejorará y racionalizará todos los mandatos, mecanismos, funciones y funciones de la Comisión de Derechos Humanos para mantener el régimen de procedimientos especiales*" y agrega que "*el Consejo completará esta revisión dentro de un año de la celebración de su primera sesión*". Por lo tanto, los procedimientos especiales son asumidos por el Consejo de Derechos Humanos y la resolución le pide que continúe manteniendo un régimen de procedimientos especiales. La resolución autorizó además al Consejo a "revisar y, si es necesario, mejorar y racionalizar todos los mandatos" dentro del año siguiente a su primera sesión (en junio de 2006).

Con respecto a la elegibilidad de los miembros, Kofi ANNAN aboga por la posibilidad que los miembros del Consejo de Derechos Humanos serán elegidos por una mayoría de dos tercios de la Asamblea General y ya no se basarán en las nominaciones dentro de los grupos regionales como es el caso actualmente en la Comisión, porque permiten el nombramiento de países que violan los derechos humanos en una escala masiva como Sudán y Zimbabue[528]. Este método de nombramiento haría que los Estados miembros sean más responsables, ya que serán elegidos entre aquellos que respetan los más altos estándares de derechos humanos y aumentan la autoridad del Consejo Económico y Social.

La idea contenida en esta propuesta es de crear una especie de competencia virtuosa entre los estados. Los países candidatos, en el momento de su elección por la

[528] Freih, L. (2005) *Les droits de l'homme seront mieux défendus sans leur Commission*, Revue Le Temps.

Asamblea General, deben comprometerse con un cierto número de puntos, en particular: abrir sus territorios a relatores especiales de la ONU, así como prometer ratificar y respetar convenciones importantes etc.: es en teoría sobre la base de sus compromisos que serán elegidos[529].

Además, los países candidatos podrían competir en la cuestión de la implementación de las obligaciones frente al sistema de los derechos humanos. Por esto, se trata de responder positivamente a las siguientes preguntas: ¿Han ratificado los candidatos los tratados de derechos humanos? ¿Están actualizados sus informes sobre la implementación de los tratados ratificados? ¿Han acordado cooperar plenamente con las Naciones Unidas, incluso con investigadores o relatores independientes? ¿Permiten una sociedad civil libre y una prensa independiente? Quizás sería prudente considerar que los países que han pasado por una transición significativa de un régimen de dictadura a un sistema democrático podrían sentarse en este consejo para compartir sus experiencias. La particularidad de estas condicionalidades es que ponen en tela de juicio el sistema de representación geográfica equitativa, además, el incumplimiento por parte del Estado miembro de sus compromisos o no lo expone automáticamente a sanciones al final de un período de prueba de doce meses por su exclusión del proceso. Dicha obligación resulta de la combinación de los Artículos 1 (3), 55 y 56 de la Carta de las Naciones Unidas[530].

Pero la implementación de estas condicionalidades requiere la revitalización de otras entidades de las Naciones Unidas que puedan intervenir en la protección de los derechos humanos a través de cualquier asistencia técnica o apoyo a las instituciones nacionales de defensa, de modo que las normas internacionales ahora se respetan mejor[531].

6. 2. Mecanismos institucionales y legales implementados al nivel regional para garantizar y proteger los derechos humanos

La presunción de la universalidad de los derechos humanos no ha impedido la creación de mecanismos regionales para la protección de los derechos humanos. Estos mecanismos no compiten con los llamados instrumentos legales "universales", por el

[529] Kazan, P. (2005) *La Commission : un organe politique*, disponible en: www.toile.org/psi.
[530] FIDH, Réforme de la CDH : préserver son mandat et ses mécanismes de protection, Eléments de proposition de la FIDH devant la Commission des droits de l'homme, 11 avril 2005 (http://www.droitsfondamentaux.prd.fr/codes/templates/en_t/images/codes/bandeauTitre.gif)
[531] Kamwanga, K. D. (2005) idem.

contrario, representan un poderoso apoyo para estos textos, al tiempo que tienen en cuenta la identidad específica y las características culturales de cada región. "Estos mecanismos agregan una riqueza significativa a la protección universal, ya que la complementan. De hecho, la solución regional o continental es interesante en la medida en que la naturaleza y la historia, al minimizar la diversidad de los sistemas socioeconómicos, han generado una concepción común de los derechos humanos"[532].

El análisis de los mecanismos de protección de los derechos humanos a nivel regional se llevará a cabo exclusivamente en los tres sistemas principales de protección existentes a este nivel, a saber: el sistema europeo, el sistema africano de protección de los derechos humanos y el sistema interamericano.

6.2.a. Mecanismos de protección en el sistema europeo.

El sistema europeo para la protección de los derechos humanos se basa esencialmente en el Convenio Europeo de Derechos Humanos (C.E.D.H.). Firmado el 4 de noviembre de 1950 y en vigor desde 1953, el Convenio Europeo de Derechos Humanos está inspirado en la Declaración Universal de Derechos Humanos. Es hoy el modelo más sofisticado de garantía efectiva de los derechos humanos, mediante el control judicial del respeto de sus derechos. Se trataba de establecer el orden público en las democracias de Europa. La originalidad del sistema radica en su carácter evolutivo y flexible, que se ha fortalecido gradualmente a través de reformas sucesivas. La Convención ha tenido un efecto indirecto innegable en todos los países europeos para una mejor defensa de los derechos humanos[533].

Antes de la reforma de 1994, tres instituciones compartían la responsabilidad del monitoreo: la Comisión Europea de Derechos Humanos, creada en 1954, el Tribunal Europeo de Derechos Humanos, establecido en 1959, el Comité de Ministros de Consejo de Europa, compuesto por los ministros de Asuntos Exteriores de los Estados miembros o sus representantes. El Tribunal Europeo de Derechos Humanos (T.E.D.H.) fue el primer tribunal cuya misión específica es supervisar el respeto de los derechos humanos. La Corte estaba compuesta por un número de jueces igual al número de estados miembros del Consejo de Europa y no al número de estados parte de la Convención.

[532] Ibidem.
[533] Oumba. P. (2008) idem., p. 15.

Sin embargo, la función de la Comisión era examinar la admisibilidad de las solicitudes dirigidas al Secretario General del Consejo de Europa. Podría ser incautado por los Estados parte y, cuando los Estados hayan aceptado el derecho de petición individual, por los solicitantes individuales (individuos, grupos de individuos u organizaciones no gubernamentales). Por lo tanto, formaba un filtro obligatorio para los solicitantes individuales, ya que no podían presentar una solicitud directamente ante el Tribunal. Las quejas exitosas eran objeto de un intento de llegar a un acuerdo amistoso. En caso de fracaso, la Comisión elaboraba un informe que establecía los hechos y formulaba una opinión sobre el fondo. La Comisión llevaba el asunto al T.E.D.H..

Con la adopción del Protocolo 11, el día 11 de mayo de 1994, se restaura "*el mecanismo de control establecido por la Convención a fin de mantener y fortalecer la eficacia de la protección de los derechos humanos y las libertades fundamentales*": los dos objetivos concretos son acortar la duración de los procedimientos y al mismo tiempo fortalecer el carácter judicial del sistema.

Entró en vigor el 1 de noviembre de 1998. La Comisión y el Tribunal Europeo de Derechos Humanos son reemplazados por un nuevo Tribunal permanente, que está compuesto por varios jueces iguales a las partes contratantes, elegidos por un período de 6 años y elegible para reelección. El propio Tribunal elige a su presidente y uno o dos vicepresidentes, por un período de 3 años. La Corte puede funcionar y emitir sentencias en comités de 3 jueces, en cámaras de 7 jueces y en una Gran Sala de 17 jueces. Este tribunal ahora puede ser incautado por una persona física, una organización no gubernamental o por un grupo de personas. La admisibilidad de las solicitudes es examinada directamente por el Tribunal. Las condiciones de admisibilidad siguen siendo las mismas y son relativamente severas, en particular debido al requisito de agotamiento de los recursos locales. De hecho, menos del 10% de las solicitudes se consideran admisibles, lo que no significa que el acceso al Tribunal sea difícil: el procedimiento es gratuito y el solicitante puede beneficiarse de asistencia legal tan pronto como su solicitud ha sido aceptada por el Tribunal.

Los poderes y la jurisdicción del Tribunal se describen mejor en su jurisprudencia: "(...) *su tarea, en virtud del artículo 19 de la Convención, es garantizar que los Estados firmantes respetan los compromisos derivados de la Convención. En particular, no le corresponde descubrir o sancionar los errores de hecho o de derecho*

presuntamente cometidos por un tribunal nacional, excepto en la medida en que pudieran haber infringido los derechos y libertades protegidos por la Convención"[534].

A pesar de los cambios provocados por el Protocolo núm. 11, al principio del siglo XXI, el Tribunal ya no podía tratar satisfactoriamente el creciente volumen de casos. A fines de 2003, alrededor de 65,000 solicitudes estaban pendientes ante la Corte. Además, el porcentaje de solicitudes que no condujeron a una sentencia sobre el fondo, generalmente porque fueron declaradas inadmisibles, fue superior al 90%. La segunda categoría más grande de solicitudes se refería a los llamados casos repetitivos, a saber, los casos que surgen de la misma causa estructural que un caso anterior en el que se ha dictado una sentencia del Tribunal que determina una violación del Convenio. Un ejemplo típico de solicitudes repetitivas se refiere a las denuncias en virtud del artículo 6 de la Convención sobre la duración excesiva de los procedimientos ante los tribunales nacionales.

Para garantizar la eficacia de la Corte a largo plazo, en el marco de la Conferencia Ministerial Europea sobre Derechos Humanos, celebrada en Roma los días 3 y 4 de noviembre de 2000, se invitó al Comité de Ministros a iniciar lo más antes posible, una reflexión profunda sobre las diversas posibilidades y opciones con el fin de garantizar la eficacia del Tribunal (...). Posteriormente, el Comité Directivo para los Derechos Humanos (CDDH) fue instruido por el Comité de Ministros para redactar un nuevo Protocolo con el fin de permitir que la Corte supere sus dificultades. También se creó un Grupo de reflexión sobre el fortalecimiento del mecanismo de protección de los derechos humanos (RDA). El CDDH transmitió al Comité de Ministros su informe final de actividades en abril de 2004, incluido el proyecto de protocolo de enmienda a la Convención.

Luego, el Comité de Ministros, durante la 114ª sesión ministerial en mayo de 2004, adoptó el Protocolo de enmienda y una Declaración para "*garantizar la efectividad de la implementación del Convenio Europeo de Derechos del hombre a nivel nacional y europeo"*. En esta declaración, los Estados miembros reconocieron la urgencia de la

[534] Véase el Caso P. G. y J. H. contra el REINO UNIDO, Sentencia 44787/98, parágrafo 76, disponible en: https://hudoc.echr.coe.int/eng#{%22appno%22:[%2244787/98%22],%22itemid%22:[%22001-59665%22]}.

reforma y se comprometieron a ratificar el Protocolo No. 14 dentro de dos años. El texto del Protocolo de modificación fue abierto a la firma de los Estados miembros del Consejo de Europa signatario del Convenio Europeo de Derechos Humanos el 13 de mayo de 2004 y entro en vigor el día 1 de junio de 2010 después de su ratificación por todas las partes.

A diferencia del Protocolo núm. 11, el Protocolo núm. 14 no realiza cambios radicales en el mecanismo de control del Convenio. El objetivo es más bien mejorar el funcionamiento del sistema ya establecido y de proporcionar a la Corte los medios procesales y la flexibilidad necesarios para tratar las solicitudes dentro de plazos aceptables, al tiempo que le permite concentrarse en los casos más importantes que requieren una revisión exhaustiva. Para hacer esto, realiza enmiendas en tres áreas principales:

- fortalecer la capacidad del Tribunal para filtrar un mayor volumen de solicitudes recibidas;

- imponer un nuevo criterio de admisibilidad (incluidas dos cláusulas de salvaguardia) con respecto a los casos en que el solicitante no ha sufrido ningún daño significativo;

- medidas para tratar casos repetitivos.

Sin embargo, habiendo sido el teatro principal de "*actos de barbaridad que revuelven la conciencia de la humanidad*" y en el espíritu de la Declaración Universal de Derechos Humanos, Europa ha registrado una evolución significante en la garantía internacional de los derechos humanos al establecer, en el marco del Consejo de Europa, instrumentos y mecanismos sólidos, en particular el mecanismo supranacional del Convenio Europeo de Derechos Humanos. La jurisprudencia del Tribunal Europeo de Derechos Humanos ha tenido un impacto profundo y beneficioso en los sistemas jurídicos y en la realidad social en los Estados miembros del Consejo de Europa. Cabe esperar que el sistema europeo pueda mantener su eficacia en un Consejo de Europa ampliado, aunque algunos estados aspirantes aún tienen un largo camino para cumplir los requisitos del respeto efectivo de los derechos humanos.

6.2.b. Mecanismos de protección en el sistema africano

El sistema africano de protección de los derechos humanos se basa en la Carta Africana de Derechos Humanos y de los Pueblos. El texto de la Carta, inspirado expresamente en la Declaración Universal de Derechos Humanos, fue adoptado el 27 de

junio de 1981 y entró en vigor el 21 de octubre de 1986. A diferencia de otros textos regionales, esta proclama que no sólo los derechos, pero también los deberes del individuo, lo que es en verdad una originalidad. El sistema africano para la protección de los derechos humanos está compuesto por dos órganos principales para vigilar el respeto de los derechos humanos, estos son la Asamblea de Jefes de Estado y de Gobierno y la Comisión Africana de Derechos Humanos, hombre y pueblos, que se complementa con la Corte Africana, pero veremos más adelante que esta Corte tiene unas competencias, una organización y un procedimiento que le son específicos.

La Comisión Africana tiene como funciones esenciales la promoción y protección de los derechos humanos y de los pueblos garantizados por la Carta Africana y otros instrumentos pertinentes (art. 30 de la Carta Africana). Como parte de su función protectora, la Comisión Africana tiene la facultad de recibir comunicaciones de Estados dirigidas contra otros Estados Parte en la Carta (arts. 47, 48 y 49) y otras comunicaciones (art. 55), incluidas en particular las quejas de las organizaciones no gubernamentales y/o de los particulares. Sin embargo, debe mencionarse que en ambos casos la Comisión Africana no tiene poder de decisión. Puede investigar, ponerse a disposición de las partes, intentar un acuerdo amistoso y, si es necesario, investigar casos, pero presenta sus informes a la Asamblea de Jefes de Estado y de Gobierno.

De ello se deduce que este órgano, es el verdadero órgano de decisión del mecanismo regional africano de derechos humanos, debido a su preeminencia en el proceso de toma de decisiones. La Asamblea de los Jefes de Estado y de Gobierno en realidad tiene el derecho de iniciativa frente a la Comisión, el poder de control y el de decisión: todas las decisiones finales relacionadas con el aspecto de protección de los derechos de hombre y pueblos por la Comisión, por lo tanto, es competencia de los Jefes de Estado y de Gobierno. Por eso, este organismo desempeña un papel real de censura de la Comisión.

La Corte Africana de Derechos Humanos ha sido establecida por el Protocolo adoptado el 9 de junio de 1998, entrado en vigor el 24 de enero de 2004. La Corte tiene una triple competencia: en primer lugar, la competencia consultiva de la Corte (art. 4 del Protocolo): la Corte puede emitir una opinión a solicitud de un Estado miembro de la UA o de una organización reconocida por la Corte, sobre los derechos garantizados por la Carta o sobre cualquier otra disposición de un instrumento jurídico relacionado con los

derechos humanos. Luego, la solución amistosa de controversias (art. 9 del Protocolo): la Corte "puede intentar" resolver las controversias de manera amistosa antes de iniciar un procedimiento contencioso de solución de controversias. Finalmente, la competencia contenciosa de la Corte (art. 3, 5, 6, 7 del Protocolo): la Corte puede recibir y atender solicitudes de la Comisión Africana, un Estado Parte en el Protocolo y cualquier organización internacional africana, tendientes a denunciar la violación de los derechos humanos por parte de un Estado Parte. Las ONG que tienen la calidad de observador ante la Comisión Africana y las personas también pueden presentar una solicitud ante la Corte, si y solo si el Estado implicado en la violación de los derechos humanos ha aceptado dicha jurisdicción, de conformidad con las Artículo 34.6 del Protocolo (Capítulo 4). La Corte también tiene competencia (art. 3 del Protocolo) para pronunciarse sobre cualquier controversia que se le señale en relación con la interpretación de las disposiciones de la Carta y cualquier otro instrumento de derechos humanos pertinente ratificado por los Estados interesados.

En términos de procedimiento, una de las diferencias fundamentales entre la Corte Africana y la Comisión, que examina los mismos tipos de violaciones de derechos humanos, es la judicialización del proceso de solicitud. Esto permite la transparencia en el tratamiento de los casos, la igualdad de las partes y su representación, de acuerdo con los principios generales del derecho a un juicio justo reconocidos por los tratados regionales e internacionales de protección de los derechos humanos. El Protocolo que establece la Corte Africana reserva un lugar importante para las víctimas al otorgarles participación, representación, protección y reparación. Estas disposiciones, complementadas por el Reglamento, deben ir acompañadas de una práctica que respete los derechos de las víctimas para asegurar la efectividad de la Corte. Las decisiones de la Corte Africana son vinculantes, a diferencia de las comunicaciones de la Comisión. Por otro lado, su ejecución depende de la voluntad de los Estados.

Aunque en los últimos años, el lugar de la Corte Africana de Derechos Humanos ha sido objeto de un animado debate científico y político. De hecho, la Asamblea de Jefes de Estado de Gobierno de la Unión Africana, durante su sesión ordinaria de julio de 2004 en Addis Abeba, decidió que: "*la Corte Africana de Derechos Humanos y de los Pueblos y el Tribunal de la justicia se fusionará en un solo Tribunal*".

Esta decisión de la Asamblea dio lugar a la preparación de un proyecto de protocolo que establece el estatuto de la Corte Africana de Justicia y Derechos Humanos. Desde entonces, el proceso de fusión está muy avanzado y su cristalización se manifestará con la adopción definitiva del Proyecto de Protocolo que establece el Estatuto de la Corte Africana de Justicia y Derechos Humanos. Sin embargo, el interés científico de esta reflexión no radica en el contexto del proceso evolutivo y formativo de la institucionalización de la fusión, sino en el de la conveniencia de fusionar la Corte de Justicia de la Unión Africana con la Corte de los derechos humanos y de los pueblos africanos.

El establecimiento de la Corte Africana de Derechos Humanos y de los Pueblos representa un paso definitivo hacia una garantía efectiva de los derechos y libertades de las personas. Sin embargo, el artículo 34 (6) del Protocolo relativo a la Corte Africana de Derechos Humanos, que hace imposible la toma de posesión de la Corte por parte de individuos u ONG si y solo si el Estado en cuestión ha hecho el famoso declaración, representa un verdadero mecanismo de frenado basado en las esperanzas suscitadas por esta Corte. Sin embargo, en el contexto de la fusión, el Proyecto de Protocolo sobre el Estatuto de la Corte Africana de Justicia y Derechos Humanos en el Artículo 31 no hace reservas en cuanto a la posibilidad de remisión a la Corte por parte de individuos o ONG, como el Protocolo núm. 11 del Convenio para la protección de los derechos humanos y las libertades fundamentales, de 11 de mayo de 1994.

Si bien, al firmar el protocolo, es posible que los Estados ingresen reservas, pero este aspecto aún está en negociación. Sin embargo, el texto inicial no incluye ninguna exclusión. La fusión también permite introducir una sección de derechos humanos en el arreglo institucional del Acta Constitutiva de la Unión. Si el Protocolo que establece la Corte Africana de Derechos Humanos no otorga fuerza vinculante a las sentencias de la Corte, el Proyecto de Protocolo de la Corte resultante de la fusión, prevé la posibilidad de que la Conferencia sancione la no ejecución de una sentencia de la Corte en su artículo 47. La fusión permite, por tanto, extender el régimen jurídico de las sanciones a las sentencias relativas a los derechos humanos.

Aun cuando, algunos autores[535] creen que el argumento de racionalización de recursos y optimización de costos que se había mantenido como pilar de la fusión de los dos tribunales, en realidad enmascara el deseo de enterrar la Corte Africana de Derechos Humanos. La calificación de los jueces podría no estar relacionada con los derechos humanos y, por lo tanto, se produciría un retroceso de la jurisprudencia desarrollada con valentía por la Comisión Africana de Derechos Humanos durante los últimos quince años.

6.2.c. Mecanismos de protección en el sistema interamericano.

El sistema interamericano para la protección de los derechos humanos comenzó formalmente con la adopción de la Carta de la Organización de los Estados Americanos[536] en 1948, que proclamaba que la protección de los derechos fundamentales, como una piedra angular del fundamento sobre cual se basaba la organización de los estados americanos.

Este principio ha sido consagrado en la Declaración Americana de los Derechos y Deberes del Hombre. De naturaleza esencialmente declarativa, la Declaración Americana de los Derechos y Deberes del Hombre fue reforzada en 1978 por la Convención Americana sobre Derechos Humanos. De esta Convención nació la Comisión de Derechos Humanos, cuya tarea principal es promover la observación y defensa de los derechos humanos y la Convención Americana sobre Derechos Humanos (CADH).

Responsable de garantizar la aplicación e interpretación de la Convención, la Comisión Interamericana de Derechos Humanos también recibe y analiza, después de que el Estado miembro ha reconocido su competencia, las peticiones de personas que contienen denuncias o quejas relacionadas con violación de la Convención Americana sobre Derechos Humanos por parte de los Estados miembros[537]. El sistema interamericano para la protección de los derechos humanos incluye dos mecanismos de monitoreo: la Comisión Interamericana de Derechos Humanos y la Corte Interamericana

---

[535] Boukongou, J.D. (2007) *Dignité humaine en Afrique centrale 1990-2007*, APDHAC, Yaoundé, 9 juin 2007, p. 114, recuperado de :
http://www.cmeyanchama.com/Documents/Guinee/DignitehumaineenAfriqueCentrale2007.pdf

[536] Carta de la Organización de los Estados Americanos, firmada en Bogotá, Colombia el 30 de abril de 1948 en la Novena Conferencia Internacional Americana, entrada en vigor el 13 de diciembre de 1951, disponible en: http://www.oas.org/dil/esp/afrodescendientes_manual_formacion_lideres_anexos.pdf.

[537] Hilling, C. (1991) *Le système interaméricain de protection des droits de l'Homme : le modèle européen adapté aux réalités latino-américaines*, Revue Québécoise de droit international, vol. 7-2/1991, pp. 210-217.

de Derechos Humanos. La Comisión Interamericana de Derechos Humanos está compuesta por siete miembros (artículo 34 de la CADH). Esto corresponde a un organismo mucho más pequeño que la antigua Comisión Europea, que por su parte estaba compuesta por tantos miembros como las Altas Partes Contratantes, o el Comité de Derechos Humanos de las Naciones Unidas, que cuenta 18 miembros. Los siete miembros representan a todos los Estados Parte[538] de la Convención Americana (artículo 35 de la CADH).

Antes de la adopción de la CADH, el papel de la Comisión Interamericana de Derechos Humanos consistía en promover y observar el respeto de los derechos humanos y las libertades protegidos por la Declaración Americana de los Derechos y Deberes del Hombre. Su papel era esencialmente consultivo. Solo después de la adopción de la CADH, la Comisión de Derechos Humanos recibió la competencia para recibir y solucionar las peticiones (denuncia o queja relacionada con violación de un derecho presentado por cualquier persona) y las comunicaciones (denuncia de una violación de un derecho presentada por un Estado miembro).

Por lo tanto, desde la adopción de la Convención Americana sobre Derechos Humanos, la Comisión Interamericana de Derechos Humanos[539] y el Corte Interamericana de Derechos Humanos[540] son las instituciones que garantizan el cumplimiento de los principios y las obligaciones previstas en la CADH. El sistema interamericano de derechos humanos funciona en dos fases. La jurisdicción inicial pertenece a la Comisión de Derechos Humanos, mientras que la Corte de Derechos Humanos solo tiene jurisdicción después del agotamiento de los recursos ante la Comisión Interamericana de Derechos Humanos. En cierto modo, se podría argumentar que la Comisión Interamericana de Derechos Humanos sienta en primera instancia mientras que la Corte tiene jurisdicción de apelación "limitada" sobre las decisiones de la Comisión.

La tarea principal de la Comisión es promover, monitorear y defender los derechos humanos decretados por la Declaración Americana de los Derechos y Deberes

[538] Argentina, Barbados, Bolivia, Brasil, Chile, Colombia, Costa Rica, Dominica, Ecuador, El Salvador, Granada, Guatemala, Haití, Honduras, Jamaica, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Surinam y Uruguay.
[539] con la sede en Washington D.C., EE. UU
[540] con la sede en San José, Costa Rica

del Hombre y la Convención Americana sobre Derechos Humanos. Responsable de garantizar la aplicación e interpretación de la Convención sobre Derechos Humanos, la Comisión Interamericana de Derechos Humanos también escucha, después de que el Estado miembro ha reconocido su competencia, las peticiones de personas que contienen denuncias o quejas relacionadas con la violación de la Convención Americana sobre Derechos Humanos por parte de cualquiera de los estados miembros. También es competente para examinar comunicaciones en las que un Estado miembro alega que otro Estado miembro ha violado los derechos humanos establecidos por la Convención. Si la Comisión acepta la petición o la comunicación, y en ausencia de una resolución satisfactoria, elaborará un informe que se enviará al peticionario y a los Estados miembros. Si las conclusiones del informe de la Comisión no se han cumplido después del vencimiento de tres meses a partir de la fecha de su entrega a las partes interesadas o si el caso no se ha remitido a la Corte Interamericana de derechos humanos, la Comisión podrá emitir un dictamen y conclusiones sobre la cuestión sometida a su examen. Luego formulará recomendaciones específicas e impondrá un plazo dentro del cual el Estado miembro debe tomar las medidas necesarias para remediar la violación de los derechos garantizados por la Convención Americana sobre Derechos Humanos.

La Corte Interamericana de Derechos Humanos, establecida el día 3 de septiembre de 1979, a través de la Convención Americana sobre Derechos Humanos en San José, Costa Rica, ejerce una función contenciosa, dentro de la que se encuentra la resolución de casos contenciosos y el mecanismo de supervisión de sentencias; una función consultiva; y la función de dictar medidas provisionales. Si bien hace veinte años ningún Estado Parte reconoció la jurisdicción contenciosa obligatoria de este tribunal, hoy existen veinte de ellos sometidos a la jurisdicción de la Corte[541]. La actividad judicial de este tribunal durante sus primeros veinte años de existencia es bastante extensa: 46 sesiones ordinarias, 23 sesiones extraordinarias al final de las cuales adoptó, en relación con 35 casos contenciosos, 16 opiniones consultivas y 61 sentencias que tienen se ocupa de las excepciones preliminares, las cuestiones de competencia y fondo, la ejecución de los laudos relativos a las reparaciones y finalmente la interpretación de las sentencias. También ha adoptado medidas de protección provisionales en más de veinte casos de extrema gravedad y urgencia, que han ayudado a prevenir daños irreparables a las

[541] Argentina, Barbados, Bolivia, Brasil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Haití, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Surinam y Uruguay.

personas. La Corte de Derechos Humanos no tiene jurisdicción hasta después del agotamiento de los recursos ante la Comisión Interamericana de Derechos Humanos y solo los estados miembros de la CADH, excluyendo individuos, pueden remitir un caso a la corte.

Al igual que los procedimientos ante la Comisión Interamericana de Derechos Humanos, la jurisdicción de la Corte Interamericana de Derechos Humanos deriva del consentimiento expreso de los Estados miembros. Cuando reconozca que se ha violado un derecho o una libertad amparados por la Convención Americana sobre Derechos Humanos, la Corte ordenará que el Estado miembro garantice a la parte lesionada el libre goce de sus derechos y orden también compensación, que tomará la forma de una "compensación justa", para la parte perjudicada. La sentencia de la Corte Interamericana de Derechos Humanos es definitiva y vincula a los Estados miembros. La Corte Interamericana de Derechos Humanos también puede, con base en una solicitud hecha por un estado miembro, emitir opiniones consultivas sobre la interpretación y aplicación de la Convención Americana sobre Derechos Humanos.

En síntesis, para que la Corte Interamericana de Derechos Humanos pueda emitir una sentencia específica contra un estado miembro relacionada con la violación de un derecho o una libertad protegida por la Convención Americana sobre Derechos Humanos, es imperativo que el Estado miembro dé su consentimiento expreso en varias ocasiones. Primero, debe haberse adherido a la Convención Americana sobre Derechos Humanos. Posteriormente, debe haber reconocido expresamente la jurisdicción de la Comisión Interamericana de Derechos Humanos. De hecho, el Estado miembro debe haber dado su consentimiento expreso en al menos tres ocasiones antes de que la Corte Interamericana de Derechos Humanos pueda imponerle su decisión.

6.3. Mecanismos implementados al nivel estatal

6.3.1. Mecanismos estatales institucionales

Cada sistema de derecho tiene medios específicos para defender el derecho a la vida privada. En los estados con un sistema legal anglosajón, la práctica de los tribunales tiene el papel predominante en la definición y la protección de las garantías de este derecho, basado en la interpretación creativa de los principios deducidos de las disposiciones constitucionales o estatutarias. Partidarios del sistema de autorregulación, los EE. UU. promueven el establecimiento de mecanismos internos de verificación y

control a nivel de las diversas agencias o empresas, que tienen el papel determinado de contribuir a la consolidación de una política correcta para respetar el derecho a la privacidad. Dichos mecanismos también fueron "prestados" por los estados europeos, de modo que, inicialmente, al nivel de las personas jurídicas de derecho privado, y últimamente dentro de algunas instituciones públicas, se introdujo la institución del oficial de protección de datos (data protection officer). Éste es un profesional independiente cuya función es supervisar el cumplimiento de las normas legales y procesales sobre el derecho a la vida privada y la protección de datos personales dentro de un "operador de datos personales", colaborando activamente con las autoridades de protección de la vida privada/ de los datos personales de los Estados miembros de la U.E. Esta institución fue regulada por primera vez por la Directiva no. 95/46/CE, como un medio alternativo al sistema clásico de notificación de procesamiento de datos con las autoridades de protección de la vida privada/ los datos personales, actualmente incorporada en la legislación nacional de Alemania, Francia, Holanda, Suecia y Luxemburgo. Actualmente el régimen legal del oficial de protección de datos está regulado por Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Los principales mecanismos institucionales para la defensa del derecho a la vida privada en Europa están representados por las autoridades independientes, designadas para este propósito, con el estatuto de autoridades administrativas públicas, con una sola persona o liderazgo colegiado. En algunos estados, la naturaleza administrativa de la autoridad es duplicada por la jurisdiccional, derivada de las atribuciones y el procedimiento seguido para garantizar el derecho a la vida privada. Es el caso de la institución competente en Francia (La Comisión Nacional de Informática y Libertades), tras los cambios introducidos en la ley de 1978 durante el año 2004, ha adquirido nuevas atribuciones, en virtud de las cuales la llamada "formación contenciosa", compuesta por seis miembros, se reúne (al menos) mensualmente para decidir sobre la sanción de los operadores controlados o la emisión de decisiones para suspender/cesar el procesamiento de datos personales (incluso, en función de las quejas recibidas para la solución).

En los estados federales (como en el caso de Alemania), tales autoridades se establecen tanto a nivel federal como en los estados federados, por lo general sus deberes

son distintos. Algunas de estas autoridades tienen una doble competencia legal, para seguir el respeto no solo de la legislación relativa a la protección del derecho a la vida privada o del derecho a la protección de datos personales, sino también a garantizar el libre acceso a la información de interés público (el caso de Alemania). En nuestra opinión, la existencia de una autoridad única facultada con la aplicación de la legislación en los dos campos es capaz de garantizar un equilibrio justo y necesario entre los dos derechos fundamentales: la vida privada y la información.

Una de las características importantes de estas autoridades es el respeto por su estatuto independiente, desde un punto de vista institucional (no subordinadas a las autoridades estatales), funcional (no estar sujetas a instrucciones sobre el contenido y la extensión de su actividad), material (beneficiarse de una infraestructura adecuada y recursos financieros suficientes para cumplir con sus deberes legales). La exigencia de la independencia de las autoridades de protección de datos personales también se ha reafirmado recientemente en la jurisprudencia de T.J.U.E. en dos casos en los que declaró que Alemania y Austria respectivamente no cumplieron con sus obligaciones en virtud del art. 28 párrafo (1) de la Directiva no. 95/46/CE, ya que transpusieron incorrectamente el requisito de que las autoridades de protección de datos ejerzan sus atribuciones "con total independencia". Con la adopción del Reglamento general de protección de datos y su entrada en vigor en el año 2016, el problema de incorrecta interpretación o implementación ya ha desaparecido, porque sus artículos son obligatorios y de directa aplicación para todos los estados miembros de la UE.

Un papel importante para garantizar el respeto del derecho a la vida privada, en las relaciones entre los ciudadanos y las autoridades públicas, son también las instituciones del defensor del pueblo (su equivalente a nivel de la UE es el Defensor del Pueblo Europeo), cuya competencia general es la defensa de los derechos fundamentales (por ejemplo, incluyendo el derecho a la vida privada), competencia que se limita a las autoridades públicas con atribuciones administrativas, y su acción no es de tipo coercitivo. En algunos estados europeos (Eslovenia, Hungría), a estas instituciones también se les asignó la función de supervisar el cumplimiento de la legislación sobre la protección de datos personales, como fue el caso de Rumanía, donde durante el período 2001-2005 el Defensor del Pueblo cumplió con las competencias acumulativas y de ese tipo.

En los EE. UU., una de las (pocas) autoridades administrativas involucradas en el respeto del derecho a la vida privada es la Comisión Federal de Comercio (*Federal Trade Commission, establecida en 1914*), que tiene deberes principalmente con respecto al respeto de los derechos de los consumidores y garantizar una competencia leal. Sobre la base de la competencia general para contribuir a combatir las "prácticas y los actos injustos o disuasivos", esta institución federal ejerce sus atribuciones, incluso en el ámbito del derecho a la privacy (en términos de la protección de los menores en el uso del Internet, de las prácticas ilegales relacionadas con el robo de identidad, tomando las medidas apropiadas de seguridad, etc.). Por otro lado, bajo la Ley de la Libertad de Información (el famoso "FIA - Freedom of Information Act" de 1966) y la Ley de la vida privada (1974), todas las agencias del gobierno federal en los EE. UU. tienen la obligación de respetar los dos derechos fundamentales de cualquier ciudadano estadounidense (o extranjero que resida legalmente en el territorio estadounidense).

Dada la evolución de las relaciones entre la U.E. y los Estados Unidos en relación con el intercambio de informaciones sobre personas sospechosas de terrorismo y otros delitos penales específicos del crimen organizado, se ha agudizado cada vez más la cuestión de la necesidad de respetar también en el territorio de los Estados Unidos, las normas relativas a la protección del derecho a la vida privada. En consecuencia, las recomendaciones de las autoridades europeas se refieren, entre otras cosas, al establecimiento en este estado de una institución central para la protección del derecho a la vida privada, junto con el reconocimiento del derecho a presentar daños ante los tribunales de derecho común, incluso a favor de los ciudadanos de otros estados, para garantizar recursos administrativos y judiciales efectivos.

En particular, este último derecho ha sido reafirmado por las autoridades estadounidenses como una garantía para respetar los derechos de los ciudadanos europeos cuya confianza se ha visto profundamente sacudida por las revelaciones realizadas en el año 2013 por el ex colaborador externo de la Agencia de Seguridad Nacional de los Estados Unidos, Edward Snowden, con respecto a programas gubernamentales (como PRISM) a través de los cuales las compañías de Internet estaban (son) obligadas a poner a la disposición de los servicios secretos de Estados Unidos informaciones obtenidas por medios de comunicaciones electrónicas privadas.

6.3.2. Mecanismos jurisdiccionales

Aunque en términos temporales, el recurso a un tribunal puede significar juzgar un juicio por un tiempo irrazonablemente largo, sin embargo, la vía judicial fue y sigue siendo el medio más efectivo para defender efectivamente los derechos de las personas. Con respecto al derecho a la vida privada, como hemos visto, a nivel regional (supraestado), se ha desarrollado una jurisprudencia rica y muy útil, a través de la contribución realizada por el T.E.D.H. al establecer el contenido y los límites del ejercicio de este derecho individual, en relación con los estados signatarios de la Convención. Queda por ver hasta qué punto T.J.U.E. a su vez, desempeñará un papel importante para garantizar el respeto del derecho a la vida privada, en el contexto de la entrada en vigor del Tratado de Lisboa, con los dos efectos principales producidos: la fuerza legal obligatoria de la Carta de los Derechos Fundamentales de la Unión Europea y la futura adhesión de la Unión Europea U.E. a la Convención, acto del Consejo de Europa.

Durante el año 2014, T.J.U.E., también dio una señal importante en la línea de afirmar su compromiso de respetar las normas de protección del derecho a la vida privada y la protección de los datos personales en dos causas principales para fijar el papel importante de los derechos fundamentales en el orden legal de la U.E. y para subrayar la propia visión de la U.E. en relación con la protección de datos personales en relación con terceros países. Estos casos confirman lo excesivo de la retención de datos de tráfico (motivo para invalidar una directiva) y la aplicabilidad del derecho de la U.E. en caso de indexar datos personales por el motor de búsqueda de Google (motivo para obligar a la empresa estadounidense a eliminar datos).

Desde la perspectiva del orden jurídico interno, los estados asociados con el sistema de derecho continental desarrollaron un mecanismo jurisdiccional en dos niveles: el relacionado con el sistema judicial clásico, basado en la práctica de los tribunales ordinarios y el correspondiente a la jurisdicción constitucional. Por lo tanto, cualquier persona que considere que su derecho a la vida privada ha sido violado por una disposición legal puede dirigirse a los tribunales de litigios constitucionales, por lo general, por medio de un problema específico relacionado con el control de la constitucionalidad a posteriori (España, Francia, Suiza, Rumanía) o pidiendo a la institución del Defensor del Pueblo que intervenga en su nombre (en Rumanía, de acuerdo con el artículo 146 letra d) de la Constitución, el Defensor del Pueblo puede presentar directamente una queja de inconstitucionalidad ante el Tribunal Constitucional). Si la

violación del derecho a la vida privada se produjo sobre la base de un acto administrativo, el tribunal de contencioso constitucional (Alemania, España) o el tribunal ordinario (en este caso, el tribunal administrativo-Francia, Rumanía) es competente para decidir; en el caso de estos últimos tribunales también siguen siendo las acciones que tienen por objeto el no respetar el derecho a la vida privada en las relaciones jurídicas derivadas de otros tipos de actos y hechos.

Estos dos tipos de control jurisdiccional son complementarios a los que se llevan a cabo a nivel supraestatal, ya que las sentencias finales de los tribunales (e incluso de los tribunales constitucionales, en algunos casos) pueden apelarse ante el T.E.D.H., después de que los recursos internos se hayan agotado y, por otro lado, la interpretación del derecho de la U.E. (que también incluye la Carta) pueden ser señalada ante el Tribunal de Luxemburgo por los tribunales nacionales.

Interesante de observar es el hecho de que la influencia jurisprudencial es mutua: los tribunales nacionales tienen en cuenta los principios consagrados en las sentencias dictadas por el tribunal de Estrasburgo, y éste, a su vez, a elegir el mejor razonamiento para las soluciones pronunciadas, a menudo se refiere a la práctica de los tribunales de los Estados miembros, en particular, aquellos con el papel de contencioso constitucional.

La evolución de la jurisprudencia constitucional de algunos Estados miembros con respecto a la legislación nacional que transpone los textos europeos con respecto a la obligación de retención incondicional y permanente de datos de tráfico, demuestra una cierta declaración programática (más o menos explícita) de los estados que desean preservar su supremacía constitucional sobre la de la Unión con respecto a las garantías que deben ser aseguradas a los derechos fundamentales (en este caso, el derecho a la vida privada).

Sin embargo, Rumanía, a diferencia de Alemania, bajo la amenaza de una acción que podría haber sido introducida por la Comisión Europea por incumplimiento de las obligaciones de los Estados miembros de conformidad con los tratados constitucionales de la U.E., adoptó una nueva ley para la implementación de la Directiva 2006/24/CE que, aunque mantuvo los mismos vicios de inconstitucionalidad notificados por el Tribunal Constitucional, no estuvo sujeto al control ante este tribunal solo después de la sentencia del T.J.U.E. de invalidación del acto principal.

Además, el impacto de las decisiones de los tribunales constitucionales de algunos Estados miembros fue lo suficientemente profundo como para marcar un cambio en la Comisión Europea que comenzó a buscar una solución de compromiso para enmendar esa directiva. Mientras tanto, el mismo T.J.U.E., como se mencionó anteriormente, declaró la invalidez de la Directiva no. 2006/24/CE, por razones relacionadas con la protección del derecho a la vida privada y a la protección de los datos personales, un hecho que, sin embargo, deja a la evaluación de cada Estado miembro la necesidad de una intervención legislativa sobre el derecho interno.

6.3.3. Tipos de responsabilidad jurídica en caso de violación de los derechos fundamentales

La garantía efectiva del derecho a la vida privada implica rigurosamente la existencia de medidas legales para responsabilizar las personas culpables de la violación de este derecho. Los sujetos activos de la responsabilidad jurídica pueden ser los estados en el orden legal internacional (o regional), pero también en el interno, a través de las autoridades representativas, así como los individuos (personas jurídicas o físicas). Las formas de responsabilidad jurídica en caso de la violación del derecho a la vida privada son las clásicas tipologías conocidas en derecho: civil, penal y administrativa.

6.3.3.1. La responsabilidad civil delictiva

Este tipo de responsabilidad interviene en los casos de vulneración del derecho a la vida privada (lato sensu) es decir con todos sus elementos y derechos derivados. La violación del derecho a la imagen o a la reputación, por ejemplo, da lugar a la facultad del titular de estos derechos para solicitar a los tribunales de derecho común que el culpable reparen los daños producidos y otorguen daños y perjuicios.

En Francia, en virtud de las disposiciones procesales civiles, el juez tiene derecho a imponer medidas para prevenir daños inminentes o detener una manifestación ilícita: la publicación de un derecho de respuesta, la prohibición de un programa de televisión, la rectificación de algunas informaciones. Sin embargo, dada la interferencia con la libertad de expresión y la libertad de prensa, tales medidas solo están disponibles

en casos de necesidad, cuando el daño del ser humano es de una severidad intolerable, es decir, en aquellos casos en los que, si la lesión continuara, sería al menos irremediable[542].

En el derecho estadounidense, este tipo de responsabilidad consiste en el llamado "*tort law*"[543] donde el "*right to privacy*" goza de una protección concebida de manera pretoriana. La invasión de la privacidad, un acto ilícito civil basado en el derecho consuetudinario que permite a la parte afectada entablar una demanda contra una persona que interviene ilegalmente en sus asuntos privados, divulga su información privada, la publicita de forma falsa o se apropia de su nombre para beneficio personal.

En Rumanía, el capítulo IV del Nuevo Código Civil ha desarrollado las disposiciones relativas a la comisión de responsabilidad delictiva con respecto a los derechos no patrimoniales (de los cuales se incluye también el derecho a la vida privada), en el sentido de que la persona que se considera perjudicada puede solicitar al tribunal, incluido el autor del delito, a su cargo, tras la publicación de la sentencia de condena, así como cualquier otra medida necesaria para cesar el comportamiento que produce el hecho ilícito o reparar el daño causado (art. 1349):

> "*(1) Toda persona tiene la obligación de respetar las reglas de conducta impuestas por la ley o las costumbres del lugar y no perjudicar, con sus acciones u omisiones, los derechos o intereses legítimos de otras personas.*
>
> *(2) El que, teniendo discernimiento, viole este deber, responde de todos los daños causados, estando obligado a repararlos íntegramente."*

Al mismo tiempo, *la persona que causa un daño por el mismo ejercicio de sus derechos no está obligada a repararlo, salvo que se abuse del derecho (art. 1353)*. La responsabilidad para el prejudicio sufrido de une persona como consecuencia de un acto culpable no puede ser limitada o excluida por convenios o actos unilaterales. Las acciones para recuperar el derecho no patrimonial infringido o para restaurar la integridad de la

[542] Viney, G. (2002) *Traité de droit civile. Les obligations. La responsabilité : effets*. Editorial Dalloz Paris, p. 565.

[543] Según el diccionario jurídico, , el tort es un agravio o ilícito civil (civil wrong), especifico para los países del Common Law, "cometido por una persona legalmente responsable (legally liable) llamado tortfeasor, que causa un perjuicio, un daño o una pérdida (injury, loss or harm) a un tercero. El Tort Law es, en consecuencia, aquella parte del Derecho que se ocupa de los actos ilícitos cometidos por personas físicas (individuals) y jurídicas (legal entities) que, sin embargo, no pueden ser considerados delitos penales (crimes) ni incumplimientos de contratos (breach of contract). No existe, por tanto, delito (crime o offense), ni incumplimiento de contrato pues no existe relación contractual (contractual relation) entre el que lo comete y el perjudicado. El tort se considera un motivo de reclamación perteneciente al Derecho civil (grounds of action in Civil Law)". Texto recuperado de: https://traduccionjuridica.es/en-que-consiste-el-tort/.

memoria de un difunto (por ejemplo) pueden ser iniciadas o continuadas incluso por el cónyuge sobreviviente o sus familiares (art. 256 del Código Civil).

En España, el artículo 1.902 del Código Civil establece un régimen de responsabilidad por hecho propio, basado en una conducta humana, consciente y voluntaria, que excluye del sistema de responsabilidad los hechos naturales que causen daño: "*el que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado*".

En la responsabilidad civil subjetiva siempre la culpa tiene el papel principal dentro de la conducta ejecutada por el agente del daño. Por a contrario de lo que sucede en la responsabilidad objetiva, la culpa permanece como elemento indispensable de la responsabilidad. Aunque el Código Civil español no considere el carácter culposo o injusto del daño sufrido por un tercero por culpa del agente, esta idea se encuentra consagrada en todo el sistema normativo al exigir que la producción del daño sea reprochable por culpa (artículo 1902) o negligencia (artículo 1.104).

6.3.3.2. La responsabilidad penal

Debido a su importancia, los derechos fundamentales gozan de protección por parte de la ley penal, además de las garantías ofrecidas por las normas de derecho internacional público o de derecho civil interno. Ciertos valores están protegidos por normas de naturaleza penal, debido a su importancia, el grado de peligro social y el impacto en la sociedad y los culpables por violación de estos valores serán responsables penalmente.

Entre los valores protegidos por la ley penal de los Estados encontramos la inviolabilidad del domicilio, la dignidad humana, la integridad física y moral, el honor y la imagen de una persona, el secreto de la correspondencia y la intimidad.

Por ejemplo, en Rumania, el Código penal rumano, en su artículo 226 prohíbe el hecho de publicar aspectos de la vida privada de las personas:
(1) La violación de la vida privada, sin derecho, como fotografiar, capturar o grabar imágenes, escuchar por medios técnicos o grabación audio de una persona en una vivienda o habitación o dependencia relacionada con ella o de una conversación privada será sancionada con pena de prisión de un mes a 6 meses o con multa.

(2) La divulgación, difusión, presentación o transmisión, sin derecho, de los sonidos, conversaciones o imágenes previstas en el párrafo. (1), a otra persona o al público, será castigada con pena privativa de libertad de 3 meses a 2 años o con multa.

En ciertos casos el código penal admite causas de eximen de la responsabilidad penal y la conducta que viola el derecho a la vida privada no se convierte en un delito. De esta forma la divulgación no genera la responsabilidad penal:

a) si fue cometido por la persona que participó en la reunión con el lesionado en la que se capturaron los sonidos, conversaciones o imágenes, si el autor justifica un interés legítimo;

b) si la persona lesionada actuó explícitamente con la intención de ser vista o escuchada por el autor;

c) si el autor descubre la comisión de un delito o contribuye a la prueba de la comisión de un delito;

d) si se captan hechos de interés público, que tienen trascendencia para la vida de la comunidad y cuya divulgación tiene mayores ventajas públicas que el daño causado a la persona lesionada.

En lo que concierne la inviolabilidad del domicilio, el Código penal rumano sanciona la violación de este derecho, pero vamos a presentar más detalles sobre este asunto en el capítulo VII.

Con referencia al derecho al honor de la persona, en Rumania ha pasado un fenómeno atípico. El Código penal antiguo (de 1968) sancionaba la insulta y la calumnia en los artículos 205 y 206: "*dañar el honor o la reputación de una persona por medio de palabras, gestos o cualquier otro medio, o por exposición a la vergüenza pública, o por atribuir a una persona un defecto, enfermedad o debilidad que, por real que sea, no debe ser revelada*", respectivamente "*afirmación o imputación en público, por cualquier medio, de un determinado hecho relativo a una persona que, que si fuera cierto, expondría a esa persona a una sanción penal, administrativa o disciplinaria, o al desacato público*".

En el año 2009, el Parlamento rumano decidió adoptar un nuevo código penal sin sancionar las conductas que constituyan insultas o calumnia para proteger el derecho absoluto a la libre expresión.

Pero, el Tribunal Constitucional rumano, por la Decisión no. 62/2007, consideró que las normas de modificación y complementación del Código Penal son

inconstitucionales y que la derogación del art. 205 y 206 y del Código Penal antiguo y la despenalización, de esta manera, de los delitos de injuria y calumnia, violan lo dispuesto en el art. 1 párr. (3) y el art. 21 de la Constitución rumana, en relación con algunos valores garantizados en el estado de derecho, el principio de libre acceso a la justicia, el derecho a un juicio justo y un recurso efectivo, tal como están regulados en el art. 6 y 13 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales. El Tribunal Constitucional destacó en su decisión que, al derogar los 2 textos de ley del Código Penal, se infringe el principio de igualdad de los derechos previsto en el art. 16 de la Constitución y se ignora lo dispuesto en el art. 30 párr. (6) de la Constitución rumana: "*La libertad de expresión no puede perjudicar la dignidad, el honor, la vida privada de la persona o el derecho a la propia imagen de uno mismo*".

Según el art. 147 párrafo 1 de la Constitución "Las disposiciones de las leyes vigentes, así como los de los reglamentos, declaradas inconstitucionales, dejarán de tener efecto legal a los 45 días de la publicación de la decisión del Tribunal Constitucional si, durante este período, el Parlamento o el Gobierno, según el caso, no concilian las disposiciones inconstitucionales con las disposiciones de la Constitución. Durante este período, las disposiciones declaradas inconstitucionales quedan suspendidas por ley".

Pero, tras la publicación de la decisión núm. 62/2007, el Parlamento no cumplió con su obligación. Como resultado, han surgido dos corrientes de opinión[544] en la doctrina jurídica y en la práctica judicial sobre los efectos de esta decisión:

1. las disposiciones del art. 205 y 206 del Código Penal antiguo continúan vigentes: esto se debe a que las decisiones del Tribunal constitucional son vinculantes y la despenalización no tiene efecto;

2. las disposiciones del art. 205 y 206 del Código Penal antiguo ya no se encuentran vigentes: no es posible sancionar penalmente la insulta y la calumnia a base de una decisión del Tribunal constitucional porque esto sería incompatible con el principio de legalidad de la incriminación consagrado en la Constitución.

En el marco legislativo español, los derechos fundamentales también gozan de protección a través de la ley penal (*Título X del Código penal - Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio*). La reforma

[544] Danileț, C. (2013) Insulta y calumnia siguen siendo infracciones. Revista Juridice.ro, Recuperado de https://www.juridice.ro/257671/insulta-si-calomnia-sunt-din-nou-infractiuni.html.

de 2015 ha modificado integral el artículo 197 (ahora 197 bis, ter, quater y quinquies). En este sentido, el legislador ha definido siete tipos de conductas delictivas en materia, que se desprenden del artículo 197, que vamos a presentar a continuación.

1. Descubrimiento de secretos o vulneración de la intimidad de otro (espionaje personal) - representa aquellos actos de una persona que accede sin autorización o consentimiento a los documentos, cartas, correos electrónicos, archivos u otros efectos personales de un individuo, con el fin de violar su privacidad o averiguar información personal secreta. Estamos ante este tipo de delitos también en los casos cuando las telecomunicaciones de una persona son interceptadas sin autorización legal o se utilizan técnicas para escuchar, transmitir, grabar o reproducir sonido, imagen, cualquier otra señal de comunicación o aplicación informática para acceder ilegalmente a la información personal de otra persona.

2. Apoderamiento, utilización o modificación de información reservada en perjuicio de un tercero - es una actividad delictiva que implica el acceso, copia, uso o modificación no autorizados de los datos personales de una persona, que se encuentran almacenados en archivos o computadoras, en medios electrónicos o en la nube, o en cualquier otro tipo de archivo o registro público o privado. El acceso implica la vulneración de los sistemas de seguridad o el uso de contraseñas correctas obtenidas mediante maniobras fraudulentas, en todo caso sin el consentimiento del titular de los datos o información.

3. Difusión, revelación publica o cesión a terceros de imágenes captadas, datos o hechos, posterior a su descubrimiento o apoderamiento de forma ilegítima y sin autorización expresa o implícita del titular. Este delito tiene una peculiaridad, el hecho de que incluso la persona que publica los datos personales es considerada culpable, aunque no actuó para obtenerlos, pero sabe que se accedió ilegalmente a ellos. La sanción por este delito es más severa cuando se publican datos personales que revelan elementos sensibles relacionados con la ideología, religión, fe, salud, origen racial o vida sexual del titular, o si la víctima es un menor de edad o una persona discapacitada. También se agrava cuando el delito es cometido por los responsables de la seguridad de los ficheros que contienen esos datos personales, sobre todo si tienen expresamente el mandato de hacerlo.

4. Difusión, cesión a terceros o revelación publica de imágenes o grabaciones que afectan gravemente la intimidad del interesado, aunque si fueron obtenidas con el acuerdo del afectado, pero sin la intención de hacerlas públicas. A menudo, las personas son filmadas o fotografiadas en momentos íntimos, con personas cercanas, para guardar recuerdos

personales y no tienen la intención de publicar estas grabaciones. Cuando estas imágenes llegan a la atención del público en general sin el consentimiento del propietario, nos encontramos ante una violación de la privacidad. La ley prevé un castigo más severo cuando el acto tiene como objetivo la obtención de beneficios materiales o cuando el delito es cometido por un cónyuge u otra persona con una relación personal similar, la víctima es menor de edad o discapacitada.

5. Intrusión, acceso y permanencia al conjunto o a una parte de un sistema de información, sin el acuerdo del titular, vulnerando los mecanismos de seguridad que lo protegen. Hay situaciones cuando los hackers consiguen infringir la seguridad de un sistema informático o de videovigilancia utilizando programas de malware y obtienen acceso a la base de datos o consiguen monitorear por un periodo de tiempo toda la información que entra y sale del sistema.

6. Intercepción no autorizada de transmisiones o de datos – consiste en actividades de intercepción ilegal, mediante la utilización de artificios o instrumentos técnicos, de transmisiones privadas de datos informáticos entre dos o más sistemas informáticos o incluso dentro de una red privada, incluidas las emisiones electromagnéticas de los mismos.

7. Uso de programas informáticos o contraseñas para fines ilícitos. Las acciones que ayudan a una persona a acceder ilegalmente a los secretos de otra persona se consideran un delito. Se considera cómplice del infractor a la persona que proporcione software, códigos o aplicaciones gratuitos o de pago que faciliten la obtención fraudulenta de contraseñas o el acceso ilegal a cuentas y archivos personales. La ley sanciona todas las actividades encaminadas a la producción, compra, importación o, de cualquier forma, el suministro de dichas herramientas por parte de terceros, con el fin de realizar actividades de espionaje o copia de datos personales.

En el capítulo VII se presentará en detalle algunos delitos relacionados con el derecho a la vida privado o con los derechos derivados.

6.3.3.3. La responsabilidad administrativa y contravencional

Esta forma de responsabilidad es específica, especialmente en el caso de la existencia de las autoridades para la protección los derechos fundamentales que tienen los instrumentos legales para la aplicación de sanciones como, por ejemplo, en el caso de los

operadores de datos personales que procesan datos sin el consentimiento informado de los titulares. Además, los funcionarios involucrados en la aplicación de la legislación específica en este asunto, en la medida en que no cumplan con las normas legales o las regulaciones internas con respecto a la política de protección de la vida privada, pueden ser sometidos a la responsabilidad administrativa, incluso con consecuencias patrimoniales.

Robert Alexy refiere que los derechos fundamentales deben ser reconocidos y protegidos en su conjunto, es decir un "*derecho fundamental como un todo*"[545]. Esta perspectiva transforma los derechos fundamentales en derechos multifuncionales, de "*manera que no es posible asociarlos a una función única: de cada derecho fundamental pueden ser extraídos múltiples deberes, decurrentes de incumbencias de distinta naturaleza, que ellos encomiendan al Estado. Por lógica consecuencia, un determinado derecho fundamental investirá su titular en diversas posiciones jurídicas de caracteres diferenciados, y con base en cada una de ellas el ciudadano podrá reclamar diferentes obligaciones del Poder Público*"[546].

Según Alexy, los derechos fundamentales cumplen dos tipos de funciones, una de defensa y otra de prestación, sin que existe una separación entre los derechos que tiene un tipo o el otro de estas funciones, sino que "*cada derecho fundamental posee, concomitantemente, esas diversas dimensiones, pudiéndose extraer deberes estatales correlatos a cada una de ellas*"[547].

En cuanto a la función de defensa de los derechos fundamentales, esta supone la prohibición de cualquier intervención no autorizada en el ámbito particular de su titular, sin distinguir entre el carácter público o privado de las medidas de intervención. Esta función impone una obligación negativa, la de no hacer, de abstenerse de actuar. Por ejemplo, la dimensión defensiva del derecho a la libertad de expresión impone al Estado o a las autoridades la obligación de no restringir o comprometer la expresión de las opiniones de su titular, cuando no exista una autorización expresa para ello, prevista en una ley constitucional.

---

[545] Alexy, R. (2007) *Teoría de los derechos fundamentales*. 2a ed., Centro de Estudios Políticos y Constitucionales, Madrid, pág. 214

[546] Wunder Hachem, D. (2014*). Derechos fundamentales económicos y sociales y la responsabilidad del estado por omisión*. Estudios constitucionales, 12(1), pp. 285-328, Recuperado de: https://dx.doi.org/10.4067/S0718-52002014000100007

[547] Alexy, R. (2017) idem., p. 216.

La función de protección deriva de la dimensión objetiva de los propios derechos fundamentales, que obliga al Estado a protegerlos frente a terceros. Entre los diversos derechos que pueden exigir protección fundamental, podemos mencionar: la salud, la vida, la dignidad y la libertad. El Estado puede ofrecer protección para estos derechos fundamentales mediante la emisión de normas de Derecho Penal, de Derecho Civil, de Derecho Procesal y de Derecho Administrativo[548].

Aunque en los dos principales sistemas de derecho analizados, el derecho a la vida privada comenzó siendo legalmente reconocido y protegido como uno de sus elementos (el derecho a la imagen), la evolución posterior difiere, por lo que su régimen legal se ha diversificado y enriquecido en el sistema de derecho continental, donde los instrumentos jurídicos adoptados a nivel regional o estatal, pero también los mecanismos de garantía específicos son más variados que los existentes en el sistema de *common law*. Identificar los elementos principales del régimen jurídico del derecho a la vida privada se describe en base a las regulaciones a nivel legislativo y las pautas dadas por la jurisprudencia de los tribunales de derecho común, constitucional o internacional. Por lo tanto, el valor agregado que se encuentra en el derecho europeo se debe a la complejidad de las garantías basadas en el derecho escrito, doblada por un control jurisdiccional de múltiples capas, perteneciente al orden jurídico nacional y supranacional, del Consejo de Europa (T.E.D.H.) y la U.E. (T.J.U.E.). Independientemente de la forma en que cierto sistema normativo tuvo éxito, el derecho a la vida privada ha ganado su valor indiscutible como un derecho fundamental.

A la luz de lo anterior, los mecanismos de control y garantía de los derechos humanos en general juegan un papel importante en la preservación de los derechos humanos. Pero debemos reconocer que aún son inadecuados en comparación con el estado actual de violaciones masivas y repetidas de los derechos humanos, es esta insuficiencia la que impide una efectividad real de estos mecanismos. Una reforma o adaptación de los mecanismos de la ONU para la protección de los derechos humanos parece útil y necesaria para garantizar de manera efectiva y efectiva los derechos fundamentales. Por lo que se refiere a los mecanismos regionales, la reforma se llevaría a cabo a la luz del sistema europeo de protección de los derechos humanos. De hecho, este último marcó un avance notable en el establecimiento de un órgano judicial cuyas sentencias tienen fuerza de cosa juzgada. El papel rector que pertenece al derecho europeo

[548] Alexy, R. (2007). idem. p. 404

se debe a la complejidad de las garantías basadas en el derecho escrito, doblada por un control jurisdiccional de múltiples capas, perteneciente al orden jurídico nacional y supranacional, del Consejo de Europa (T.E.D.H.) y la U.E. (T.J.U.E.).

Además, el mecanismo europeo ha experimentado una evolución sobre el principio de reciprocidad que ya no se tiene en cuenta en el ámbito de los derechos humanos. Estos ejemplos muestran que el sistema regional europeo tiene una contribución positiva a la protección de los derechos humanos, en la que el sistema universal debe inspirarse para asegurar la efectividad y efectividad de los derechos fundamentales.

Finalmente, a pesar de logros demostrados en el campo de la protección de los derechos humanos, los desafíos del siglo XXI son muchos y variados: la *justiciabilidad* de los derechos culturales, sociales y económicos, abolición universal de la pena de muerte, prohibición absoluta de la tortura, prohibición de determinadas manipulaciones genéticas, etc. Entre estos desafíos también se encuentran la adopción de medidas preventivas y la implementación de mecanismos efectivos de protección, la salvaguarda de los derechos humanos en situaciones de emergencia y el desarrollo de los medios de reparación de las víctimas de las violaciones.

El futuro de la protección de los derechos humanos depende actualmente en gran medida de las medidas de implementación nacional, entendiéndose que el derecho internacional y el derecho interno están en constante interacción en esta área. Las obligaciones convencionales de protección vinculan no solo a los gobiernos, sino también a todos los órganos estatales como tales (poderes y agentes). Los estándares internacionales de protección son directamente aplicables en el derecho interno, lo que beneficia a todos los seres humanos bajo la jurisdicción de sus respectivos estados. Este es el estándar de protección más efectivo (tanto a nivel internacional como nacional), ya que siempre prevalece sobre los demás. Una manifestación del surgimiento de normas imperativas de derecho internacional (jus cogens) y el desarrollo del régimen de obligaciones erga omnes promovería considerablemente el establecimiento de un sistema eficaz de vigilancia permanente de la situación de los derechos humanos en el mundo.

CAPÍTULO VII. El derecho a la vida privada

La privacidad es un concepto amplio, que abarca (entre otras cosas) desde la libertad de pensamiento, el control sobre su propio cuerpo, la intimidad en el hogar, el control de la información sobre uno mismo, el rechazo de la vigilancia, la protección de la reputación y la protección contra registros e interrogatorios sin orden judicial. Una y otra vez los filósofos, los teóricos del derecho y los juristas han reconocido la gran dificultad de alcanzar una concepción satisfactoria de la privacidad. Arthur Miller ha declarado que la privacidad es "difícil de definir porque es exageradamente vaga y evanescente"[549]. Según Julie Inness[550], el discurso legal y filosófico de la privacidad se encuentra en un estado de "caos".

William Beaney[551] menciona que "incluso el defensor más enérgico del derecho a la privacidad debe confesar que es problemático definir la esencia y el alcance de este derecho". Según Robert Post, "*la privacidad es un valor tan complejo, tan enredado en dimensiones competitivas y contradictorias, tan lleno de significados diversos y distintos, que a veces me desespero al intentar abordarlo de manera útil*"[552].

Varios teóricos han examinado los intereses que la ley protege bajo la rúbrica de privacidad y han concluido que son distintos y no están relacionados. La privacidad tiene "una capacidad proteica de ser todo para todos los abogados", ha observado Tom Gerety[553]. Judith Thompson[554] incluso ha argumentado que la privacidad como concepto no tiene una función útil, ya que lo que llamamos privacidad realmente equivale a un conjunto de otros intereses más primarios.

Según el método tradicional de conceptualización, una concepción es una categoría, una imagen mental abstracta, lo que hace que la privacidad sea distinta de otras cosas, que según los criterios caen en otras categorías. Las personas pueden usar la palabra "privacidad" de manera incorrecta al referirse a cosas fuera de la categoría o al

---

[549] Miller, A. R. (1971) *The Assault on Privacy: Computers, Data Banks, and Dossiers*; University of Michigan Press; First Edition, p. 25;
[550] Inness, J. C. (1992) *Privacy, Intimacy, and Isolation*; Oxford University Press.
[551] Beaney, W. M. (1966) *The Right to Privacy and American Law*, Revista Law and Contemporary Problems 253-271 p. 255
[552] Post, R. C. (2001) *Three Concepts of Privacy*, the Georgetown Law Journal, vol 89/2087, p. 2087.
[553] Gerety, T. (1977) Redefining Privacy, Harvard Civil Rights-Civil Liberties Law Review, Vol. 12, pp. 233-296
[554] Thomson, J. J. (1975) *The Right to Privacy*, Philosophy & Public Affairs, Vol. 4, No. 4 (Summer, 1975), pp. 295-314

no referirse a cosas dentro de la categoría. El propósito de conceptualizar es definir las características únicas de la privacidad. El uso de la palabra "privacidad" debe clarificarse para que coincida con la categoría conceptual de privacidad. Dadas las grandes dificultades de capturar todo lo que se emplea como "privacidad", las formas a menudo dispares de usar la palabra "privacidad" y la falta de acuerdo sobre el significado preciso de la palabra, ha determinado a muchos académicos buscar establecer criterios claros para distinguir "privacidad" de otras cosas. Se pueden omitir algunas cosas, pero el objetivo es establecer una concepción que abarque la mayoría de las cosas que comúnmente se ven bajo la rúbrica de "privacidad"[555].

En el año de 1890, Samuel Warren y Louis Brandeis escribieron su famoso artículo "El derecho a la privacidad"[556], aclamado por una multitud de académicos como la base de la ley de privacidad en los Estados Unidos. La influencia del artículo de Warren y Brandeis no puede ser cuestionada: el artículo inspiró un interés significativo y atención a la privacidad; generó al menos cuatro acciones de agravio del derecho consuetudinario para proteger la privacidad; y enmarcó la discusión sobre la privacidad en los Estados Unidos a lo largo del siglo veinte.

Warren y Brandeis comenzaron destacando nuevos desarrollos tecnológicos que representaban una amenaza potencial para la privacidad y se centraron en cómo podría desarrollarse el sistema de derecho "common law" para proteger el interés del ser humano, llamado "privacidad".

Los autores, sin embargo, no pasaron mucho tiempo exponiendo un concepto inédito de la privacidad. Warren y Brandeis definieron la privacidad como el "derecho a ser dejado en paz- the right to be let alone", una frase adoptada del famoso tratado del juez Thomas Cooley en 1880[557]. El derecho de Cooley a "ser dejado en paz" era, de hecho, una forma de explicar que el intento de tocar físicamente era un daño extracontractual y no estaba definido como un derecho a la privacidad. El uso de Warren y Brandeis de la frase fue coherente con el propósito de su artículo: demostrar que muchos de los elementos del derecho a la privacidad existían dentro del derecho consuetudinario (common law).

---

[555] Solove, D. J. (2002) *Conceptualizing Privacy*, California Law Review, Vol. 90, p. 1096

[556] Warren, S. D. y Brandeis, L. D. (1890) *The right to privacy*, Harvard Law Review, Vol. 1, No. 1 - Vol. 130, No. 2, disponible en: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

[557] Cooley, TH. M. (1880) *A Treatise on the Law of Torts or the Wrongs Which Arise Independently of Contract*, Callaghan Chicago.

Los autores declararon que el principio subyacente de la privacidad era "el de la personalidad inviolable". Mencionaron que el valor de la privacidad "no se encuentra en el derecho a tomar las ganancias derivadas de la publicación, sino en la tranquilidad o el alivio que ofrece la capacidad de evitar cualquier publicación". Warren y Brandeis observaron que, cada vez más, "*la empresa moderna y la invención, a través de las invasiones a su privacidad, han sometido [a un individuo] a dolor y angustia mental, mucho más de lo que podría causar una simple lesión corporal*".

Los autores señalaron que este tipo de daño generalmente no estaba protegido por la ley de responsabilidad civil. Si bien la ley de difamación protegía las lesiones a la reputación, la privacidad implicaba "lesiones a los sentimientos", una forma psicológica de dolor que era difícil de traducir en la ley de responsabilidad civil de su época, que se centraba más en las lesiones tangibles.

La formulación de la privacidad como el derecho a ser dejado en paz describe solo un atributo de la privacidad. Entender la privacidad como algo que no se puede hacer (no disturbar, no tacar) no proporciona mucha orientación sobre cómo se debe valorar la privacidad frente a otros intereses, como la libertad de expresión, la aplicación efectiva de la ley y otros valores importantes. Ser dejado en paz no nos informa sobre los asuntos en los que exactamente debemos ser dejados en paz. Warren y Brandeis hablaron de "personalidad inviolada", que podría considerarse como una descripción del contenido de la esfera privada, pero esta frase es vaga, y los autores no elaboraron el tema. En la medida en que el hecho de ser dejado en paz se refiere a la "ninguna interferencia del estado", el jurista Ruth Gavison[558], considera que "*reclamar el derecho a la privacidad típico no significa rechazar la interferencia del estado en absoluto. Significa reclamar por una interferencia estatal en forma de protección legal contra otras personas que puedan violar el derecho de ser dejado en paz*".

El derecho a ser dejado en paz presenta la privacidad como un tipo de inmunidad o aislamiento. Como muchos comentaristas lamentan, definir la privacidad como el derecho a ser dejado en paz es demasiado amplio. Por ejemplo, la autora Anita Allen explica: "Si la privacidad simplemente significa «estar solo», cualquier forma de conducta ofensiva o perjudicial dirigida hacia otra persona podría caracterizarse como

[558] Gavison, R. E. (1980) *Privacy and the Limits of Law*, The Yale Law Journal, Vol. 89, No. 3, pp. 421-471

una violación de la privacidad personal. Un puñetazo en la nariz sería una invasión de la privacidad tanto como una miradita en el dormitorio"[559].

Según el filósofo Ferdinand Schoeman, Warren y Brandeis "nunca definen qué es la privacidad"[560]. Edward Bloustein, un conocido teórico legal de la privacidad observó que el artículo de Warren y Brandeis se centró en las lagunas existentes en los conflictos de derecho consuetudinario y no intentó desarrollar una concepción de la privacidad.

Aunque fue criticado por algunos teóricos, el artículo de Warren y Brandeis estaba muy adelantado en aquella época y contenía destellos de información sobre una teoría más sólida de la privacidad. Consideramos que el objetivo de los autores no era proporcionar una concepción integral de la privacidad, sino explorar las raíces del derecho a la privacidad dentro del sistema de derecho consuetudinario para poder explicar cómo podría desarrollarse el dicho derecho. El artículo fue, sin duda, un comienzo profundo para desarrollar una concepción de la privacidad. Sin embargo, si bien el derecho a ser dejado en paz ha sido invocado por jueces y comentaristas a menudo, sigue siendo una concepción bastante amplia y vaga de la privacidad.

Seguidamente, se analizará el contenido y la naturaleza jurídica del derecho a la privacidad, destacando las obligaciones correlativas a cargo del Estado y de los otros sujetos de derecho de abstenerse de conductas que puedan perjudicar la esfera privada del individuo.

Por ende, este capítulo investigará el contenido de los derechos y obligaciones específicos del derecho a la vida privada, después de examinar por primera vez las características que determinan la naturaleza jurídica de este derecho dentro de los diversos sistemas jurídicos, y luego analizar particularmente la forma en que adquirió el valor reconocido por un derecho fundamental. Debido a que el derecho a la vida privada no es un derecho absoluto, identificaremos los principales límites que pueden ser admitidos en su ejercicio, y al final, se esbozarán los tipos de mecanismos para la protección legal de este derecho.

El desarrollo tecnológico de la segunda mitad del siglo XX ha permitido el uso creciente de computadoras electrónicas en la actividad actual de las instituciones

[559] Allen, A. L (1988) *Uneasy Access: Privacy for Women in a Free Society*, Editorial Rowman & Littlefield, p. 6.
[560] Schoeman, F (1984) *Privacy: Philosophical Dimensions of the Literature, An Anthology*, Editorial Cambridge University Press, p. 14.

públicas, empresas privadas y, posteriormente, de cualquier individuo. Como efecto directo de este progreso, la información se ha procesado en gran cantidad y en poco tiempo, a través de aplicaciones informáticas dedicadas al establecimiento y gestión de bases de datos, haciendo así la transición de guardar, por ejemplo, registros o grabar exclusivamente en medios físicos (papel), en su administración electrónica, mucho más fácil y menos costoso.

La posesión y comunicación de datos personales, que directamente identifica o permite la identificación de una persona física, incluida en archivos computarizados, es, según los autores de la literatura especializada dedicada a los derechos humanos, un aspecto "moderno" de la vida privada personal (en el sentido dado por esta noción a través de Jurisprudencia del T.E.D.H., a la que nos referimos en las secciones anteriores.)

Por lo tanto, el hecho legal que determinó el surgimiento de este "aspecto moderno" de la privacidad personal fue determinado inicialmente por la evolución tecnológica especial de la segunda mitad del siglo XX. ley, que permitía el uso de métodos de procesamiento de información sobre el individuo, en particular, por parte de las autoridades. Los riesgos representados por cometer errores o abusos en esta actividad, que pueden dañar los intereses personales de los involucrados, llevaron a la adopción de las primeras regulaciones destinadas a establecer garantías de protección legal del derecho a la vida privada en el contexto informativo (la primera la ley fue adoptada en la tierra alemana de Hesse en 1970).

La expansión de las tecnologías de procesamiento e intercambio de información, perpetuamente sujetas a innovación, a nivel mundial, ha introducido otra dimensión para la protección legal de la nueva ley que ya se había esbozado a nivel nacional: la inclusión de reglas específicas en instrumentos internacionales (o regionales), dirigidas a para proporcionar una mayor protección del derecho a la privacidad en el contexto del procesamiento (procesamiento) de datos por medios automatizados y circulación de datos transfronteriza.

La primera iniciativa de este tipo pertenece a la Organización para la Cooperación y el Desarrollo Económico, que adoptó en 1980 la "Recomendación del Consejo sobre las Directrices que rigen la protección de la privacidad y la transferencia de datos personales al extranjero", seguida en breve por el Consejo de Europa con su Convenio sobre Protección de Datos personal desde 1981. Siendo plenamente consciente de los desafíos impuestos por las evoluciones en la sociedad contemporánea, basados en

los métodos de comunicación informativa, el T.E.D.H. ha desarrollado en las últimas décadas una práctica importante relacionada con el respeto del derecho a la privacidad, desde la perspectiva del procesamiento de la información personal, que también debe ser tomado en cuenta por las autoridades estatales, incluso al invocar el cumplimiento de algunas atribuciones legales, a partir de su jurisprudencia, en particular en el caso de Rotaru v. Rumania, se puede deducir que la retención de datos personales por parte de una autoridad lo público puede constituir una interferencia ilegítima en la vida privada, en una sociedad democrática, si no se rige por reglas que garanticen los derechos del individuo contra la arbitrariedad del poder del estado.

Sin embargo, la verdadera "revolución" en este asunto fue provocada por la política de las instituciones de la Unión dedicadas después del Tratado de Maastricht, que afirma cada vez más los derechos fundamentales en la UE y que regularon mediante un acto vinculante la protección del derecho a la privacidad en relación con el procesamiento y el movimiento entre estados de datos personales – el RGPD. Por otro lado, el derecho a la protección de datos personales probablemente no habría alcanzado su dimensión actual, la autonomía del derecho a la privacidad, si su estado hubiera permanecido estrictamente localizado a nivel de los sistemas legales nacionales con la expansión de los efectos de la globalización, por lo que las primeras leyes apuntaban a la protección de datos personales de Alemania y Francia, que han permanecido sin cambios durante varias décadas, han sufrido cambios importantes en particular, después de la adopción del RGPD.

El fenómeno de la globalización en las últimas décadas se ha percibido en varias formas, y se asocia con conceptos como "desterritorialización", lo que implica el desarrollo variado de las actividades sociales, independientemente del área geográfica de donde provienen los participantes, de modo que los eventos globales pueden ocurrir / reproducirse casi simultáneamente, a través de las telecomunicaciones, las computadoras digitales, los medios audiovisuales y otras facetas de este fenómeno implican el aumento del nivel de interconexión social rápida más allá de las fronteras geográficas o políticas, lo que permite intercambios intensos de personas, servicios, información, capital o bienes, así como su desarrollo en forma de un proceso a largo plazo, continuamente dinámico y en evolución, con una influencia que se manifiesta en varios niveles: económico, político, cultural, legal.

La globalización se considera una característica constitutiva de la vida moderna, en el que el uso de las tecnologías más nuevas y de mayor rendimiento desempeñan un papel central. El proceso de globalización, sus componentes y el efecto sobre las actividades sociales no está sujeto a investigación solo para sociólogos. Por ende, la aparición y el desarrollo de organizaciones internacionales también se consideran un aspecto de la globalización política y legal, y se dan como ejemplos la Unión Europea o la Asociación de Libre Comercio de América del Norte.

A nivel de estas organizaciones, desde el punto de vista normativo, existe una cierta tendencia excesiva a la regulación supraestatal, en la cual los Estados-nación cooperan para adoptar reglas que transgredan su jurisdicción territorial. En vista del impacto de estas organizaciones, se apoya la idea de la necesidad de expandir las instituciones democráticas liberales a nivel transnacional, bajo el aspecto de respetar las reglas específicas del estado de derecho y la elección democrática de los representantes de los estados. Con respecto a la Unión Europea, existen opiniones doctrinales que es necesario consolidar la democracia dentro de esta organización, con respecto a la elección de organismos representativos y la garantía efectiva de los derechos civiles, políticos, sociales y económicos de todos los europeos.

Por lo cual, tanto el fenómeno mismo de la globalización como sus efectos están profundamente influenciados por el desarrollo rápido y continuo de técnicas de comunicación que permiten superar las fronteras terrestres y abolir las barreras en la transmisión de información. El surgimiento de Internet también fue un momento esencial para profundizar estos procesos; pero sus efectos beneficiosos a menudo parecen superados por los altos riesgos involucrados, por un lado, la presunta falta de seguridad en la transmisión de información a través de redes, las técnicas de intercepción también hacen progresos considerables y, por otro lado, la pretendida preservación del anonimato de los usuarios de Internet, como garantía de la libertad de expresión, con todos sus países implícitos (exponer o incluso mostrar ciertos aspectos de la vida personal en Internet puede ser una fuente real de información para los usuarios que, bajo la protección del anonimato, cometen actos delictivos de como phishing, robo de identidad, falsificación de medios de pago, la pedofilia en Internet, etc.).

Por lo tanto, cuando se discute la posibilidad o necesidad de regular Internet ("gobernanza de Internet"), las opiniones son igualmente divergentes, divididas entre los defensores y los detractores de la absoluta libertad de expresión en Internet. El Grupo de

Trabajo Art. 29 emitió a su vez o una serie de documentos y recomendaciones sobre el tema de Internet. En consecuencia, es necesario aplicar el principio de proporcionalidad entre el interés legítimo de los usuarios de Internet a permanecer en el anonimato, como garantía de que "huellas" dejadas por ellos no son monitoreados y capaz conducir a la realización de un perfil completo o al uso con fines ilegítimos y el interés de los gobiernos o de algunas organizaciones para detectar a las personas que violan las disposiciones legales imperativas o los derechos de propiedad intelectual, por el contenido fraudulento de la información difundida en Internet.

Partiendo de la afirmación de que *"Internet no es un gueto anárquico donde las reglas de la sociedad ya no se aplican"*, el Grupo de Trabajo del Art. 29, sin embargo, subraya la importancia de aplicar las mismas reglas de conducta que permiten la protección del derecho a la privacidad y la protección de datos personales en el entorno en línea, de manera similar al entorno fuera de línea, y cualquier restricción que pueda imponerse a estos derechos deberá cumplir con los requisitos de la necesidad y la proporcionalidad de una interferencia, de acuerdo con la práctica del T.E.D.H.. En nuestra opinión, es aún más imperativo encontrar un equilibrio necesario entre los intereses de todas las partes involucradas en el uso de Internet, no solo desde la perspectiva de las restricciones que podría imponer el estado, sobre consideraciones relacionadas con el orden público o la seguridad nacional, sino también desde el punto de vista de cualquier persona física cuyos datos personales puedan ser publicado y difundido en Internet en modo incontrolado o incluso fraudulento por los usuarios de Internet;

En tales situaciones, es necesario equilibrar el derecho a la protección de los datos personales del usuario anónimo de Internet y el derecho a la protección de los datos personales de la "víctima" del usuario de Internet. Estos casos son cada vez más comunes debido a la difusión del interés en acceder redes sociales disponibles en Internet, a través de las cuales los datos personales (datos de identificación, preferencias, imágenes, etc.) se ponen a disposición del público, a veces incluso con el consentimiento explícito, pero no informados sobre los riesgos involucrados, de sus propietarios.

Las regulaciones adoptadas por los estados europeos y las instituciones de la UE con respecto a la protección de datos personales han tenido un impacto especial en las relaciones económicas con los otros terceros países o con otras organizaciones internacionales. Como resultado de la globalización en esta área donde la información personal fluye inherentemente entre estados (por ejemplo, dentro de compañías dentro de

una compañía multinacional), para cumplir con las restricciones impuestas por la ley europea, otros estados también han adoptado regulaciones. diseñado para garantizar la protección de datos personales. Además, la transferencia de datos personales desde el territorio de la UE a un tercer país que no proporcionaría un nivel adecuado de protección de datos personales está, en principio, prohibida. Las experiencias recientes en las relaciones relativamente tensas entre la UE y los EE. UU. en el caso de la transferencia de datos de los pasajeros de las aerolíneas que realizan vuelos a este estado o del acceso por parte de las autoridades estadounidenses de los datos financieros y bancarios de los ciudadanos europeos, almacenados por SWIFT en el territorio estadounidense, han sido razones importantes que EE. UU. adopte una serie de leyes con respecto a este sector, y las revelaciones hechas por Edward Snowden en 2013 parecen acelerar este proceso.

Si el fenómeno de la globalización ha influido significativamente en la aparición de regulaciones con respecto a la protección de datos personales, también se observa el mismo fenómeno con respecto a la internacionalización de estas regulaciones y la influencia interestatal en su adopción. Por lo tanto, en el "diálogo transatlántico" entre la UE y los EE. UU., excluyendo las especies mencionadas anteriormente, hay un proceso con dos implicaciones dobles: por un lado, EE. UU., Aunque bastante tímido, ha iniciado una serie de leyes destinadas a defender la privacidad. y datos personales en el procesamiento automático, y por otro lado, los legisladores de la UE también han adoptado regulaciones que involucran el procesamiento de datos personales importantes y sensibles a través de la naturaleza de los datos y el propósito de su uso, con el pretexto de correlacionarse con las regulaciones de los EE. UU., en particular, en el campo de la seguridad, como pasaportes y libros electrónicos que contienen datos biométricos, retención de tráfico y datos de ubicación durante largos períodos ("retención de datos"), recopilación de conjuntos de datos personales pertenecientes a pasajeros de compañías aéreas de la UE para fines relacionado con la prevención y sanción de actos terroristas.

Todas estas regulaciones han requerido a su vez la adopción de reglas especiales destinadas a la protección de datos personales. En este contexto, está totalmente justificado la necesidad de adoptar un instrumento legal internacional que integre las reglas y principios de protección de la privacidad y los datos personales, a los que se adhiere la mayoría de los estados del mundo, a fin de eliminar las diferencias de estándares en la garantía efectiva de estos derechos, acoge con satisfacción desde este

punto de vista la iniciativa de las autoridades de protección de datos personales desde 2009 , hasta la presente, que se mantiene en la etapa de proyecto.

Por lo tanto, gracias al progreso tecnológico que ha influido en los sistemas de comunicación tradicionales entre organizaciones y / o entre personas, mediante métodos para eliminar las barreras espaciales y temporales a nivel global, se ha revelado que era natural, pero también necesario, adoptar reglas específicas que garantiza la protección de la información así transmitida y que puede afectar la privacidad de las personas, como resultado de los riesgos involucrados en el uso de estas nuevas tecnologías.

Al entrar en la era de la información, el derecho a la privacidad ganó nuevas connotaciones, lo que se traduce en la génesis de un nuevo derecho, el derecho a la protección de datos personales, que trataremos en la segunda parte de este documento. Como las evoluciones en la esfera tecnológica representan un proceso dinámico continuo, se espera que estos dos derechos también experimenten transformaciones y adaptaciones contextuales, que solo pueden percibirse parcialmente en este momento. Como hemos visto anteriormente, se pueden detectar varias generaciones de regulaciones aplicables en este campo: las de nivel nacional, en la fase incipiente (nacional), en algunos estados europeos, las de nivel regional, en la fase intermedia (regional) de la adopción de convenios o actos sindicales, influenciados por los primeros, que a su vez determinaron la adopción o modificación de las regulaciones nacionales en los Estados miembros de las respectivas organizaciones regionales en la fase avanzada (supranacional), porque en la actualidad, bajo el efecto de la globalización, el derecho a la vida privado y el de protección de datos personales para beneficiarse de una protección extendida también a nivel de otros estados, en la fase actual (transnacional), con la perspectiva de uniformizar su régimen legal a nivel de organizaciones internacionales en una fase futura (internacional).

El derecho a la privacidad, aunque es un derecho relativamente reciente (de la cuarta generación de derechos fundamentales), como reacción a la exposición pública de la vida del individuo debido a las modernas técnicas de información y comunicación, ha experimentado una evolución impresionante, con una dinámica perpetua, en nivel legislativo y jurisprudencial, tanto dentro de los sistemas legales nacionales como supranacionales, que actualmente se benefician de un régimen legal totalmente impugnado, que denota la importancia de los valores sociales que protegen y en los que se basan: dignidad humana, libertad individual, el libre desarrollo de su personalidad.

Independientemente de la forma en que ha obtenido reconocimiento, tanto en los sistemas de derecho, continental y común, el derecho a la vida privada, que tiene el estatus de derecho constitucional, contribuye al cumplimiento de otros derechos fundamentales con los que está relacionado y, por otro lado, al ser un derecho relativo, puede estar sujeto a restricciones determinadas por la defensa de otros derechos con preeminencia dentro de ciertas relaciones jurídicas concretas, o por la necesidad de proteger valores sociales importantes como el orden público o la seguridad nacional.

La realización efectiva de su contenido complejo, incluso bajo el aspecto de verificar la legitimidad de las limitaciones permitidas y de asumir la responsabilidad por la violación de este derecho, se controla mediante los más altos mecanismos administrativos y judiciales, lo que, una vez más, subraya el carácter fundamental de El derecho a la privacidad, de acuerdo con las características identificadas en el primer capítulo de este trabajo. En la segunda parte, analizamos si el derecho a la protección de datos personales, formado sobre la base del derecho a la privacidad en el contexto del procesamiento de datos personales, mantiene las mismas características del régimen legal.

7.1. La naturaleza jurídica del derecho a la vida privada

Debido a su importancia, los derechos fundamentales se incluyen en las declaraciones de derechos o en las Constituciones, lo que denota su fuerza jurídica suprema. La definición de los derechos fundamentales enunciada en el capítulo anterior abarca los rasgos de los derechos subjetivos que protegen los valores esenciales cuyo carácter supremo es reconocido por las normas jurídicas de fuerza superior dentro de un sistema normativo o en el fundamento de la jurisprudencia de los tribunales de contencioso constitucional o internacional y que están garantizados por la Constitución, por leyes y por el control ejercido por dichos tribunales.

A partir de estos elementos definitorios, analizaremos en lo que sigue cómo se ha reflejado el derecho a la vida privada en los instrumentos jurídicos nacionales e internacionales, con el fin de demostrar el carácter fundamental de este derecho en el orden jurídico interno e internacional de los Estados. ¿Por qué es importante demonstrar el carácter fundamental de este derecho? Para poder analizar hasta qué punto podemos interferir en su esfera, limitando su ejercicio o el ejercicio de otros derechos componentes.

También para comprender como podemos ejercer este derecho en el mundo digital, protegiéndolo de la curiosidad manifestada por los demás internautas o por las autoridades. Son muchos los motivos que determinan la necesidad de disecar el concepto de "la vida privada" el esfuerzo será recompensado por las conclusiones que vamos a conseguir.

Como hemos visto, el reconocimiento jurídico del derecho a la vida privada no coincide con el momento histórico de su ocurrencia, difícil de ser determinado con certeza, desde un punto de vista temporal o geográfico. Algunos de los componentes del complejo contenido del derecho a la vida privada, de conformidad con lo establecido en el artículo 8 del Convenio Europeo de Derechos Humanos (el derecho a un hogar, el derecho a la vida privada y familiar y el secreto de la correspondencia), fueron reconocidos como derechos fundamentales en las constituciones de los Estados relativamente temprano.

Pero el uso de la frase "el derecho a la vida privada" por los poderes constituyentes ha ocurrido en la época reciente, de las grandes transformaciones de la conciencia individual, marcadas por un lado de la implementación de los mecanismos de la defensa de los derechos humanos internacionales y, por otra parte, por la influencia ejercida en las regulaciones por las nuevas técnicas con potencial intrusivo en la privacidad del individuo.

Por lo tanto, se puede afirmar que el nacimiento "jurídico" del derecho fundamental a la vida privada es diferente de un Estado a otro, algunos actuando al respecto como resultado de la evolución del derecho internacional de los derechos humanos, y otros, por el contrario, poseyendo "derechos de autor" a través de sus constituciones o práctica judicial interna, que posteriormente influyeron en las regulaciones internacionales también. Lo interesante es analizar cómo la legislación de la Unión Europea, organización internacional con objetivos inicialmente predominantemente económicos, ha logrado imponer un complejo catálogo de derechos fundamentales a los Estados miembros, incluso el derecho a la vida privada, concomitantemente con la entrada en vigor del Tratado de Lisboa (implícitamente, la Carta de los Derechos Fundamentales de la Unión Europea), cuestiones que también se tratarán más adelante.

El derecho a la vida privada puede ser incluido en la categoría de los derechos de cuarta generación, aunque, si aceptamos la clasificación de los derechos en

generaciones definidas cronológicamente, tal derecho, visto desde una perspectiva histórica, podría incluirse también en la primera generación[561], siendo un derecho indisoluble ligado al ser humano, pero que, de hecho, no ha adquirido protección jurídica antes del siglo XX.

Además, la doctrina del derecho constitucional sitúa el derecho a la vida privada en la categoría de inviolabilidades, como un aspecto de respeto a la personalidad humana, y también se considera un derecho humano, en su aspecto del derecho a la privacidad o el respeto por la vida personal. Por ejemplo, un derecho que se puede incluir claramente en la cuarta generación es el derecho a la protección de datos personales, como derecho correlativo, desprendido del derecho a la vida privada, en su aspecto de protección de las informaciones que caracterizan al individuo ("privacidad informativa"), debido a su reciente consagración legal, relacionada con las realidades de la sociedad contemporánea dominada por el uso generalizado de las tecnologías de la información y las comunicaciones electrónicas.

Si nos referimos estrictamente a los principios derivados de la jurisprudencia del Tribunal Europeo de Derechos Humanos, se puede observar que el derecho a la vida privada es un derecho complejo, en constante cambio y evolución que, a su vez, influye los legisladores constitucionales u ordinarios de los Estados miembros del Consejo de Europa. Tal observación puede justificar la conclusión de que el derecho a la vida privada no es un derecho que pueda enmarcarse fácil y rigurosamente en una categoría u otra, en una generación u otra.

No obstante, para nuestro enfoque científico actual, consentimos la tesis de que el derecho a la vida privada - stricto sensu - es un derecho civil inviolable, surgido con el ser humano y destinado a defender a través de su contenido todo el complejo de valores reconocidos a la personalidad humana y que, dado el momento de su valor legal, forma parte de la cuarta generación de derechos.

En cuanto al atribuirle el carácter del derecho fundamental, la clarificación de este estatuto es posible (y) utilizando la "prueba" consagrada en la jurisprudencia del Tribunal Supremo de los Estados Unidos: "Si un derecho no puede ser negado sin violar los principios fundamentales de libertad y de la justicia que sustentan todas las

[561] Esta clasificación está realizada por J. F. Renucci, que sitúa el derecho a la vida privada y familiar en la categoría de derechos civiles y políticos: Renucci, J. F. (2009) *Tratado de derecho europeo de derechos humanos*, Hamangiu Publishing House, Bucarest, p. 169

instituciones civiles y políticas, entonces ese es un derecho fundamental"[562]. Sobre la base de esta prueba, observamos que, en todos los principales ordenamientos jurídicos, el derecho a la vida privada, en su conjunto o en particular, a través de sus elementos constitutivos, ha adquirido el reconocimiento de su naturaleza fundamental.

7.2. El carácter del derecho fundamental a la vida privada en los sistemas nacionales de derecho

7.2.1. El sistema de derecho anglosajón

La caracterización del derecho a la vida privada como derecho fundamental se llevó a cabo por diferentes caminos en el sistema "common-law", en comparación con el sistema legal romano-germánico, de manera específica a los medios tradicionales de estos sistemas de derecho.

En los Estados Unidos, la existencia del derecho fundamental a la vida privada[563] ha sido reconocida en la jurisprudencia, un derecho que actualmente se beneficia de un estatus privilegiado en la jerarquía de los derechos regulados en el sistema legal estadounidense. Así, en la sentencia dictada por el Tribunal Supremo en el asunto Griswold c. Connecticut[564], se consideró que el derecho a la vida privada es un derecho personal fundamental, aunque no esté expresamente previsto por la Constitución, sino que respeta los principios enunciados en la Novena enmienda[565] de la Constitución de los Estados Unidos, según la cual el catálogo de derechos consagrados en la Constitución no es exhaustivo, al que se pueden añadir otros derechos consagrados por la voluntad del pueblo.

---

[562] Dictamen expresado en el caso Powell v. Alabama, 287 U.S. 45, 67: "The fact that the right involved is of such a character that it cannot be denied without violating those fundamental principles of liberty and justice which lie at the base of all our civil and political institutions, is obviously one of those compelling considerations which must prevail in determining whether it is embraced within the due process clause of the Fourteenth Amendment, although it be specifically dealt with in another part of the Federal Constitution. Evidently this court, in the later cases enumerated, regarded the rights there under consideration as of this fundamental character". Texto disponible en: https://caselaw.findlaw.com/us-supreme-court/287/45.html

[563] Turkington, R. C. y Allen, A. L. (2002) *Privacy Law: Cases and Materials (American Casebook Series) 2nd Edition,* Editorial *West Group,* p. 61-66

[564] United States Supreme Court, Griswold v. Connecticut (1965) No. 496, 381 U.S. 479, disponible en: https://caselaw.findlaw.com/us-supreme-court/381/479.html

[565] "La enumeración en la Constitución, de ciertos derechos, no debe entenderse que niega o menosprecia otros que retiene el pueblo." - Constitucion de los Estados Unidos de America 1787, diponible en: https://www.constitutionfacts.com/content/constitution/files/USConstitution_Spanish.pdf

En la opinión de los jueces que dictaron esta sentencia, el derecho a la vida privada es, más antiguo que *Bill of Rights* (aunque no estaba regulado expressis verbis), y "*el objetivo de las autoridades de controlar o impedir las actividades que, según la Constitución, están sujetas a regulaciones de nivel estatal, no se puede lograr invadiendo la esfera de las libertades protegidas*".

También, de modo pretoriano fue reconocido en los EE.UU. el derecho a la protección de datos personales (privacidad informativa) en la causa Whalen v. Roe[566], donde el Tribunal Supremo de Justicia de los Estados Unidos se pronunció sobre la legalidad de las actividades de recolección, almacenamiento y diseminación de datos extraídos de las bases de datos públicos. Se observa que, en el derecho estadounidense, el uso de la noción de "privacy" implica ambos significados, nombrando tanto el derecho a la vida privada, como el derecho a la protección de datos personales, la distinción se está realizando caso por caso, dependiendo del contexto, mediante la asociación del criterio determinante, "informational privacy" (por lo tanto, la privacidad es el género próximo, y la privacidad informativa es la diferencia específica).

La doctrina estadounidense aprecia que, antes de esta consagración pretoriana expresa, los orígenes del derecho a la vida privada se encontraban en las fuentes constitucionales escritas – las enmiendas de la Constitución de los Estados Unidos.

Así, la Primera Enmienda consagra la libertad de la religión, de la expresión, la libertad de la prensa y de asociación; La Tercera Enmienda - el derecho a no tener tropas militares en el domicilio de nadie; La Cuarta Enmienda - el derecho a no ser sometido inmotivado a los registros y a los embargos; La Quinta Enmienda - el derecho a no a declarar contra sí mismo en ningún juicio criminal. Todos estos derechos se consideran normas constitucionales y formas de vida privada legalmente protegidas[567].

Los derechos basados en la Constitución Federal y sus enmiendas determinan el contenido del derecho fundamental a la vida privada, siendo de gran importancia su dimensión espacial, en particular (La Cuarta Enmienda[568]), y la dimensión relacional o

---

[566] United States Supreme Court, WHALEN v. ROE (1977), No. 75-839, 429 U.S. 598, disponible en: https://caselaw.findlaw.com/us-supreme-court/429/589.html

[567] R. C. Turkington, A. L. Allen (2002) *Privacy Law: Cases and Materials (American Casebook Series) 2nd Edition,* Editorial *West Group,* p. 22.

[568] *"El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas".*

asociativa (La Primera Enmienda[569]), incluso si el texto real de la ley fundamental no contiene ninguna referencia al término "privacy".

Actualmente, algunos estados de los Estados Unidos (por ejemplo, Carolina del Sur) han incorporado a sus constituciones expresamente el derecho a la vida privada, las aplicaciones de este derecho encontrándose también a nivel infra-constitucional, en diversas leyes (códigos o estatutos) a nivel federal[570] o estatal[571].

7.2.2. El sistema de derecho continental

Los Estados con sistema de derecho continental han adoptado un método diferente para reconocer el carácter fundamental del derecho a la vida privada, en comparación con el sistema anglosajón. De este modo, tres situaciones son reconocibles: estados que han sido pioneros en la inclusión expresa en las constituciones de este derecho, sin ninguna influencia externa; estados que han incluido en sus constituciones este derecho, como resultado de la adhesión a algunos de los instrumentos jurídicos internacionales; estados que proclamaron el valor constitucional, por lo tanto, fundamental, del derecho a la vida privada, vía contenciosa constitucional. La característica común de todas estas situaciones se da por la comprensión y la apropiación interna del contenido complejo del derecho a la vida privada, con referencia también a la interpretación establecida en esta materia por la Convención Europea de Derechos Humanos, en su jurisprudencia unánime reconocida.

La Constitución alemana de Weimar (1919), aunque no preveía expresamente un derecho a la vida privada, abordando la cuestión de la libertad de la religión y el énfasis en el carácter laico del ejercicio de los derechos civiles, formula así: "*Nadie está obligado a revelar sus creencias religiosas. Las autoridades no tienen derecho a solicitar informaciones sobre la pertenencia de una persona a un culto religioso a menos que*

[569] *"El Congreso no hará ley alguna por la que adopte una religión como oficial del Estado o se prohiba practicarla libremente, o que coarte la libertad de palabra o de imprenta, o el derecho del pueblo para reunirse pacíficamente y para pedir al gobierno la reparación de agravios".*

[570] „Privacy Act" (La Ley de la vida privada), 88 Stat. 1896, 31.12.1974, "Children's Online Privacy Protection Act" (La Ley de la protección de la vida privada de los menores en Internet), 112 Stat. 2681-728, 21.10.1998.

[571] Por ejemplo, en Michigan, „Identity Theft Protection Act" (La Ley de la protección contra el robo de Identidad) de 2004, en Illinois, „Personal Information Protection Act" (La Ley de la protección de la información personal) de 1994 o en California „Security of Personal Information" (La seguridad de la información personal), parte del Código Civil.

dependan de ciertos derechos o deberes o, si es necesario, para lograr una estadística requerida por la ley" (Art. 136-Derechos civiles y políticos).

El contenido de este derecho, que implica la obligación negativa impuesta al Estado, de no obligar a la divulgación de la religión, puede ser asimilado con el derecho a la vida privada informativa, ya que será desarrollado por la jurisprudencia de la Convención Europea de Derechos Humanos, sobre la base de la experiencia alemana ("el derecho a la autodeterminación informativa"[572]), consagrado por el Tribunal Constitucional Federal de Karlsruhe).

La mayoría de los Estados europeos han adoptado o modificado sus propias constituciones después de la Segunda Guerra Mundial, ampliando el catálogo de los derechos incluidos en las leyes fundamentales, asumiendo los consagrados en los grandes instrumentos jurídicos internacionales adoptados en la segunda mitad del siglo XX.

En Alemania, el impacto devastador de las ideologías políticas que condujeron a atrocidades impensables para una civilización moderna ha influido decisivamente en la modificación de la Constitución. Así, en 1948, Alemania adoptó una nueva ley fundamental a nivel federal (promulgada en 1949 y revisada sucesivamente después de la reunificación, en 1993 y 2009) en la que la dignidad humana se eleva no sólo al rango de valor, sino también de derecho fundamental, desde el primer artículo[573]. El segundo artículo[574] estaba dedicado al reconocimiento del derecho al libre desarrollo de la personalidad humana, respetando los derechos de los demás, el orden constitucional y la moral. Estos dos rasgos definitorios para el nuevo estado alemán fueron la base para el esquema de la teoría de los derechos de la personalidad, a partir de la cual otros estados fueron inspirados posteriormente, y sobre la base de la cual el Tribunal Constitucional Federal en Alemania construyó una jurisprudencia en materia de defensa del derecho a la vida privada.

---

[572] Este derecho se definió como el derecho de cualquier individuo a decidir entre qué límites podrían divulgarse los datos sobre su vida privada y a protegerse de la tendencia progresiva de transformarse en una "propiedad pública".

[573] (1) El pueblo alemán reconoce la inviolabilidad e inalienabilidad de los derechos humanos como la base de cualquier comunidad, paz y justicia en el mundo.

(2) Los siguientes derechos fundamentales son directamente aplicables, con fuerza obligatoria para el poder legislativo, ejecutivo y judicial.

[574] Art. 2 Las libertades personales

(1) Toda persona tiene derecho al libre desarrollo de su personalidad, siempre que no infrinja los derechos de los demás o se ajuste sin perjuicio del orden constitucional o de la ley moral.

(2) Toda persona tiene derecho a la vida y a la integridad física. La libertad de la persona es inviolable. Cualquier interferencia con estos derechos sólo es posible bajo la ley.

En la misma medida, la Constitución de Bélgica, por ejemplo (adoptada en 1970 y modificada en 1994) ha regido claramente los dos derechos: el derecho a la vida privada y a la dignidad. Cabe destacar que la dignidad humana, en la concepción del constituyente belga, más allá de ser un derecho fundamental, es una garantía para el ejercicio de otros derechos de la misma importancia, en particular, los derechos socioeconómicos y culturales, juntos dentro del mismo artículo.

Y otros Estados europeos han previsto el derecho a la vida privada en la categoría de los derechos fundamentales, registrándolos en las constituciones; Damos sólo algunos ejemplos al respecto: la Constitución de Portugal[575] (1976), la Constitución Española[576], la Constitución de Eslovenia [577](1997), la Constitución de la República de Macedonia[578] (1992), la Constitución de Rumanía[579] (1991).

Un caso especial está representado por Francia. Pese a que la Declaración de los derechos humanos y del ciudadano de 1789 haya representado un hito en las teorías filosóficas y jurídicas para la proclamación de los derechos del individuo, Francia, en ninguna de las revisiones de su ley fundamental, no incluyó el catálogo de derechos y libertades fundamentales en su Constitución. Sin embargo, el preámbulo de la Constitución de 1958 subraya el apego del pueblo francés por los derechos humanos y los principios de la soberanía nacional, tal como se definen en la Declaración de 1789, confirmada y complementada por el preámbulo de la Constitución desde 1946[580]. Gracias a la jurisprudencia del Consejo Constitucional francés, sobre la base del principio del "bloque de constitucionalidad" establecido por este, ha sido consagrada el argumento de

[575] Según la Constitución de ese estado, en el art. 35 se reconoce el derecho de los ciudadanos a tener acceso a sus datos incluidos en la base de datos automatizados y a ser informados con respecto a la utilización de dichos datos, se garantiza el derecho a solicitar la rectificación y actualización de las informaciones contenidas en dichas bases de datos, se prohibió utilizar los medios de tratamiento de datos relacionados con creencias políticas, religiosas, filosóficas, afiliaciones políticas y sindicales. La Constitución regula claramente, en el art. 34 y, respectivamente, art. 36, la inviolabilidad de la residencia y la correspondencia, así como los derechos relacionados con la familia, el matrimonio y la filiación.

[576] El art. 18 de la CE reconoce y garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

577 En los art. 34-38 de dicha Constitución, revisada sucesivamente, varios derechos se rigen por separado: el derecho a la dignidad y a la seguridad personal, el derecho a la integridad física, psíquica, a la vida privada y a la personalidad, la inviolabilidad de domicilio, el derecho a la protección de la correspondencia y otros medios de comunicación, la protección de datos personales.

[578] Los artículos 11, 16, 17, 18 protegen la dignidad y reputación, la libertad de expresión, la privacidad de las comunicaciones y la privacidad.

[579] En la Constitución rumana de 1991, revisada en 2003, se incluye en el art. 26 El derecho a la vida íntima, familiar y privada, junto con la inviolabilidad del domicilio (art. 27) y el secreto de la correspondencia (art. 28).

[580] Melin-Soucramanien, F. (2009) *Les constitutions de la France de la Revolution a la IVe Republique*, Editorial Dalloz, Paris.

que, para la protección de los derechos y las libertades fundamentales, los dos textos deben entenderse como parte de la Constitución francesa.

El derecho a la vida privada no se ha tenido en cuenta como un derecho natural, "esencial e inviolable para el ser humano", tanto como para que los autores de la Declaración de 1789 inscriban expresamente en su texto. De esta forma, después de un largo desarrollo, basado en la jurisprudencia de los tribunales de derecho civil (pero también penal) y en la legislación de las relaciones jurídicas cubiertas por el respeto de los derechos de la personalidad en el tratamiento automatizado de datos (en los años '70), El Consejo Constitucional fue el que consagró el reconocimiento del valor constitucional y fundamental de este derecho[581].

En referencia a algunos de los componentes del derecho a la vida privada, identificados por la doctrina francesa (la libertad de la residencia, el derecho al secreto, el derecho a la inviolabilidad de la correspondencia, el derecho a la protección de la información nominativa, el derecho a una vida privada normal, el derecho a la vida sexual), se puede admitir que, sin embargo, este derecho fue elevado parcial y temporalmente al rango de un derecho constitucional en las primeras constituciones francesas (hasta el año 1848, por ejemplo, la inviolabilidad del domicilio), sin reanudar también en las leyes fundamentales posteriores.

Del mismo modo, el Consejo Constitucional reconoció el valor constitucional de algunos de los componentes del derecho a la vida privada (por ejemplo, el derecho a una vida familiar normal o la inviolabilidad del domicilio). Desde el punto de vista legislativo, los inicios de la garantía legal del derecho a la vida privada se remontan al siglo XIX, cuando por una ley de 1868 se ordenó que cualquier publicación, por escrito periódico, que se refiera a un hecho de la vida privada constituye contravención y se castiga con una multa de 500 francos[582].

A pesar de que, la conclusión que un autor francés extrae indica la reserva para el correcto reconocimiento del valor constitucional del derecho a la vida privada, en su conjunto, permaneciendo, por tanto, una libertad pública de segundo nivel[583].

---

[581] El derecho al respeto de la vida privada fue expresamente reconocido por el Consejo Constitucional con la decisión no. 94-352, de 18 de enero de 1995, con respecto a La Ley de orientación y programación de la seguridad, disponible en: https://www.conseil-constitutionnel.fr/decision/1995/94352DC.htm.

[582] Bertrand, A. (1999) *Droit à la vie privée et droit à l'image*, Editorial Litec.

[583] Lebreton, G. (2008) *Libertés publiques et droits de l'homme*, Editorial Sirey, p. 303: "El derecho balcanizado, el derecho a la vida privada a menudo encuentra grandes dificultades para ser reconocido en su globalidad. Si bien algunos de sus componentes se encuentran desde la Revolución, este derecho tuvo

Un debate especial es la naturaleza jurídica de este derecho en el ordenamiento jurídico de los Estados de la U.E. Los Estados que son miembros de la U.E., ya sea con un sistema de derecho continental o anglosajón, independientemente de si el derecho a la vida privada se incluye o no en sus constituciones (lato sensu), hay que tener en cuenta su valor de derecho fundamental en las actividades de aplicación del derecho de la U.E., en virtud de las obligaciones derivadas de los tratados constitutivos e implícitamente, de la Carta de los Derechos Fundamentales de la Unión Europea (*El derecho a la vida privada y familiar - art. 7*).

Las excepciones de este principio son los estados que declararon solemnemente ciertas derogaciones a los tratados europeos, mediante las cuales preservan la supremacía del derecho nacional. Mismamente, estados como el Reino Unido (que ya está en camino de salir de la UE) y Polonia, por el Protocolo no. 30 anexo al Tratado de Lisboa, declararon que las disposiciones de la Carta no amplían las competencias del Tribunal de Justicia de la Unión Europea, ni de los órganos jurisdiccionales nacionales para constatar que las leyes o prácticas de dichos estados no se ajustan a los derechos, libertades y principios consagrados en la Carta.

Cualquier referencia al derecho nacional en la Carta se interpretará por referencia al derecho nacional de estos dos estados. La República Checa también ha reiterado, mediante una declaración formal anexada al Tratado de Lisboa, que sus disposiciones sólo son aplicables a los Estados miembros en la medida en que apliquen el derecho de la unión y, como tal, se interpretarán en de acuerdo con sus tradiciones constitucionales.

En la misma medida, los Estados miembros del Consejo de Europa reconocen la existencia y el valor del derecho fundamental a la vida privada, como consecuencia de la inclusión en su derecho nacional de las disposiciones del Convenio para la protección de los derechos humanos y las libertades fundamentales, en particular, del art. 8 lo que defiende este derecho:

> *"1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia*

que esperar hasta 1970 para ser consagrado como tal por una ley. Su valor constitucional sigue siendo muy incierto. Estas vacilaciones enfatizan su carácter frágil, más que en el caso de otras libertades públicas. [...] Mientras su valor constitucional no se asiente claramente, el derecho a la vida privada seguirá siendo, por desgracia, una libertad pública de segundo nivel."

esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

7.3. El carácter de derecho fundamental a la vida privada a nivel de las organizaciones internacionales

Según las aclaraciones anteriores, las reglamentaciones nacionales de algunos países europeos se inspiraron en los documentos adoptados por las organizaciones internacionales y regionales a las que se adhirieron y que a mediados del siglo XX atribuyeron una importancia esencial (del derecho fundamental, por lo tanto) al derecho de la vida privada, junto con otros derechos reconocidos a este nivel.

Así, a nivel internacional, la Organización de las Naciones Unidas consagra este derecho en dos de sus principales documentos, en una redacción más o menos idéntica: La Declaración Universal de los Derechos Humanos de 1948 se ha pronunciado en el art. 12 que "*Nadie será objeto de intromisiones arbitrarias en su vida particular, en su familia, en su domicilio o en correspondencia, ni de ningún toque de su honor o reputación*".

Toda persona tiene derecho a la protección de la ley contra tales intromisiones y en este sentido también el Pacto Internacional de los Derechos Civiles y Políticos (adoptado en 1966, en vigor en 1976), en el art. 17 dispone que

"(1) Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. (2) Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

También en la Convención internacional sobre la protección de los derechos de todos los trabajadores migratorios y de sus familiares[584], el derecho de la vida privada goza de reconocimiento y garantías:

[584] Adoptada por la Asamblea General de la ONU en su resolución 45/158, de 18 de diciembre de 1990.

"Ningún trabajador migratorio o familiar suyo será sometido a injerencias arbitrarias o ilegales en su vida privada, familia, hogar, correspondencia u otras comunicaciones ni a ataques ilegales contra su honor y buen nombre. Todos los trabajadores migratorios tendrán derecho a la protección de la ley contra tales injerencias o ataques" (artículo 14).

El reconocimiento del derecho a la vida privada no requiere una cierta edad. Las Naciones Unidas reconocen el derecho del niño a la vida privada desde su nascimiento. La Convención sobre los Derechos del Niño[585], adoptada en 1989, en el artículo 16, lo contempla prácticamente en los mismos términos que los demás convenios y tratados internacionales:

"1. Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y a su reputación.

2. El niño tiene derecho a la protección de la ley contra esas injerencias o ataques".

Como se observa, estos documentos reflejaron en el contenido del mismo derecho la protección previsto por otras regulaciones, en particular las adoptadas a nivel nacional, de diferentes derechos (derecho a la vida privada, derecho a la vida familiar, la inviolabilidad del domicilio y el secreto de la correspondencia). Vale la pena señalar la preocupación de la organización internacional sobre los nuevos desafíos de la sociedad de la información.

En 1990, la Asamblea General de la Organización de las Naciones Unidas adoptó las directrices sobre los archivos informatizados de datos personales, documento del que resultan los principios de la protección de datos personales que se encuentran en la legislación de muchos estados y en los actos de algunas organizaciones regionales (Consejo de Europa).

También, a nivel internacional, la Organización para la Cooperación y el Desarrollo Económico, ha adoptado una serie de actos relativos a la protección de los datos personales, en particular: Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales[586] (1980) y las Directrices de la OCDE para la Seguridad de Sistemas y Redes de Información: hacia una cultura de Seguridad[587] (2002).

[585] Texto disponible en: https://www.un.org/es/events/childrenday/pdf/derechos.pdf.
[586] Texto disponible en: https://www.oecd.org/sti/ieconomy/15590267.pdf.
[587] Texto disponible en: https://www.oecd.org/sti/ieconomy/34912912.pdf.

El primer documento adoptado por la Organización para la Cooperación y el Desarrollo Económico en este ámbito pasó por un procedimiento de revisión, finalizado en el año 2013, con el fin de armonizarlo con los últimos avances tecnológicos[588].

En los dos continentes americanos, en África y en Europa, a nivel regional, se han adoptado varios convenios que dan valor al derecho a la vida privada. Dentro del sistema regional Interamericano, la Organización de los Estados Americanos ha estipulado en la Convención Americana sobre los Derechos Humanos[589] (Pacto de San José, 1969) el derecho a la vida privada (art. 11.2), el derecho a la vida familiar (art. 17) y el derecho al nombre (art. 18).

La Carta Africana de los derechos humanos y de los pueblos (Carta de Banjul - adoptada en 1981 y en vigor desde 1986) reconoce, en el sistema regional africano de protección de los derechos humanos de la Organización para la Unidad Africana, una serie de derechos del individuo, como el derecho a la dignidad (art. 5), a la libertad y a la seguridad (art. 6) a la existencia y a la autodeterminación (art. 20).

Estos derechos gozan también de una protección por parte del Protocolo relativo a la Carta africana de derechos humanos y de los pueblos para la creación de una Corte africana de los derechos humanos y de los pueblos, documento oficial que instituye un instrumento procesal de protección efectiva de los derechos humanos contenidos en la Carta Africana. Desde su primer artículo, el Protocolo menciona la existencia de un Tribunal Africano de Derechos Humanos y de los Pueblos capacitado a analizar y juzgar todos los casos y todas las faltas de acuerdo sobre la aplicación e interpretación de la Carta, del Protocolo o de otro instrumento ratificado, cuando este notificado a pronunciarse. El Tribunal tiene competencia tanto consultiva como contenciosa.

El año 2003 marcó un importante hito, la Unión Africana: adoptó el Protocolo de Maputo, que entró definitivamente en vigor en el año 2005. Es un protocolo adicional a la Carta Africana de Derechos Humanos, que garantiza derechos e igualdad a las mujeres, incluyendo derechos a la dignidad, a la familia, al matrimonio, a tomar parte en el proceso político, a la igualdad social y política con los hombres, o el derecho para controlar su salud sexual, entre otros. Estos instrumentos adoptados en África tienen por

[588] Véase Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales, disponibles en http://www.oas.org/es/sla/ddi/docs/directrices_ocde_privacidad.pdf.
[589] El texto de la convención es disponible en: https://www.corteidh.or.cr/tablas/17229a.pdf.

objeto reconocer los derechos humanos, incluidas las obligaciones del individuo, y los derechos de los pueblos.

El sistema de consagración y protección de los derechos humanos a nivel regional que nos interesa especialmente es el europeo[590], formado en torno a tres organizaciones: la Unión Europea, la Organización para la Seguridad y la Cooperación en Europa (OSCE) y el Consejo de Europa. Así, al nivel de la Unión Europea, las instituciones de la Unión y los Estados miembros han reconocido la importancia del respeto de los derechos humanos, en primer lugar partiendo de la jurisprudencia creada por el Tribunal de Justicia de las Comunidades Europeas (ahora Tribunal de Justicia de la Unión Europea) y, posteriormente, a través del art. 6 del Tratado de la Unión Europea, en el que se afirma que la Unión se basa en los principios de la libertad, de la democracia, del respeto de los derechos humanos y de las libertades fundamentales. Estos derechos, garantizados por el Convenio y como resulta de las tradiciones constitucionales comunes de los Estados miembros, representan principios generales del derecho de la Unión y del estado de derecho, todos ellos siendo al mismo tiempo principios comunes para los Estados miembros.

Por lo que se refiere al derecho de la vida privada, este derecho se rige expresamente por una serie de actos obligatorios de la Unión, de modo que, con la adopción de la Carta[591], se incluyen dos derechos distintos en el catálogo de los derechos fundamentales: el derecho a la vida privada y familiar y el derecho a la protección de los datos personales.

El derecho a la protección de datos también está asumido por los dos tratados constitutivos, modificados en virtud del Tratado de Lisboa. Con el fin de perseguir el cumplimiento de este derecho por parte de las instituciones y organismos de la Unión, también se ha establecido una autoridad de supervisión y control – La Autoridad Europea de la Protección de los Datos Personales, siguiendo el modelo de los existentes en los Estados miembros de la U.E. Por lo tanto, en la U.E., la Carta proclamó el derecho a la

[590] El derecho europeo de los derechos humanos se considera *original*, desde la perspectiva de los derechos garantizados y de los mecanismos de control, en particular, a través de su "jurisdiccionalización", la voluntad de proteger eficazmente los derechos humanos y la ampliación del derecho europeo de los derechos humanos a todas las ramas del derecho -J.-F. Renucci (2009) *Tratado de derecho europeo de derechos humanos, Hamangiu Publishing House, Bucarest*, p. 27

[591] La Carta fue proclamada solemnemente por las instituciones europeas (Parlamento, Consejo y Comisión) en Niza en el año 2000 y posteriormente, a través del Tratado de Niza (2001); Tras su enmienda, se proclamó de nuevo en 2007

vida privada y familiar en el art. 7, incluyendo en su contenido el respeto debido a la vida privada y familiar, al domicilio y al secreto de las comunicaciones.

Con respecto a la Organización para la Seguridad y la Cooperación en Europa, no tomamos en cuenta la adopción de un documento importante sobre el respeto de la vida privada o la protección de los datos personales, tanto más cuanto que las normas jurídicas de los derechos humanos se encuentran en fuentes de tipo "*soft law*", actos internacionales de carácter político y jurídico, lo que no significa, sin embargo, que las acciones emprendidas por esta organización no suelen tener el objetivo y la búsqueda del cumplimiento de estos derechos en los Estados miembros.

Pero el instrumento internacional más importante adoptado a nivel europeo en derechos humanos, que demuestra su plena eficiencia y actualidad, y más de 50 años después de su creación, está representado por el Convenio para la Protección de los Derechos y Libertades Fundamentales[592], el sistema internacional más antiguo, complejo, pero también más eficaz para la protección de los derechos humanos, debido en particular al papel desempeñado por el Tribunal Europeo de los Derechos Humanos (T.E.D.H.). Adoptado el 4 de noviembre de 1950 en Roma, por el Consejo de Europa, sólo 1 año después de la creación de dicha organización, el C.E.D.H. entró en vigor el 3 de septiembre de 1953 y fue modificado posteriormente por 14 protocolos adicionales, reconociendo los derechos y las libertades que no existían en la versión original. También se hicieron algunas modificaciones de procedimiento, la más importante de es la creación de un único órgano jurisdiccional permanente - el T.E.D.H., con la entrada en vigor el 1 de noviembre de 1998 de Protocolo No. 11 en la Convención.

El C.E.D.H. y los protocolos adicionales consagran un verdadero catálogo de derechos fundamentales, del que se han inspirado los electores nacionales o sindicales y los legisladores, cuantas veces han tenido que redactar textos esenciales en materia de legislación de los derechos humanos. Sin insistir en este tema, conservaremos que el derecho al respeto de la vida privada y familiar se rige por el art. 8 del Convenio:

"1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

[592] también llamado Convenio Europeo de Derechos Humanos (C.E.D.H.) El texto del Convenio es disponible en: https://www.echr.coe.int/documents/convention_spa.pdf

2. No podrá haber injerencia de la autoridad en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

El Consejo de Europa adoptó una serie de instrumentos jurídicos para la protección de la vida privada, incluso la protección de los datos personales y, a este respecto, podemos decir que es un pionero en materia. El Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal[593] (1981), modificado en el año1999, para permitir la adhesión de las Comunidades Europeas, y en 2001 mediante un Protocolo adicional sobre las autoridades de supervisión y las transferencias internacionales de datos. El Comité de los Ministros también adoptó resoluciones y recomendaciones sobre el respeto del derecho a la vida privada y a la protección de los datos personales en diversos ámbitos de actividad, algunos de los cuales adquirirán el carácter de hard law, por ser incluidos en el acquis comunitario (por ejemplo, en el contexto del acquis de Schengen, los países candidatos a la adhesión a este espacio están obligados a aplicar en la legislación nacional la Recomendación 87/15 de 17 de septiembre de 1987 del Comité de los Ministros del Consejo de Europa, que regula el uso de datos personales en el sector de la policía.

Durante el año 2012, se ha iniciado un proceso de reforma de los principales instrumentos jurídicos que rigen el sistema de garantía del derecho a la protección de los datos personales tanto a nivel de la U.E., como del Consejo de Europa, con el objetivo de adaptar las reglamentaciones a los últimos avances tecnológicos y aumentar la armonización de la legislación en los Estados miembros de estas organizaciones.

Por lo tanto, el derecho a la vida privada ha evolucionado del estatuto de un derecho natural, subjetivo e inviolable al de un derecho fundamental, reconocido tanto por los grandes sistemas jurídicos, de *common law* y de *civil law*, La forma en que este derecho ha transgredido de su estatuto de derecho civil al derecho constitucional específico, ya sea a través de los instrumentos de jurisprudencia constitucional, o por los legisladores u organizaciones internacionales para la protección de los derechos humanos, es pertinente determinar la naturaleza innegable del derecho fundamental a la vida privada

[593] El texto del Convenio es disponible en: https://rm.coe.int/16806c1abd

en los ordenamientos jurídicos sujetos al análisis. En la misma línea, la integración del derecho a la vida privada en los instrumentos en la parte superior de la jerarquía normativa de cualquier ordenamiento jurídico y su invocación por los jueces constitucionales denotan la incorporación en los elementos de la definición de los derechos fundamentales, que recordamos al principio de este capítulo.

7.4. Los elementos del derecho de la vida privada

Intentar proponer una definición para el derecho a la vida privada puede resultar muy difícil. La jurisprudencia internacional y algunos autores han reconocido que el derecho a la vida privada representa un concepto amplio, no susceptible de definiciones exhaustivas, y cuyo contenido es más extenso que el del derecho a la privacidad[594]. De tal forma que existen varios autores que abogan por una separación clara entre las dos nociones, en el sentido de que el derecho a la vida privada tiene un alcance mucho mayor que la privacidad te tipo que el primero comprende al segundo:

> *"Cuando hablo de privacidad no pretendo referirme en general a la vida privada, sino a un concepto más reciente, que en su configuración actual ha surgido seguramente a los finales del siglo XX. Desde luego, no es nada sencillo definir la privacidad"* [595].

Incluso la Real Academia Española define la privacidad como: "*ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión*", una relación de tipo parte-conjunto.

El objeto del derecho a la vida privada es la propia vida privada, analizada dentro de las relaciones jurídicas que nacen entre los titulares de este derecho (individuos) y la sociedad. Debido a su naturaleza autónoma y variable y teniendo en cuenta las diferentes condiciones morales, sociales, políticas o temporales, el derecho a la vida privada no puede analizarse en su sentido más estrecho, sin perder una serie de matices importantes, determinadas de manera precisa por las influencias anteriormente indicadas, y que construyen su complejidad. Sobre la base de este razonamiento, consideramos que un análisis significativo de los elementos del derecho a la vida privada se puede hacer por

[594] Maqueo Ramírez, M. S., Moreno González, J., Y Recio Gayo, M. (2017). *Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario*. Revista de derecho (Valdivia), 30(1), pp. 77-96.
[595] Piñar Mañas, J. L. (2010) *¿Existe privacidad?*, en *Protección de Datos Personales, Compendio de lecturas y legislación,* Editorial Tiro Corto, México, p. 16

referencia a la jurisprudencia del T.E.D.H[596]., que ha sido y sigue siendo la fuente de inspiración para los legisladores y los jueces de los Estados del sistema romano-germánico. Dependiendo de estos elementos, observaremos las similitudes y distinciones con el sistema anglosajón, donde estas existen.

La lectura del art. 8 del C.E.D.H nos ayuda a destacar en primer lugar dos observaciones: la disposición del Convenio responde a los elementos específicos de varios derechos distintos, respectivamente, el derecho a la vida privada, el derecho a la vida familiar, la inviolabilidad del domicilio y el secreto de la correspondencia; los dos párrafos del texto consagran, por una parte, el derecho de las personas al respeto de la vida privada y familiar, y, por otra, la obligación del Estado de abstenerse a infringir el derecho, salvo el cumplimiento de las condiciones acumulativas y expresamente reguladas (las condiciones de una injerencia legítima).

Sobre la base de una dinámica evolutiva de la conceptualización del derecho a la vida privada y del principio según cuál de los derechos protegidos por la Convención no deben ser teóricos e ilusorios, sino concretos y eficaces, la jurisprudencia del T.E.D.H., fundamentada sobre las disposiciones del art. 8 de la Convención, ha identificado varias categorías dentro de este derecho fundamental: el derecho a la vida personal privada, el derecho a la vida social privada, el derecho a la vida familiar, el derecho a la correspondencia, el derecho al domicilio.

En cuanto al contenido de la noción de vida privada, la jurisprudencia del T.E.D.H. ofrece una interpretación de esta en un doble sentido[597]:

-stricto sensu: la esfera íntima de las relaciones personales (es decir, todo sobre el desarrollo personal, en particular, la integridad física y moral de la persona, la filiación, el nombre y la nacionalidad), la vida sexual (incluido el principio de la libertad de la vida sexual), el derecho a la imagen, los datos personales;

- lato sensu: socializar la vida privada (el derecho a la identidad, el derecho a desarrollar relaciones con sus semejantes y el mundo exterior, el derecho a desarrollar una actividad profesional y de tener relaciones laborales interpersonales), el derecho al conocimiento de los propios orígenes, el derecho al respeto por una forma de vida.

---

[596] T.E.D.H., Caso Amann v. Switzerland, Sentencia de 16 de febrero de 2000, párr. 65, entre otros.
[597] Bogdan, D. y Selegean, M. (2005) *Drepturi şi libertăţi în jurisprudenţa Curţii Europene a Drepturilor Omului (Derechos y libertades en la jurisprudencia del Tribunal Europeo de Derechos Humanos),* Editorial All Beck Publishing House, Bucarest, p. 240;

Como tal, la noción fue interpretada por algunos autores[598] mediante la identificación de algunos "campos de aplicación" retenidos de la práctica del T.E.D.H.: la identidad personal, la integridad física y moral, la colección y el uso de las informaciones, la vida sexual.

En la literatura francesa[599] el derecho a la vida privada se incluye entre las libertades públicas, junto con el derecho de disponer de su propio cuerpo, el derecho a la integridad física, la libertad de circulación, el derecho a la seguridad.

Sobre la base de las principales fuentes de derecho escrito (Ley 78-17 de 6 de enero de 1978 sobre la tecnología de la información, archivos y libertades y el art. 9 del Código Civil) y la jurisprudencia en la materia, el mismo autor identificó en el contenido del derecho a la vida privada seis elementos esenciales: la libertad de la residencia/del domicilio, el derecho al secreto, el derecho a la inviolabilidad de la correspondencia, el derecho a la protección de la informaciones personales, el derecho a una vida familiar normal, el derecho a la vida sexual.

Según otro autor francés[600], la jurisprudencia francesa ha establecido la distinción entre el derecho a la vida privada y el derecho a la vida familiar (una noción relacionada con la primera). Como en la ley alemana, estas dos nociones se tratan por separado, y la interpretación de su contenido se hace sobre la base de diferentes motivos constitucionales. Un aspecto interesante se reproduce en la Constitución de Rumanía, que en el art. 26 garantiza el respeto del derecho a la vida íntima, familiar y privada (con un título enunciativo, sin especificar sus elementos en concreto):

> *"(1) Las autoridades públicas respetan y protegen la vida privada, familiar y personal.*
>
> *(2) La persona física tiene derecho a disponer de ella misma si no viola los derechos y las libertades de los demás, el orden público o la moralidad pública".*

Además, el art. 48 incluye las normas relativas a la familia, el matrimonio y la protección de los hijos del/fuera del matrimonio, mientras que la inviolabilidad del domicilio y el secreto de la correspondencia están regulados en otros dos artículos separados, el artículo 27 y respectivamente el artículo 28.

---

[598] Sudre, F., Milano, L. y Surrel, H. (2019) *Droit européen et international des droits de l'homme*, Editorial Presses Universitaire de France Paris.
[599] Lebreton G. (2008) *Libertés publiques et droits de l'homme*, Editorial Sirey.
[600] Burgorgue-Larsen, L. (2012) *La convention européenne des droits de l'homme*, Editorial LGDJ Paris.

El Código Civil rumano, al regular el derecho a la vida privada, proclama en el art. 71, párrafo 1 que "Toda persona tiene derecho al respeto de la vida privada".

En el párrafo 2 del mismo artículo establece que "nadie puede ser sometido a interferencia en su vida íntima, personal o familiar, en su domicilio, residencia o correspondencia, sin su consentimiento o sin respetar los límites previstos en el art. 75". El apartado 3 del art. 71 prevé la prohibición del uso, de cualquier manera, de la correspondencia, manuscritos u otros documentos personales, así como de la información de la vida privada de una persona, sin su consentimiento o sin respetar los límites previstos en el art. 75.

De acuerdo con el art. 75 del nuevo Código Civil, no constituye una violación del derecho a la vida privada o de los derechos correlativos, las interferencias permitidas por la ley o por los convenios y pactos internacionales de derechos humanos en los que Rumania es parte.

Nadie puede interferir o interferir en la vida íntima, familiar y privada de otra persona sin el consentimiento de esta última, consentimiento que debe ser explícito y expresado libremente, las autoridades tienen la obligación positiva de tomar todas las medidas y disposiciones posibles y razonables para proteger este derecho fundamental. En esta posición:

- los jueces tienen la obligación de declarar una audiencia judicial secreta en procedimientos en los que la publicidad afectaría estos valores, de acuerdo con la ley;

- escuchar, grabar o transmitir imágenes o palabras se considera un ataque a la vida privada de la persona si no existe un consentimiento expreso y previo en este sentido.

- cualquier persona tiene derecho exclusivo a su propia imagen;

- está prohibido publicar aspectos de la vida matrimonial de las personas.

En el sistema de derecho estadounidense, como hemos visto, el derecho a la vida privada ha nacido de manera pretoriana e incluye el derecho a la inviolabilidad del domicilio, reconocido bajo la Cuarta Enmienda de la Constitución de los Estados Unidos.

En la Constitución española el derecho a la vida privada está regulado por el artículo 18, como un conjunto de tres derechos fundamentales:

> *"1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*

2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.

3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

El desarrollo de la protección de estos derechos se encuentra, principalmente, en la Ley Orgánica no. 1/1982, de 5 de mayo, de protección civil del derecho al honor, la intimidad y la propia imagen, texto legal que intenta separar los supuestos de intromisión ilegítima (art. 7), de aquellos actos que no pueden clasificar del mismo modo, porque existe un consentimiento o porque se recogen imágenes públicas (art. 8).

Las provisiones de esta Ley se complementan con las normas de protección penal relativas a los delitos de injurias y calumnias (artículos 205-210; 491, 496, 404-5 Código Penal), y con los textos normativos de la Ley Orgánica no. 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, desarrollada por el Real Decreto 596/1999, de 16 de abril. Este último acto establece garantías específicas para el derecho a la intimidad, como la obligación de destruir las grabaciones de las videocámaras si no contienen pruebas de la comisión de alguna infracción penal o administrativa grave, junto con la obligación de informar el público de la existencia de instrumentos de grabación en ciertos espacios públicos.

Consideramos que los componentes identificados por la doctrina y la jurisprudencia del T.E.D.H., que los ha enmarcado dentro de la esfera de la noción de "derecho a la vida privada personal", y que es la más cercana al contenido del concepto anglosajón de *privacy*, pertenecen a la esencia del derecho a la vida privada.

Los otros elementos, en relación con el derecho a la vida familiar, la inviolabilidad del domicilio o el secreto de la correspondencia, aunque se incluyeron bajo el "paraguas" del mismo artículo 8 del Convenio, son aspectos relacionados con el derecho a la vida privada, con el que están entrelazados, y que ayudan en casos particulares a darle forma a su contenido, pero con el que no se identifican completamente, siendo susceptibles a estudiarse como derechos distintos. Siendo así, nuestro análisis se centrará en los elementos del derecho a la vida privada personal, y los

componentes colaterales que traspasan el mundo real y empiezan a manifestarse cada vez más en el mundo digital, un mundo digital amenazado de ataques cibernéticos, de intrusiones non autorizadas, de una carencia de regulación.

Para proponer medidas de seguridad y garantías para la protección del derecho a la vida privada tenemos que estudiar su contenido, los elementos que lo componen y los demás derechos relacionados.

El espacio digital es un ámbito donde ciudadanos y estados se encuentran e interaccionan entre si cada día, en condiciones similares. Cada uno de los actores quiere defender su territorio digital, sus prerrogativas y sus derechos intentando trasladar las reglas del mundo real en el mundo digital, un proceso que a veces no es tan fácil. A veces la legislación clásica no está preparada para regular problemas que aparecen en el mundo digital y aquí encontramos la mayoría de los derechos vulnerados. A veces los individuos ganan en frente de las autoridades cometiendo delitos y fraude, a veces los estados superan los límites de poder admitidos por la ley porque el espacio digital es muy volátil.

En este contexto vamos a analizar en adelante el contenido de los derechos derivados del derecho a la vida privada, subrayando las características que los hacen vulnerables al trasladarlos en el mundo digital.

Reducir el análisis de estos elementos también se justifica por la conexión intrínseca que tienen con el tema de nuestro trabajo, ya que aspectos como la inviolabilidad del domicilio o el derecho a un ambiente saludable, aunque son parte del complejo contenido del derecho a la vida privada, no tienen un significado especial para la individualización de la persona por referencia al área de información privada.

7.4.1. El derecho al nombre

Este derecho asegura a cada individuo una identidad que lo caracteriza en la relación con los otros miembros de la sociedad y que, en cierta medida, revela sus lazos familiares. Al nivel internacional, el derecho al nombre se encuentra regulado explícitamente por:

a) el Pacto Internacional de Derechos Civiles y Políticos (1966) en el artículo 24 párrafo 2: *"Todo niño será inscrito inmediatamente después de su nacimiento y deberá tener un nombre";*

b) la Convención de las Naciones Unidas sobre los Derechos del Niño (1989) en el artículo 7, primer párrafo: "*El niño será inscripto inmediatamente después de su nacimiento y tendrá derecho desde que nace a un nombre, a adquirir una nacionalidad y, en la medida de lo posible, a conocer a sus padres y a ser cuidado por ellos*";

c) la Convención Interamericana de Derechos Humanos (1969) en el artículo 18: "*Toda persona tiene derecho a un nombre propio y a los apellidos de sus padres o al de uno de ellos. La ley reglamentará la forma de asegurar este derecho para todos, mediante nombres supuestos, si fuere necesario*".

En la legislación española, la regulación del nombre y apellidos aparece contenida en el artículo 109 del Código Civil[601] y en los artículos 11, 50 a 57 de la Ley del Registro Civil de 2011[602]. Conforme al artículo 11, entre los derechos que las personas tienen ante el registro civil se encuentra también "*el derecho a un nombre y a ser inscrito mediante la apertura de un registro individual y la asignación de un código personal"*. En España las personas son designadas por un nombre y apellidos, correspondientes a ambos progenitores. En Rumania, las personas pueden tener un nombre de bautizo y un nombre de familia (similar al apellido español) que es común con ambos padres (si se conocen).

Tanto la Ley del Registro Civil como su Reglamento establecen pautas de determinación, así que una persona no puede tener más de un nombre compuesto ni más de dos simples. esta prohibición no se encuentra en la legislación rumana. En ambos sistemas de derecho está prohibido a asignar a una persona un nombre que objetivamente la puede perjudicar, afecta su identificación o introduzca a error en cuanto al sexo. otra particularidad de la legislación española es la interdicción de imponer al nacido el mismo nombre que uno de sus hermanos, o su traducción o transcripción en otro idioma, a no ser que hubiera fallecido. En cuanto a los apellidos, si estamos en lasituacion de que ambos padres son conocidos, el padre y la madre podrán decidir de común acuerdo el orden de transmisión de su primer apellido antes de la inscripción registral. En falta de tal acuerdo,

---

[601] Artículo 109 del Código Civil (Real Decreto de 24 de julio de 1889, BOE-A-1889-4763):
"La filiación determina los apellidos con arreglo a lo dispuesto en la ley. Si la filiación está determinada por ambas líneas, el padre y la madre de común acuerdo podrán decidir el orden de transmisión de su respectivo primer apellido, antes de la inscripción registral. Si no se ejercita esta opción, regirá lo dispuesto en la ley. El orden de apellidos inscrito para el mayor de los hijos regirá en las inscripciones de nacimiento posteriores de sus hermanos del mismo vínculo. El hijo, al alcanzar la mayor edad, podrá solicitar que se altere el orden de los apellidos".

[602] Ley 20/2011, de 21 de julio, del Registro Civil, BOE-A-2011-12628, disponible en: https://www.boe.es/eli/es/l/2011/07/21/20/con

el orden de los apellidos será establecido por la ley, que mantiene la prioridad del apellido paterno sobre el materno.

La doctrina rumana del derecho civil coloca el derecho al nombre en la categoría de derechos personales no patrimoniales, definiendo el nombre como "ese atributo de identificación de la persona física que consiste en el derecho humano a ser individualizado, en la familia y en la sociedad, por las palabras establecidas, bajo las condiciones de la ley, con este significado"[603]. El contenido del derecho al nombre incluye una serie de prerrogativas, tales como: el derecho a tener y a usar un nombre, el derecho a solicitar la corrección de los errores en los documentos del estado civil (u otros documentos), el derecho a oponerse al uso sin derecho de ese nombre por otra persona.

La naturaleza jurídica de este derecho viene dada por su carácter opuesto erga omnes, inalienable, indescriptible, personal, universal, legal y unitario. A pesar de su "inalienabilidad", el nombre (lato sensu) se puede modificar o cambiar administrativamente. Algunas de las prerrogativas identificadas por los autores civilistas están estrechamente relacionadas con el ejercicio del derecho a la protección de datos personales (o de las informaciones nominativas, como también se conoce en el derecho francés), en virtud de la cual una persona puede solicitar y obtener de cualquier persona que procese los datos nominales, la rectificación (si corresponde) u oponerse a su uso en ciertas operaciones de procesamiento. El derecho se encuentra regulado por los artículos 82 – 86 del Nuevo Código Civil Rumano y por la Ley no.119/1996 sobre el registro civil.

Al nivel europeo, el T.E.D.H. tuvo la oportunidad de pronunciarse en varias circunstancias[604] sobre el contenido del derecho al nombre, en casos que tratan sobre el establecimiento del nombre común (stricto sensu - apellido) de los cónyuges, la elección del nombre de un niño por parte de los padres, el cambio del nombre (lato sensu - apellido y /o nombre) por medios administrativos. De estos casos resulta que los estados deben

[603] Beleiu, Ghe. (1994) *Drept civil roman* (*Derecho civil rumano)*. Editorial: Sansa SRL, Bucarest.

[604] Sentencias T.E.D.H. Burghartz contra Suiza, de 22 de febrero de 1994; Boulgakov contra Ucrania, de, 11 de septiembre de 2007; S. y Marper contra Reino Unido, 4 de diciembre de 2008 y SS T.E.D.H. 1 julio 2008 (T.E.D.H. 2008/46) Caso *Daroczy contra Hungría y 17 de febrero de 2011, Caso Golemanova contra Bulgaria.* Las sentencias, relativas al cambio de nombre de una persona en relación con el que se venían utilizando habitualmente, contienen soluciones diferentes en cuanto a la posición mantenida por el Tribunal: "En el primer caso se entiende vulnerado el artículo 8 del Convenio, mientras que en el segundo prevalece el interés público de proteger la estabilidad de la identificación personal de los individuos sobre el interés del demandante de proteger su vida privada. La razón que justifica la diferencia del criterio utilizado en una y otra sentencia, para estimar en la primera y desestimar en la segunda la vulneración del artículo 8, se encuentra en la forma en que se había atribuido el nombre que se pretendía cambiar, en cada caso: impuesto por las autoridades en el primero de los supuestos, frente al segundo en que el nombre le había sido atribuido a la demandante por su padre al nacer".

reconocer el derecho de cualquier persona a tener el nombre que desea, sin injerencias no permitidas de las autoridades responsables del registro civil, pero al mismo tiempo se permite un cierto margen de apreciación a favor de los estados, dentro de los reglamentos emitidos (relacionados con el orden público o moral). Un caso especial es el cambio de nombre como resultado del cambio de sexo (en el caso de los transexuales), una situación que se analizará en la subsección sobre el derecho a disponer de la propia persona.

En el derecho estadounidense, basado en la doctrina de la responsabilidad civil (tort law), se consagra el derecho de una persona a solicitar una compensación de una persona que se ha apropiado de sus elementos personales que la definen, como su nombre o características[605].

7.4.2. El derecho a la identidad

En cierta medida relacionado con el derecho al nombre, el derecho a la identidad se refiere a la posibilidad de que cualquier individuo de conocer sus propios orígenes que lo definen como persona, en relación con los demás. En particular, este derecho fue invocado por las personas adoptadas que desean descubrir la identidad de los padres biológicos (para obtener la llamada "seguridad emocional") y, posiblemente, contactarlos, o por las personas que pretendieron establecer o contestar la paternidad de un niño.

El T.E.D.H. reconoció que algunas de estas solicitudes estaban bien fundamentadas en las provisiones del art. 8 de la Convención, teniendo en cuenta que el derecho a la vida privada también implica el derecho a "establecer y desarrollar relaciones con otras personas y con el mundo exterior". En cambio, en otros casos, T.E.D.H. apreció que no era desproporcionado rechazar la solicitud de ser reconocido como sucesor de una persona fallecida, si el solicitante era su sobrino, el Tribunal considerando que la identidad puede variar "dependiendo del grado de proximidad de los ascendientes en relación con los cuales se va a establecer este derecho".

El primer paso para reconocer el derecho a conocer la identidad biológica se dio en el caso *Mikulić c. Croacia*. El caso surge de una situación fáctica clásica, siendo el demandante un hijo nacido fuera del matrimonio, que quiere establecer la paternidad

[605] Prosser, W.S (1960) *Privacy*. California Law Review, vol.48, no.3, recuperado de: https://heinonline.org/HOL/LandingPage?handle=hein.journals/calr48&div=31&id=&page=

hacia el hombre al que considera su padre. Se queja, entre otras cosas, de la violación de su derecho a la intimidad por la ausencia de una decisión judicial en su caso, lo que la deja en la incertidumbre sobre la identidad de su padre.

Para determinar si hubo o no una violación a la privacidad de la demandante, el T.E.D.H. analizo en contrapartida el derecho del demandante a conocer su identidad biológica y el derecho del presunto padre a negarse a someterse a una prueba de ADN, que a su vez está protegido por el artículo 8 de la Convención, que protege la integridad física de la persona frente a injerencias arbitrarias del Estado. Establece que el Estado croata violó el derecho del solicitante en virtud del art. 8 por el hecho de que no mantuvo un justo equilibrio entre los dos derechos analizados, implementando medidas procesales que permitirían la solución del caso y salir del impasse de la denegación de la prueba de ADN. El Tribunal fallo que las personas en la situación del demandante tenían un interés vital, amparado por la Convención, en obtener la información necesaria para descubrir la verdad sobre un aspecto importante de su identidad personal, el de conocer a sus padres.

En el caso *Godelli c. Italia*[606], el Tribunal clarifico la cuestión, concluyendo que el derecho a conocer la propia identidad biológica forma parte de la amplia noción de vida privada, solo cuando el niño está buscando las verdaderas conexiones biológicas y no tiene otras conexiones ya atribuidas con una familia ya existente en su vida. La conclusión es lógica en la luz de la jurisprudencia europea que considera que el articulo 8 protege la continuidad de la vida privada familiar, solo si tal vida existe y se demuestra que es anterior al juicio.

En el contenido del derecho a la identidad fueron admitidos, de acuerdo con la evolución dinámica de la jurisprudencia de la T.E.D.H, el derecho a tener un nombre, el

[606] En el caso Godelli contra Italia, la demandante (adoptada en su niñez) consideraba que se había vulnerado su derecho a la vida privada porque la legislación italiana que protege la voluntad manifestada en el parto por la madre biológica de mantener en secreto su identidad le ha negado el derecho de descubrir sus orígenes por. Al respecto, el Tribunal Europeo de Derechos Humanos señaló que "el deseo de la demandante no es poner en cuestión su filiación adoptiva sino conocer las circunstancias de su nacimiento y de su abandono incluyendo la identidad de sus padres biológicos y que el derecho a conocer su ascendencia se encuentra en el campo de aplicación de vida privada, que engloba aspectos importantes de la identidad personal, entre los que la identidad de los progenitores es una parte". La sentencia menciona que: "el artículo 8 protege un derecho a la identidad y al desarrollo personal y a establecer y desarrollar vínculos con sus semejantes y con el mundo exterior y que este desarrollo contribuyen el establecimiento de detalles de su identidad como ser humano y el interés vital, protegido por el Convenio, a obtener las informaciones necesarias para descubrir la verdad en relación a un aspecto importante de su identidad personal, por ejemplo, la identidad de sus progenitores". En conclusión, el Tribunal Europeo concluyó que "se había vulnerado el derecho a la vida privada de la demandante porque la legislación italiana no había conseguido un equilibrio de proporcionalidad entre los intereses de las partes en conflicto (derecho a los orígenes de la hija y anonimato de la madre biológica)".

derecho a ser reconocidas las creencias religiosas, el sexo o la identidad étnica. En el orden constitucional de algunos estados europeos, el derecho a la identidad se asimila regularmente con el reconocimiento del estado del origen y de la pertenencia a una determinada etnia de sus ciudadanos y a su expresión, cultural, política, lingüística o religiosa.

En la jurisprudencia reciente[607] del T.E.D.H, se admitió que, de acuerdo con el principio de autonomía personal, se otorga protección a la esfera personal de cada individuo, incluido el derecho a establecer los detalles de su identidad como ser humano, y la identificación de género, nombre y orientación sexual, así como la vida sexual, son detalles relacionados con de la identidad individual, entrando en la esfera personal protegida por el art. 8. El Tribunal dictaminó que la identidad étnica es también un detalle que se relaciona con la identidad del individuo que queda bajo la protección del art. 8. En este caso, el T.E.D.H. incluso definió la esfera de elementos que podrían constituir la identidad étnica de una persona: "vínculos objetivamente verificables con el grupo étnico, como el idioma, el nombre, la empatía y otros".

En España, la Constitución no menciona el derecho a la identidad, pero la doctrina considera que "*la búsqueda de los propios orígenes puede inferirse de otros principios y derechos constitucionales como son la dignidad (art. 10.1), el libre desarrollo de la personalidad (art. 10.1), la integridad física y moral (art. 15), la intimidad (art. 18) o la investigación de la paternidad (art. 39.2)*" [608]. Esta derivación de un derecho constitucional ayuda al titular a proteger su derecho a la identidad mediante el recurso de amparo previsto por el artículo 53.2 de la Constitución Española. en la opinión de algunos autores[609], el derecho a los orígenes se goza de la protección jurisdiccional del recurso de amparo si se acepta que es una especie del derecho a la

[607] Sentencia T.E.D.H. *Ciubotaru v. Moldova* - 27138/04, Judgment 27.4.2010 - En 2002, cuando solicitó la sustitución de su antiguo documento de identidad soviético por uno moldavo, Ciubotaru afirmó que su origen étnico era rumano. Como le dijeron que su solicitud no sería aceptada a menos que indicara el origen étnico moldavo, como en los documentos soviéticos suyos y de sus padres, accedió. Posteriormente solicitó a la autoridad estatal competente que cambiara su entrada de identidad étnica de "moldavo" a "rumano". Su solicitud fue rechazada con el argumento de que, dado que sus padres no habían sido registrados como de etnia rumana en sus certificados de nacimiento y matrimonio, era imposible que él figurara como de etnia rumana. Se le aconsejó que buscara en los archivos rastros del origen rumano de sus antepasados. Se rechazaron las apelaciones a los tribunales nacionales. El Tribunal determinó que el procedimiento de Moldavia para cambiar la etnia registrada violaba el artículo 8 (derecho a la vida privada) del Convenio Europeo de Derechos Humanos.

[608] Jarufe Contreras, D (2013) *Tratamiento legal de las filiaciones no biológicas en el ordenamiento jurídico español: adopción "versus" técnicas de reproducción asistida*, Editorial Dykinson, Madrid;

[609] Igareda Gónzalez, N. (2014) *El derecho a conocer los orígenes biológicos versus el anonimato en la donación de gametos*, Revista Derechos y Libertades, núm. 31/2014, pp. 227 a 249.

integridad (previsto en el art. 15 CE), pero perdería este privilegio procesal si aceptamos la tesis que identifica sus orígenes en el principio a la dignidad (regulado por el art. 10.1 CE), situación en que será defendido mediante los procedimientos ante los tribunales ordinarios.

En lo que concierne el derecho a conocer los propios orígenes biológicos existen opiniones[610] que abogan por la derivación de este derecho de las provisiones del artículo 10.1 CE (la dignidad humana) como también hay teorías que encuentran los orígenes de este derecho en el contenido del derecho a la identidad y desarrollo personal, que a su turno deriva del principio de la dignidad humana. Una persona que no puede conocer sus orígenes no se puede considerar una personalidad completa y su salud emocional, psíquica o física se puede ver afectada por esta falta de información. De aquí se puede extraer una conexión directa entre el derecho a conocer sus orígenes y el derecho a la integridad física y moral (previsto por el art. 15 de la Constitución y protegido por el recurso de amparo).

El derecho a conocer los orígenes biológicos está expresamente regulado por la Ley 54/2007 de 28 de diciembre, de Adopción Internacional, exactamente en el artículo 12 que estipula lo siguiente: "*Las personas adoptadas, alcanzada la mayoría de edad o durante su minoría de edad a través de sus representantes legales, tendrán derecho a conocer los datos que sobre sus orígenes obren en poder de las Entidades Públicas, sin perjuicio de las limitaciones que pudieran derivarse de la legislación de los países de procedencia de los menores*". El derecho está bien confirmado por el art. 180.6 del Código Civil: "*Las personas adoptadas, alcanzada la mayoría de edad o durante su minoría de edad a través de sus representantes legales, tendrán derecho a conocer los datos sobre sus orígenes biológicos*", pero no puede afectar la filiación adoptiva ya establecida, de acuerdo con el art. 180.4 del Código Civil: "*La determinación de la filiación que por naturaleza corresponda al adoptado no afecta a la adopción*".

En Rumania, el derecho a la identidad está expresamente reconocido por el artículo 6 de la Constitución:

"1) El Estado reconoce y garantiza el derecho de las personas que pertenecen a las minorías nacionales a preservar, desarrollar y expresar su identidad étnica, cultural, lingüística y religiosa.

[610] Gómez Bengoechea, B. (2007) *Derecho a la identidad y filiación: Búsqueda de orígenes en adopción internacional y en otros supuestos de filiación transfronteriza*, Editorial Dykinson, Madrid;

2) Las medidas de protección adoptadas por el estado para preservar, desarrollar y expresar la identidad de las personas pertenecientes a las minorías nacionales deben ser conformes con los principios de igualdad y non discriminación en relación con los demás ciudadanos".

Pues, en este caso, se trata de un derecho a la identidad étnica y cultural sin estar directamente vinculado con el conocimiento de los orígenes biológicos individuales. Según la legislación rumana este derecho pertenece a las personas que forman parte de grupos étnicos minoritarios y no está reconocido a todo individuo que desea conocer sus padres biológicos. En caso de Rumania, solamente el derecho a la identidad étnica, cultural y religiosa goza de una protección constitucional, al mismo tiempo que el derecho a la identidad biológica queda sin una regulación legal expresa.

7.4.3. El derecho a la propia imagen

El reconocimiento y la protección del derecho a la vida privada, tanto en los EE. UU., como en Europa, se debe en primer lugar, a la necesidad de reconocer el derecho a la propia imagen, entendido como la capacidad de cualquier individuo para preservar su propia imagen y disponer de su uso, sin ningún tipo de injerencia externa.

"*La imagen humana individualiza a las personas y las distingue de los demás, les confiere una proyección externa que aporta elementos para conocer su modo de ser personal. La imagen humana es un reflejo, una representación de toda la persona en su conjunto, pero –como es generalmente reconocido- la parte del cuerpo que mejor plasma la personalidad del hombre es la cara*"[611]. Siendo un elemento identificable, a veces incluso con un valor patrimonial determinado (por ejemplo, en los casos de los artistas famosos), este derecho goza de una protección jurídica efectiva. La violación del derecho a la propia imagen, mediante la difusión non autorizada de grabaciones o fotos de una persona, puede afectar negativamente su derecho a la intimidad, junto con el derecho a la vida privada o al honor.

Este derecho consiste en el poder exclusivo de una persona de disponer de su propia imagen como considera, por ejemplo, reproducirla, publicarla, exponerla o venderla. Como consecuencia de este derecho, queda prohibida cualquier conducta que

[611] Azurmendi Adarraga, A. (1998) *El derecho a la propia imagen: su identidad y aproximación al derecho a la información*, 2da. ed., Fundación Manuel Buendía, Universidad Iberoamericana, México, pp. 21 y ss

tiene como resultado la publicación no autorizada de información personal. El consentimiento del titular de los datos es imperativo para determinar si una cierta conducta es legal o ilegitima. No importa si el consentimiento es obtenido de modo gratuito o a base de una recompensa pecuniaria

El desarrollo fulminante de la jurisprudencia de los tribunales en los dos continentes con respecto a este elemento del derecho a la vida privada se debe principalmente a la proliferación de los medios modernos de capturar la imagen, a través de la fotografía, la prensa y audiovisual, y más recientemente, del Internet. A partir del análisis de la doctrina y la jurisprudencia de los dos sistemas de derecho, se pueden destacar dos categorías principales de violaciones del derecho a la imagen: el uso sin el consentimiento del interesado de su imagen a través de divulgaciones públicas y el uso con mala fe de la imagen de la persona, que puede traerle una violación de su reputación y de su honor. El artículo escrito por Samuel D. Warren y Louis Brandeis[612] en 1890, el caso Bismarck de Alemania en 1898[613] o el caso de Rachel de Francia (1858)[614] entran en la primera categoría, y el punto de partida es la publicación no permitida de algunas fotografías o retratos en un periódico.

En la segunda categoría se pueden ingresar aquellos actos punibles por una acción civil en los EE. UU. bajo "tort law", en el caso de la divulgación pública de informaciones que presentan una imagen contraria a la realidad[615]. En Francia, tales actos se sancionan sobre la base de la Ley de la Prensa del 29 de julio de 1881. En este estado, el interés por la protección del derecho a la imagen se restableció en los años '60-'70, con la ocasión de unos juicios famosos (Picasso, Gerard Philippe y Brigitte Bardot) y que estuvieron al origen de la regulación del art. 9 del Código Civil francés ("Toda persona tiene derecho al respeto de su vida privada") y de otras disposiciones del Código Penal

[612] Warren, S. D. y Brandeis, L. D. (1890) idem.
[613] Véase la nota 439.
[614] En Francia, el caso conocido como Affaire Rachel se presentó en 1858, cuando la hermana de una actriz famosa (Rachel) realizó un contrato con un diseñador para que hiciera un retrato del físico de Rachel estando en su lecho de muerte y que posteriormente fue publicado en varios medios de comunicación sin el consentimiento de sus demás parientes; estos últimos acudieron ante los jueces con el respectivo reclamo por el respeto a la memoria de la actriz. Los jueces reconocieron que "el derecho a oponerse a tal reproducción es absoluto, (…) el cual no podría ser desconocido sin enfriar los sentimientos más íntimos, los más respetables de la naturaleza y de la piedad doméstica".
[615] Barnett, S. (1999) *The Right to One's Own Image': Publicity and Privacy Rights in the United States and Spain*. American Journal of Comparative Law 47, pp. 555–582

francés que sancionan, entre otras, fotografiar desde lejos la persona sin su conocimiento[616].

La jurisprudencia del siglo pasado abunda en sentencias pronunciadas contra de algunos periodistas o algunas publicaciones que perjudicaron en ambos sentidos el derecho a la imagen de las personalidades públicas, incluso si se supone que renunciaron tácitamente a una parte de su vida privada a través de la exposición debida a su celebridad o dignidad ocupada. Uno de los principales problemas que surgen en relación con el derecho a la imagen es la necesidad de encontrar un equilibrio justo y proporcional entre el derecho a la vida privada y la libertad de expresión de la prensa o el derecho del público a tener acceso a informaciones de interés general.

El T.E.D.H. también tiene una rica jurisprudencia[617] en el campo de los derechos de la imagen, con sentencias ya famosas como el llamado juicio "Caroline de Monaco"[618]. Típico de estos procesos es el carácter público del titular del derecho, dado los diferentes matices dados por la naturaleza de esta publicidad: debido a las cualidades personales nativas (actores, cantantes o deportistas famosos) o debido a la calidad del funcionario público o encargado público de alto nivel. Según este último criterio, se sostuvo que el derecho a la vida privada es mucho más bajo o incluso inexistente cuando un dignatario está en el ejercicio de su función o está involucrado en actividades relacionadas con su condición de persona pública. Para determinar en qué medida se produjo una injerencia con el derecho a la privacidad y se excedió el interés público en obtener informaciones a través de la prensa ("el perro guardián de la democracia"), se tuvieron en cuenta las técnicas utilizadas por los periodistas. Por ende, el uso de dispositivos de alto rendimiento que permiten la captura de imágenes y / o sonidos desde una gran distancia, de manera invasiva, sin el permiso y el conocimiento de los interesados, es una violación grave del derecho a la imagen / derecho a la privacidad[619].

---

[616] Bertrand, A. (1999*) Droit à la Vie Privée et Droit à l'Image*, Editorial Litec : Paris, p. 147

[617] Sentencia Observer y Guardian contra Reino Unido de 26 noviembre 1991 [T.E.D.H. 1991, 51], serie A núm. 216, pgs. 29-30, ap. 59 y Bladet Tromso y Stensaas contra Noruega [GS] núm. 21980/1993, ap. 59, T.E.D.H. 1999-III), serie A núm. 239, pg. 28, ap. 63; Bladet Tromso y Stensaas contra Noruega [GS], núm. 21980/1993 [T.E.D.H. 1999, 22], ap. 62, T.E.D.H. 1999-III.

[618] En el denominado caso *Von Hannover contra Alemania* [nº 59320/00, de 24 de junio de 2004], la princesa Carolina de Mónaco –que interpuso la denuncia como Caroline von Hannover– alegó que las resoluciones de los tribunales alemanes habían infringido su derecho al respeto de la vida privada y familiar, garantizado por el Art. 8 C.E.D.H..

[619] Welkowitz, D. S. (2013) Privatizing Human Rights? Creating Intellectual Property Rights from Human Rights Principles, Akron Law Journals, Akron Law Review: Vol. 46: Iss. 3, Article 3, recuperado de: https://ideaexchange.uakron.edu/cgi/viewcontent.cgi?article=1088&context=akronlawreview

El derecho a la imagen también se asimiló al derecho al secreto, entendido como el derecho de cualquier individuo a oponerse a la captura y a la divulgación de su imagen o su voz, o informaciones con respecto a la vida privada. La protección de este derecho en Francia se beneficia de una doble garantía, tanto penal como civil, la persona lesionada pudiendo obtener el pago de daños para reparar el prejuicio. Además, de conformidad con el art. 9 del Código Civil, el Tribunal también puede ordenar cualquier medida para impedir el logro u ordenar cesar la violación de la intimidad de la vida privada[620].

En España, el derecho a la propia imagen es un derecho fundamental protegido por el artículo 18 de la Constitución Española. Su contenido también está regulado por la Ley Orgánica 1/1982 de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen[621]. Este derecho posee una faceta positiva, consistente en la facultad de difundir cada uno su propia imagen, y una negativa que permite requerir la autorización para la reproducción de su imagen o incluso impedirla.

El Tribunal Constitucional (en las sentencias no. 231/88, 99/94, 81/2001 y 83/2002) ha reconocido el carácter autónomo de este derecho constitucional que goza de mecanismos específicos de protección en caso de injerencias en la esfera personal de su titular, mediante la publicación de reproducciones de la imagen que pueden afectando la reputación del titular exponiendo su vida íntima. En este contexto, el titular tiene la posibilidad de solicitar conductas negativas por parte de los terceros, en base al reconocimiento de este derecho fundamental oponible erga omnes. Desde imágenes de su

---

[620] Lebreton G. (2008) idem.

[621] Artículo séptimo: "*Tendrán la consideración de intromisiones ilegítimas en el ámbito de protección delimitado por el artículo segundo de esta Ley: 1. El emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas; 2. La utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción; 3. La divulgación de hechos relativos a la vida privada de una persona o familia que afecten a su reputación y buen nombre, así como la revelación o publicación del contenido de cartas, memorias u otros escritos personales de carácter íntimo; 4. La revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela; 5. La captación, reproducción o publicación por fotografía, filme, o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos, salvo los casos previstos en el artículo octavo, dos; 6. La utilización del nombre, de la voz o de la imagen de una persona para fines publicitarios, comerciales o de naturaleza análoga; 7. La imputación de hechos o la manifestación de juicios de valor a través de acciones o expresiones que de cualquier modo lesionen la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación; 8. La utilización del delito por el condenado en sentencia penal firme para conseguir notoriedad pública u obtener provecho económico, o la divulgación de datos falsos sobre los hechos delictivos, cuando ello suponga el menoscabo de la dignidad de las víctimas*".

apariencia física hasta elementos de sus manifestaciones íntimas, todos los componentes de la esfera personal gozan de reconocimiento legal y protección jurisdiccional.

En Rumania el derecho a la propia imagen se encuentra regulado de forma indirecta por la Constitución en el artículo 30: "la libertad de expresión no puede perjudicar la dignidad, el honor, la vida privada de la persona y tampoco el derecho a la propia imagen". El contenido del derecho está definido por el artículo 73 del Nuevo código Civil que dispone: "Toda persona tiene derecho a su propia imagen. En el ejercicio del derecho a su propia imagen, podría prohibir o impedir la reproducción, de cualquier forma, de su apariencia física o voz o, en su caso, el uso de dicha reproducción".

No solo el uso de la imagen por parte de la prensa puede estar sujeto a la protección de este derecho. La videovigilancia también está sujeta a la ley. Sin embargo, la protección no es absoluta si el lugar supervisado es público, y el sujeto que lo lleva a cabo son las autoridades, con un propósito legítimo (la defensa del orden público).

7.4.4. El derecho a disponer de la propia persona

Este derecho ha sido considerado por la doctrina como uno de los derechos humanos más naturales, inalienables e indescriptibles, también conocido como "libertad corporal" (o el derecho a disponer del cuerpo propio). Su apariencia está estrechamente vinculada a las demandas feminista con respecto al control sobre la maternidad, pero que, por razones religiosas, morales o consuetudinarias, solo más tarde fue sometido a la protección jurídica.

En los Estados Unidos el derecho a usar anticonceptivos fue admitido en base a la Sentencia de la Corte Suprema en la causa Griswold v. Connecticut (381 U.S. 479 - 1965)[622], como un elemento del derecho a la privacidad. Las limitaciones que pueden presentarse a este derecho deben ser proporcional al propósito perseguido: "el propósito de las autoridades de controlar o prevenir actividades que, de acuerdo con la Constitución, están sujetas a regulaciones estatales, no puede lograrse por medio de la naturaleza que

[622] Griswold v. Connecticut, 381 U.S. 479 (1965), fue una decisión histórica de la Corte Suprema de los Estados Unidos en la que la Corte dictaminó que la Constitución de los Estados Unidos protege la libertad de las parejas casadas para comprar y usar anticonceptivos sin restricciones gubernamentales. El caso involucró una "ley Comstock" de Connecticut que prohibía a cualquier persona usar "cualquier droga, artículo medicinal o instrumento con el propósito de prevenir la concepción". El tribunal sostuvo que la ley era inconstitucional y que "el efecto claro de [la ley de Connecticut ...] es negar a los ciudadanos desfavorecidos ... el acceso a asistencia médica e información actualizada con respecto a los métodos adecuados de control del embarazo." Por una votación de 7 a 2, la Corte Suprema derogó la ley alegando que violaba el "derecho a la privacidad conyugal", sentando las bases para el derecho a la privacidad con respecto a las prácticas íntimas.

pueda invadir la esfera de las libertades protegidas". Esta Sentencia fue seguida por otros casos en los que la Corte Suprema de los EE. UU. admitió la prevalencia del derecho a la vida privada, por ejemplo, la causa Roe v. Wade, 410 U.S. 113 (1973), en el que se reconoció el derecho al aborto, con la imposición de unas condiciones destinadas a garantizar la vida y la salud de la madre y el niño.

En Alemania, el Tribunal Constitucional Federal[623], en el contexto de una legislación que sanciona el aborto, defiende el derecho a la vida privada de la madre en caso de la interrupción del embarazo antes del término (en las situaciones y las condiciones permitidas por ley). El Tribunal consideró que, al formular el derecho a la asistencia social, la ley debe proteger el derecho a la vida privada del beneficiario y contener disposiciones que previenen la obligación de la madre de repetir las razones personales por las cuales tomó la decisión, sin ignorar al mismo tiempo la necesidad de respetar el deber constitucional de proteger la vida del no nacido.

Otros problemas derivados del derecho a disponer de uno mismo están relacionados con: el uso de las drogas, la transexualidad, la donación de órganos y tejidos, estudios clínicos, experimentos de ingeniería genética. Junto con el derecho supremo de la persona a tomar sus propias decisiones con respecto a su cuerpo, en el contenido de este derecho se incluye la obligación del individuo de no violar los derechos de los demás, el orden público o la buena moral. Desde este punto de vista, las limitaciones legales que se pueden presentar a este derecho generalmente se refieren a la protección del grupo social del que es miembro: exámenes médicos impuestos en el entorno escolar o antes del matrimonio, las medidas tomadas por las autoridades competentes para la prevención o el combate de epidemias[624].

Algunos autores franceses[625] incluyeron el derecho a disponer del propio cuerpo en las libertades físicas "frente a las ciencias de la vida", separado del derecho a la vida privada: el derecho a mantener las relaciones sexuales, el derecho a procrear (natural o asistida médicamente), el derecho a cambiar de sexo, el derecho a donar órganos o productos del cuerpo, el derecho a decidir su propia muerte.

---

[623] Sentencia de la Segunda Sala, del 28 de mayo, 1993 –2 BvF 2/90 y 4, 5/92; Recuperado de: https://www.kas.de/c/document_library/get_file?uuid=0a66a4a6-1683-a992-ac69-28a29908d6aa&groupId=252038

[624] Evans, E. (2004) *Derechos Constitucionales*. Tomo I. Editorial Jurídica. Santiago.

[625] Lebreton, G. (2008) idem ; Miquel, P. -A. (2008) *Respect et inviolabilité du corps humain*, Revista Noesis. Recuperado de: http://journals.openedition.org/noesis/1383

Una discusión controvertida es sobre el derecho a la eutanasia, en forma de eutanasia voluntaria activa[626] (el uso de sustancias letales para terminar con la vida de un paciente con enfermedad terminal), que también se conoce como "suicidio asistido", si se realiza con el apoyo de un profesional médico. Aunque, es una práctica aceptada en estados como Bélgica, Luxemburgo, los Países Bajos, Suiza o los estados de EE. UU. Oregon y Washington, la mayoría de los estados europeos rechazan la idea de legalizar este derecho, visto por las partes interesadas como un elemento del derecho a la libre determinación.

En el mismo sentido, la Recomendación 1418 (1999), adoptada por la Asamblea Parlamentaria del Consejo de Europa el 25 de junio de 1999, alienta a los Estados miembros a respetar y proteger la dignidad de los pacientes incurables y moribundos, en todos los aspectos, en particular manteniendo la prohibición absoluta de poner fin intencionalmente a sus vidas, teniendo en cuenta que su derecho a la vida está garantizado por el art. 2 de la Convención, que el deseo de morir expresado por ellos nunca puede ser la base legal de la muerte causada por un tercero y no puede servir como una justificación legal para la ejecución de las acciones destinadas a causar la muerte.

En un caso famoso, Pretty Vs. Reino Unido[627], el T.E.D.H. admitió que la noción de autonomía personal puede incluir el derecho de una persona a realizar actividades percibidas como de naturaleza física o moral que son perjudiciales o peligrosas para su persona (según la jurisprudencia anterior). Por lo tanto, constituiría una violación del art. 8 de la Convención imponer un tratamiento médico sin el consentimiento de una persona con discernimiento, al lograr el daño de la integridad física de la respectiva persona. Sin embargo, en este caso, se pretendía reconocer el derecho a morir, lo cual es contrario a los principios de la Convención que defienden la vida, la dignidad y la libertad como valores supremos. En consecuencia, el Tribunal sostuvo que las restricciones impuestas por el Estado británico con respecto al castigo de las personas que responderían a una solicitud de "suicidio asistido" no son desproporcionadas ni arbitrarias, en relación con los valores defendidos.

La libertad sexual también es parte del contenido del derecho a disponer de la propia persona[628]. Desde este punto de vista, los estados se enfrentaron a varios desafíos

[626] Hume, D. (1995) *Sobre el suicidio y otros ensayos*. Alianza Editorial. Madrid.
[627] Sentencia 2346/02 Caso Pretty c. Reino Unido, 29 de abril de 2002, disponible en: https://www.law.utoronto.ca/utfl_file/count/documents/reprohealth/echr_uk_2002_pretty_espanol.pdf
[628] Bonilla Sánchez, J. J. (2010) *Personas y derechos de la personalidad,* Editorial Reus, Madrid.

provocados por los principales cambios producidos en las costumbres y la moral de la sociedad moderna, que llevó a una adaptación de la ley y la práctica judicial con respecto al reconocimiento de los derechos de las personas homosexuales o transgénero.

La jurisprudencia del T.E.D.H., a su vez, ha desempeñado un papel importante en el cambio de la legislación nacional en algunos estados para no excluir a las personas con una determinada orientación sexual de realizar actividades (por ejemplo, en el Reino Unido, la legislación que prohibía el empleo de personas homosexuales en el ejército). La libertad sexual ejercida entre los adultos y en el ámbito privado debe respetarse como tal, incluso si tales actos pueden "golpear, sorprender o molestar a otros que consideran que la homosexualidad es inmoral". Aun cuando, se permite un cierto margen de apreciación de los estados que pueden imponer limitaciones al ejercicio de este derecho, para proteger el orden público o los derechos de otras personas (menores o adultos incapacitados).

En el caso de los transexuales, el T.E.D.H., desde la Sentencia en la causa Cossey v. Reino Unido[629] hasta la Sentencia de la causa Christine Goodwin v. El Reino Unido[630] ha cambiado su jurisprudencia, reconociendo el derecho de estas personas a obtener por parte de las autoridades competentes la modificación de los documentos del estado civil, correspondientes a su nueva "identidad". Desde esta perspectiva, el derecho a disponer de la propia persona no se puede disociar del derecho al nombre y a la identidad, previamente analizados.

7.4.5. El derecho a la integridad física y moral

Una parte de la doctrina francesa[631] enmarca el derecho a la integridad física dentro de las libertades físicas "confrontadas con las ciencias de la vida", junto con el

[629] Cossey v. Reino Unido, Demanda No. 10843/84, Corte E.D.H. (1990), disponible en http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57641.
[630] Chirstine Goodwin era una mujer transexual que se sometió a una operación de cambio de sexo. Tras la intervención quirúrgica, enfrentó varios inconvenientes en su trabajo y manifestó haber sido víctima de acoso. Como el registro civil del Reino Unido no admitía alteraciones de la partida de nacimiento en lo que respecta al género, Goodwin debió mantener el certificado en el que se la identificaba como hombre. Esto le generó diversas molestias y humillaciones. Además, tuvo dificultades en el ámbito de la Seguridad Social: a los efectos legales era considerada un hombre, por lo que se le impuso el pago de aportes hasta los sesenta y cinco años, edad prevista para el retiro de los trabajadores del sexo masculino. Para evitar preguntas por parte de su empleador, firmó un acuerdo específico mediante el cual ella pagaba directamente sus aportes. Sin embargo, este sistema también resultaba engorroso, ya que los expedientes administrativos de personas trans eran catalogados como "sensibles", por lo que Goodwin debía solicitar turnos especiales para poder discutir sobre sus aportes.
[631] Lebreton G. (2008) idem .

derecho a disponer del propio cuerpo, incluido aquí: la prohibición de la tortura, el trato inhumano y degradante, la esclavitud y el trabajo forzado, los experimentos médicos, etc. La integridad física de la persona se ve de manera bastante distinta del derecho a la vida privada, y goza de una protección aún más efectiva dentro de los instrumentos internacionales[632] y las constituciones estatales[633], en relación con la prohibición de la tortura y los tratos inhumanos y degradantes (considerado un derecho absolutamente) e interfiriendo con la libertad individual.

Sin embargo, en la jurisprudencia[634] del T.E.D.H., por ejemplo, la integridad física y moral de la persona constituye el primer elemento señalado por el Tribunal dentro de la noción (que no puede ser exhaustiva) del derecho a la vida privada. La expresión de la plurivalencia y la interconexión entre los elementos del derecho a la vida privada, el contenido del derecho a la integridad física puede cruzarse con el del derecho a disponer de la propia persona, en situaciones tales como: la recolección de tejidos u otros productos del cuerpo humano[635], la vacunación obligatoria, las pruebas de la embriaguez de los conductores. El derecho del individuo a tener su propia integridad física puede en estos casos estar sujeto a limitaciones legítimas por parte de los estados.

En relación con la forma en que ciertos "productos" del cuerpo humano pueden ser recolectados, utilizados y almacenados, el Comité de Ministros del Consejo de Europa elaboró la Recomendación No. R (92) 1 sobre el uso del análisis de ácido

---

[632] El artículo 7 del Pacto Internacional de Derechos Civiles y Políticos dispone: "*Nadie será sometido a torturas ni a penas o tratos crueles, inhumanos o degradantes. En particular, nadie será sometido sin su libre consentimiento a experimentos médicos o científicos*."

[633] La Decimotercera Enmienda a la Constitución de los Estados Unidos, apartado no. 1: "Ni en los Estados Unidos ni en ningún lugar sujeto a su jurisdicción habrá esclavitud ni trabajo forzado, excepto como castigo de un delito del que el responsable haya quedado debidamente convicto". Artículo 22 de la Constitución Rumana: "Se garantiza el derecho a la vida, así como el derecho a la integridad física y psíquica de la persona. Nadie será sometido a torturas ni a penas o tratos inhumanos o degradantes. La pena de muerte está prohibida". Artículo 15 de la Constitución Española: "Todos tienen derecho a la vida y a la integridad física y moral, sin que, en ningún caso, puedan ser sometidos a tortura ni a penas o tratos inhumanos o degradantes. Queda abolida la pena de muerte, salvo lo que puedan disponer las leyes penales militares para tiempos de guerra".

[634] T.E.D.H. – Sentencia de 04.12.2008, S. y Marper c. Reino Unido, 30562/04 y 30566/04, estableciendo que "la conservación sistemática e indiscriminada por parte de autoridades públicas de huellas dactilares y muestra y perfiles de ADN de personas no condenadas vulnera el Artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales". El fallo, publicado en un momento en el que el desarrollo de bases de datos biométricos en Europa y las transferencias de dichos datos resultan de especial actualidad, subraya la necesidad de limitar su tratamiento reflejando un justo equilibrio entre los intereses públicos y privados en juego. La sentencia representa además un paso decisivo en la clarificación de las relaciones entre el derecho a la vida privada protegido por el artículo 8 del C.E.D.H. y los principios generales de protección de datos personales.

[635] Espinosa de los Monteros, R. Z. (2014) *El impacto de la prueba de ADN en los derechos fundamentales (I)*, Diario La Ley, ISSN 1989-6913, Nº 8283.

desoxirribonucleico (ADN) dentro del marco de la administración de justicia penal[636] (adoptado el 10 febrero de 1992). Este acto fue un fundamento para la sentencia del T.E.D.H. en una de las causas importantes con respecto al respeto del derecho a la vida privada en el contexto del uso de huellas digitales, muestras biológicas y perfiles de ADN por parte de la policía. De las tres categorías de datos, el Tribunal determinó que la retención de las muestras biológicas y de los perfiles de ADN presenta más riesgos debido a las informaciones que contienen (incluido el estado de salud y la relación genética con la familia del propietario), así como el temor de las personas de que puedan ser utilizados en el futuro (en ingeniería genética, por ejemplo), un aspecto legítimo que se tiene en cuenta al evaluar la injerencia producida en la vida privada de los solicitantes.

Al respecto, no importa si en la actualidad solo se utiliza una parte limitada de la información extraída de la fórmula del ADN y tampoco no se causa un daño inminente a la persona interesada. Los perfiles de ADN contienen un código de identificación único, que puede conducir a la individualización exacta del propietario, mediante un procesamiento automático y también tiene la capacidad de proporcionar información sobre las relaciones genéticas entre los individuos, incluida su etnia. Por estas razones el T.E.D.H. consideró en este caso que el estado (Reino Unido), al retener estos datos pertenecientes a menores sospechosos de cometer delitos, por períodos ilimitados de tiempo, excedió de manera arbitraria y desproporcionadamente los límites de una injerencia permitida por la Convención.

La integridad moral parece un concepto bastante difícil de comprender en una definición jurídica, estando sujeto a variables habituales o religiosas. El T.E.D.H. ha establecido que esta noción cae dentro del alcance del art. 8 de la Convención en el caso de la divulgación no autorizada de información de los antecedentes penales de una persona a terceros. Por otro lado, también se invocó la integridad moral contra el demandante, como una razón para rechazar su reclamo de compensación por un hecho por el cual actuó voluntariamente (relaciones sexuales con un adulto)[637].

[636] El texto es disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/5/2290/32.pdf
[637] August v. Reino Unido, asunto nº 36505/02, de 21 de enero de 2003

7.4.6. El derecho al honor

Ya mencionado anteriormente, al examinar el derecho a la imagen, el derecho al honor y a la reputación se prestó por la doctrina del derecho constitucional del derecho civil e incluso penal; de hecho, los autores del derecho civil francés criticaron el reconocimiento de esta nueva categoría de derechos, considerándolos, de hecho, solo una aplicación de las normas de responsabilidad civil. Se podría considerar que el origen del reconocimiento judicial de este derecho se remonta en Francia, entre 1897-1899, un período marcado por una serie de demandas presentadas contra algunos escritores como Emile Zola o Jules Verne, por personas que afirmaron haber encontrarse en las descripciones poco halagadores de los personajes en sus obras de ficción.

El derecho al honor se considera un derecho derivado del derecho a la vida privada y tiene como objetivo respetar la dignidad humana frente a los actos externos que pueden dañar la imagen de una persona a la vista del público. En una opinión, el derecho a la reputación figura como parte de la integridad física y mental de la persona, lo que generalmente interfiere con la libertad de expresión. Dado el valor intrínsecamente igual de los dos derechos fundamentales, tanto el poder legislativo como el poder judicial tienen la misión de garantizar un equilibrio justo en caso de conflicto entre el derecho a la reputación y la libertad de expresión[638]. En este sentido, el T.E.D.H. considera como violaciones del art. 8 de la Convención, la publicación en la prensa de algunas fotografías acompañadas de comentarios difamatorios[639], la acusación pública de una persona por ser parte de los cuerpos de represión de un antiguo estado totalitario.

---

[638] Peces-Barba Martínez, G. (1981) *Los derechos fundamentales en la cultura jurídica española*. Editorial: Universidad Complutense. Facultad de Derecho, Madrid, p. 227, recuperado de: https://e-archivo.uc3m.es/bitstream/handle/10016/10378/derechos_Peces_ADH_1981.pdf?sequence=1&isAllowed=y

[639] Asunto: *Vicent del Campo c. España* (25527/13) – "Profesor y jefe de servicio en la Escuela de Artes y Oficios de León, el Sr. Vicent del Campo fue acusado de acoso por una de sus compañeras. Al haber sido rechazada la queja de esta compañera que instaba la adopción de medidas administrativas, esta presentó una solicitud de responsabilidad patrimonial ante la Junta de Castilla y León. Ante el silencio de la Administración, instó en enero del 2007 una demanda ante la jurisdicción contencioso-administrativa. En noviembre de 2011, el Tribunal Superior de Justicia de Castilla y León se pronunció contra la Administración regional obligando a indemnizar a la compañera afectada. Consideró responsable a la Administración porque la demandante había sido víctima de acoso y las Autoridades competentes no habían hecho nada para impedirlo. La sentencia citaba en varias ocasiones el nombre del Sr. Vicent del Campo y estimaba había acosado y perseguido a su compañera. En diciembre de 2012, el Sr. Vicent del Campo solicitó acceder al expediente y ser parte en el procedimiento, aduciendo que había tenido conocimiento de la sentencia por la prensa local. Las jurisdicciones nacionales rechazaron su solicitud de ser parte debido a que sólo la Administración podía ser parte demandada en semejante caso, incluso si a título individual un funcionario podía ser identificado y su comportamiento juzgado. El recurso de amparo interpuesto por la demandante ante el Tribunal Constitucional fue inadmitido por falta de relevancia constitucional. El 2 de abril de 2013, Sr Vicente del campo interpuso una demanda ante el Tribunal Europeo de Derechos

Las garantías de respetar este derecho pueden ser civiles o penales, en algunos estados se incrimina la ofensa y la calumnia como delitos que perjudican la dignidad. La doctrina del derecho penal definió la dignidad desde dos puntos de vista: subjetivo (el sentimiento de aprecio que una persona tiene hacia si misma) y objetivo (la buena notoriedad, la reputación, la estima, la consideración que una persona disfruta por parte de los demás). La causa que excluye la existencia del delito e, implícitamente, la responsabilidad de la persona incriminada es la prueba de la verdad, por la que se demuestra que la afirmación o imputación de los hechos se cometió para defender un interés legítimo.

En España, el derecho al honor este expresamente regulado por el artículo 18.1. de la Constitución Española: "*Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen*". Pero el contenido y el alcance del derecho está regulado por la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad familiar y a la propia imagen. Previamente, la protección del honor de una persona estaba regulada solo por dos artículos del Código Civil, respectivamente el art. 1092 y el art. 1902.

Según el apdo. 3 del art. 1, Ley Orgánica 1/1982, "*el derecho al honor, a la intimidad personal y familiar y a la propia imagen es errenunciable, inalienable e imprescriptible*". Ningún acuerdo o declaración unilateral de a renuncia a la protección legal de este derecho serán válidos, excepto las situaciones previstas en el artículo dos de la ley, es decir las limitaciones impuestas por la ley o por usos sociales, como también cuando existe una autorización legal en este sentido.

Desde el momento de su consagración legislativa, el derecho al honor gozó de la protección del ordenamiento jurídico, siendo considerado por la doctrina como uno de los derechos clásicos de la personalidad. Su contenido y límites han sido ampliamente debatidos en la literatura, resultando varios significados de esta noción: el aspecto inmanente del derecho o la autoestima y el aspecto trascendente que supone reconocer o reflejar la autoestima en las relaciones con los demás, es decir, la fama social de un individuo. En este sentido se observa que el honor de una persona está vinculado a las

---

Humanos. En conjunto, el T.E.D.H. concluye que la injerencia en el derecho al respeto de la vida privada del Sr. Vicent del Campo no estaba debidamente justificada y que ha habido violación del artículo 8". Texto recuperado de: https://www.mjusticia.gob.es/gl/area-internacional/tribunal-europeo-derechos/jurisprudencia-tedh/asuntos-espana-sido-parte/convenio-europeo-derechos/articulo-derecho-vida-privada.

circunstancias sociales, históricas, temporales y geográficas de forma que el concepto cambia a menudo de forma y contenido, lo que antiguamente representaba una falta de respeto y una lesión para el honor de una persona, hoy en día, puede tener ningún impacto o significado sobre el tema[640].

La afectación del derecho al honor depende en gran medida de la estructura de personalidad del interesado, como también de su papel en la sociedad, su vida privada o profesional, porque las circunstancias personales pueden influir en gran medida sobre la gravedad de la lesión de la esfera de este derecho[641].

En Rumania, la consagración legislativa del derecho al honor se encuentra en el texto del art. 72 del Nuevo Código Civil, que establece en su primer párrafo que "toda persona tiene derecho al respeto a su dignidad", agregando en el segundo párrafo que "cualquier daño al honor y reputación de una persona, sin su consentimiento o sin cumplimiento de los límites previstos en el art. 75". El legislador se limita, por tanto, a la consagración del derecho a la dignidad, sin definir, este concepto, enfoque, por supuesto, problemático, dado que el objeto de tal derecho es, por su naturaleza, "irreductible a una definición precisa"[642].

En lo que concierne los límites establecidos por el legislador en el art. 75, mencionamos que las intrusiones permitidas por la ley o por los convenios y pactos internacionales de derechos humanos firmados por Rumania no constituyen una violación. Del mismo modo, el ejercicio de los derechos y libertades constitucionales de buena fe y de conformidad con los pactos y convenciones internacionales en los que

---

[640] STC 185/1989, de 13 de noviembre, Recurso de amparo 1422/87 interpuesto por don Manuel Peláez del Rosal, representado por don Luciano Rosch Nadal y asistido de Letrado, contra el Acuerdo del Pleno del Ayuntamiento de Priego (Córdoba);

[641] STC 46/2002, de 25 de febrero, Recurso de amparo 3251/98. Promovido por don Ramiro Grau Morancho frente a las Sentencias de la Sala de lo Civil del Tribunal Supremo y de la Audiencia Provincial de Madrid que, en un litigio de protección del derecho al honor, desestimaron su demanda por un artículo publicado en el diario «El País» sobre escritos anónimos; STC 20/2002, de 28 de enero. Recurso de amparo 4342/98. Promovido por don José Velasco Aroca frente a la Sentencia de la Sala de lo Social del Tribunal Superior de Justicia de Madrid que estimó parcialmente su demanda contra Caja Postal, S. A., y declaró improcedente su despido.; STC 204/2001, de 15 de octubre. Recurso de amparo 4022/98. Promovido por don José María García Pérez y Antena 3 Radio, S.A., respecto a la Sentencia de la Sala de lo Civil del Tribunal Supremo que, en grado de casación, confirmó su condena por intromisión ilegítima en el honor de don Ramón Mendoza Fontela en el programa de radio Supergarcía en la Hora Cero; STC 148/2001, de 27 de junio. Recurso de amparo 3377/97. Promovido por don Manuel Rincón Granados frente a las Sentencias de la Sala de lo Penal del Tribunal Supremo y de la Audiencia Provincial de Málaga que lo condenaron por delito de calumnias al secretario del Ayuntamiento de Vélez-Málaga.

[642] Matefi, R. (2019) *El derecho al honor en el contexto legislativo nacional e internacional y en la jurisprudencia correspondiente* (Dreptul persoanei la reputaţie, în contextul reglementărilor legale naţionale şi internaţionale şi a jurisprudenţei în materie), Revista Universul Juridic no.3, pp. 57-63.

Rumania es parte no puede constituir una violación de los derechos de otro. Es decir que el derecho de una persona a expresar su opinión, si está legalmente ejercitado, no puede infringir el derecho al honor de otra persona a quien se refiere.

El legislador establece también una presunción de acuerdo tácito de la persona a quien se refiere una determinada información o un determinado material, en la situación en la que esta misma persona pone a disposición de un periodista las informaciones sobre sí mismo. En tal caso, no se requiere un acuerdo por escrito de la persona afectada, porque debería saber que el periodista puede usar la información para informar al público.

7.4.7. El derecho al olvido

Pese a que no se reconoce como tal en muchos sistemas de derecho, el derecho al olvido (right to oblivion) ha encontrado su expresión en algunos casos juzgados por los tribunales internacionales, incluido el T.E.D.H. Por ejemplo, en Francia, el derecho a olvidar ha sido reconocido en el contexto del derecho legítimo de una persona condenada que ha expiado su sentencia, a reanudar su vida normal sin recordarle al público los hechos por los cuales fue juzgado en el pasado; su violación da lugar al derecho a obtener daños y perjuicios[643].

En un caso histórico, *Google España v. Costeja*, el Tribunal de Justicia de las Comunidades Europeas (TJCE) mencionó en su sentencia que un operador de motor de búsqueda en Internet es responsable del tratamiento de los datos personales que aparecen en páginas web publicadas por terceros. Por lo tanto, en determinadas circunstancias, las personas pueden solicitar a los motores de búsqueda que eliminen los enlaces a páginas web que contengan datos personales. En ese caso, el demandante, el Sr. Costeja, solicitó que los registros de una condena pasada se eliminaran de las entradas de búsqueda de Google como resultado de las búsquedas con el nombre de Costeja.

Como dice originalmente el T.J.U.E., los derechos del interesado "*anulan, por regla general, no solo el interés económico del operador del motor de búsqueda, sino también el interés del público en general en encontrar esa información en una búsqueda relacionada con el nombre del sujeto"*[644]. El derecho a solicitar la remoción de material, finalmente reconocido por el TJUE, se asemeja mucho al derecho francés al olvido, que

[643] Bertrand, A (1999*) Droit à la Vie Privée et Droit à l'Image*, Editorial Litec : Paris, p. 43
[644] Véase la nota 483.

permite a un individuo oponerse a la publicación de información sobre una condena después de que se haya cumplido la sentencia y se haya producido la rehabilitación. Sin embargo, las raíces del nuevo derecho al olvido se extienden mucho más allá del antiguo derecho francés al olvido y alcanzan controles y equilibrios más críticos previamente adoptados en la tradición europea de los derechos humanos.

En Francia, por iniciativa de la Comisión Nacional de Informática y Libertades, se ha creado un grupo de trabajo a nivel parlamentario que busca legislar el derecho al olvido en las operaciones realizadas en Internet. De acuerdo con estas regulaciones, los datos almacenados en la memoria de las computadoras deben destruirse después de un cierto tiempo, para que nunca se vuelvan a grabar[645]. El derecho al olvido permitirá evitar la situación en la que las personas son víctimas de las informaciones que permanecen (actualmente) en Internet por un período indefinido.

Poco después del caso Google España, el Parlamento Europeo adoptó el nuevo Reglamento General de Protección de Datos (RGPD), que incluye una disposición sobre el derecho al olvido (también conocido como derecho al borrado), con pasos específicos para que los responsables del tratamiento borren la información cuando lo soliciten. Además, de acuerdo con el artículo 18 del RGPD, conocido como "*derecho a la limitación del tratamiento*", el interesado "*tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos personales*". Cuando el procesamiento está limitado, los controladores de datos pueden almacenar los datos personales, pero no procesarlos más. El responsable del tratamiento debe hacer que los datos sean inaccesibles, en lugar de eliminarlos por completo como en el caso del derecho al olvido.

El interesado tiene derecho a la supresión en varias circunstancias específicas, incluso cuando "los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo" [646]. Por el contrario, el "a la limitación del tratamiento" se aplica de manera más estricta, entre otras cosas, a los casos en los que "*el interesado impugne la exactitud de los datos personales, durante un plazo que permita*

[645] Boizard, M. (2016) *Le temps, le droit à l'oubli et le droit à l'effacement*. Revista Les Cahiers de la Justice 2016/4 (N° 4), pp. 619 – 628.
[646] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), articulo 17. 1.a.

al responsable verificar la exactitud de estos". La limitación debe ocurrir inmediatamente después de la solicitud del interesado y durar "por un plazo que permita al responsable verificar la exactitud de los datos".

Mientras tanto, han aparecido varias propuestas legislativas similares sobre un derecho al olvido en varias jurisdicciones, incluidas Argentina, Brasil, Chile, Colombia, México, Nicaragua, Japón, Corea del Sur y Hong Kong. En particular, en julio de 2015, Rusia fue el primer país en firmar un proyecto de ley que codificaba el derecho al olvido. El reconocimiento por parte de la Unión Europea del derecho al olvido ha provocado reacciones negativas por parte de los juristas en los Estados Unidos y en otros lugares. Los escépticos argumentan que el derecho al olvido pone en peligro la libertad de expresión y el acceso a la información, que según los más preocupados críticos podría poner en peligro la historia de la humanidad[647].

El debate sobre la necesidad de encontrar un equilibrio entre la privacidad y la libertad de expresión se ha convertido en una lucha sin ganadores, especialmente en el entorno en línea. Según un comunicado sobre periodismo abierto de la Organización para la Seguridad y Cooperación en Europa, "la necesidad legítima de proteger la privacidad y otros derechos personales no deben socavar el papel principal de la libertad de los medios de comunicación y el derecho a buscar, recibir y difundir información de interés público como condición básica para la democracia y la participación política"[648]. Además, enfoques internacionales diversos y opuestos siguen polarizando constantemente el debate.

En Europa, el derecho al olvido ha sido reconocido desde hace mucho tiempo, al menos mientras los tribunales europeos han reconocido el derecho a la autodeterminación informativa. El término autodeterminación informativa se utilizó por primera vez en el contexto de una sentencia constitucional alemana relacionada con la información personal recopilada durante el censo de 1983. El término alemán es "informationelle Selbstbestimmung". En esa ocasión, el Tribunal Constitucional Federal de Alemania dictaminó que: "*Este derecho básico garantiza la capacidad de la persona*

[647] King, G. (2014) *EU 'Right to be Forgotten' Ruling Will Corrupt History*. Recuperado de: https://cpj.org/2014/06/eu-right-to-be-forgotten-ruling-will-corrupt-histo/

[648] OSCE. The Representative on Freedom of the Media Dunja Mijatović (2016) Communiqué No.1/2016. 3rd Communiqué on Open Journalism, recuperado de: https://www.osce.org/files/f/documents/5/8/219391.pdf

para determinar, en principio, la divulgación y el uso de sus datos personales. Las limitaciones a esta autodeterminación informativa se permiten solo en caso de un interés público primordial"[649].

Durante las primeras etapas de la sociedad de la información, Europa decidió evitar la aparición de modelos de negocio basados en la explotación de la "miopía de la privacidad". Como dice el profesor Fromkin[650], la miopía de la privacidad podría llevar a la muerte de la privacidad porque las personas han estado renunciando a su privacidad poco a poco al revelar sus datos con demasiada frecuencia y de forma demasiado barata. En ese momento, Fromkin pensó que no todo estaba perdido, pero eso fue hace mucho tiempo. Luego vino Facebook y la NSA. A diferencia de Europa, otras jurisdicciones de todo el mundo respaldaron diferentes estrategias políticas que conducen al crecimiento imparable de empresas que han prosperado gracias a la miopía de la privacidad. Existe una suposición equivocada de que "*Europa está exportando la censura a todo el mundo*". En realidad, el debate sobre el derecho al olvido tiene que ver con la protección de datos frente a intereses económicos en lugar de la protección de datos frente a la libertad de expresión. Deben descartarse las percepciones erróneas sobre el alcance del derecho al olvido, en particular las cuestiones sobre si el fallo del T.J.C.E. y los acontecimientos posteriores no tomaron en consideración la libertad de expresión[651]. Además, el equilibrio entre el derecho al olvido y los derechos en competencia proviene del Reglamento General de Protección de Datos recientemente promulgado.

En particular, la disposición sobre el derecho al olvido, artículo 17, establece que la obligación del responsable del tratamiento no se aplicará en la medida en que el tratamiento de datos sea necesario "para ejercer el derecho a la libertad de expresión e información". La misma disposición no se aplicará si el procesamiento es necesario "para fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos" en la medida en que el derecho al olvido "pueda hacer imposible o perjudicar gravemente el logro de los objetivos de ese procesamiento".

[649] *BVerfGE 65, 1 vom 15.12.1983 (Volkszahlungs-Urteil)*.
[650] Froomkin, A. M. (2000) *The Death of Privacy?* Standford Law Review 52/5, recuperado de: https://cyber.harvard.edu/privacy/Fromkin_DeathOfPrivacy.pdf
[651] Frosio, G. F. (2017) *The Right to Be Forgotten: Much Ado About Nothing*. SSRN Electronic Journal. 10.2139/ssrn.3009153.

Además, la "excepción de los medios de comunicación" del GDPR parece sustancialmente más amplia que su equivalente en la Directiva de Protección de Datos anterior. La excepción ya no se limita al procesamiento de datos "realizado únicamente con fines periodísticos o con fines de expresión artística o literaria". Más bien, la excepción apunta de manera más general a reconciliar los derechos de protección de datos con "el derecho a la libertad de expresión e información, incluido el procesamiento de datos personales con fines periodísticos y de expresión académica, artística o literaria".

Finalmente, en el caso del "a la limitación del tratamiento", que fue calificado recientemente por el GDPR como se mencionó anteriormente, el controlador debe restringir el procesamiento y, por lo tanto, hacer que los datos sean inaccesibles inmediatamente después de la reclamación, y "durante un período que permita el responsable del tratamiento para verificar la exactitud de los datos personales". De hecho, el legislador ha introducido una disposición que logró un equilibrio a favor de la privacidad al restringir preventivamente el acceso al contenido, en espera de la verificación de su exactitud.

Los efectos paralizantes sobre la libertad de expresión deberían ser limitados. En primer lugar, este es un escenario más restringido e intrínsecamente diferente que el derecho al olvido o al borrado porque solo se aplica a los casos en los que se cuestiona la exactitud de los datos personales. En segundo lugar, la restricción de acceso a los datos cuya precisión se cuestiona debería ser bastante breve. De acuerdo con el GDPR, la restricción debe levantarse tan pronto como los controladores de datos realicen la verificación de la exactitud de los datos. Esto debería ocurrir en el mismo intervalo de tiempo que, el tiempo de procesamiento de las solicitudes del derecho al olvido, que se ha reducido cada vez más en los últimos dos años a menos de 20 días por solicitud.

7.5. Los sujetos activos y pasivos del derecho a la vida privada

La cuestión de los temas legales relacionados con el respeto de un derecho fundamental puede abordarse desde dos perspectivas[652]: la de los titulares o los beneficiarios del derecho (sujeto activo) y la de los *obligados* del derecho (sujeto pasivo).

En la primera categoría, en virtud del principio de universalidad, pueden registrarse tanto las personas físicas (ciudadanos, extranjeros o apátridas), como las

[652] Favoreu, L. y otros (2008) „*Droit constitutionnel*", Editorial : Dalloz, Paris, 11e édition.

personas jurídicas (de derecho público o privado). Sin embargo, también existen derechos fundamentales que deben ser ejercidos exclusivamente por las personas físicas (el derecho a la vida, por ejemplo) o exclusivamente por los ciudadanos de un estado (el derecho a ser elegido en las más altas dignidades públicas) o por los extranjeros o apátridas (derecho de asilo).

Los sujetos pasivos de los derechos fundamentales son, ante todo, las autoridades, como representantes del poder estatal que tiene la obligación negativa de abstenerse de violar un derecho, pero también la obligación positiva de adoptar medidas legislativas o administrativas que permitan el libre ejercicio de un derecho[653]. En segundo lugar, los sujetos pasivos son las otras personas físicas o jurídicas[654] con quienes el titular de un derecho fundamental desarrolla relaciones legales y que también tienen obligaciones principalmente negativas, de no producir intromisiones que no estén permitidas en el ejercicio del derecho.

Teóricamente, es posible distinguir entre los titulares y los beneficiarios de un derecho fundamental, en el sentido de que el titular tiene una prerrogativa en su propio beneficio o del otro, mientras que el beneficiario del derecho se convierte en un objeto de la norma legal, incluso sin ser titular del derecho respectivo, según la opinión de algunos autores[655].

Con respecto a la dignidad humana, si bien, es difícil hacer una distinción entre los aspectos subjetivos y objetivos, ya que la persona humana es considerada tanto titular como beneficiaria de los derechos que surgen de este principio con valor constitucional. Como manifiestan algunos autores españoles, "*la mera adquisición de la personalidad es, conforme al artículo 10.1 de la Constitución Española, el único requisito para la posesión de dignidad y para el disfrute de la capacidad jurídica iusfundamental a ella anudada, que, en ese sentido, vendría a identificarse con la capacidad para ser titular de los derechos inviolables que le son inherentes"*[656].

---

[653] Villaverde Menéndez, I.; Requejo Rodríguez, P; Aláez Corral, B.; Fernández Sarasola, I; Bastida Freijedo, F.J.; Presno Linera, M.A. (2004) *Teoría general de los derechos fundamentales en la Constitución española de 1978*, Editorial Tecnos, Madrid, Capitulo 4, pág. 83.

[654] Por ejemplo, según el artículo 12 de la Constitución portuguesa, el principio de la universalidad incluye las personas jurídicas entre los beneficiarios: "*Todos los ciudadanos gozan de los derechos y están sujetos a los deberes que se consignan en la Constitución. 2. Las personas colectivas gozarán de los derechos y los deberes compatibles con su naturaleza*".

[655] Bioy, X. (2011) *Droit constitutionnel, bioéthique et vie privée.* Recueil des cours de l'Académie Internationale de Droit Constitutionnel, 17. pp. 103-178.

[656] Villaverde Menéndez, I.; Requejo Rodríguez, P; Aláez Corral, B.; Fernández Sarasola, I; Bastida Freijedo, F.J.; Presno Linera, M.A. (2004) *idem.*, pág. 84

Como ya hemos analizado, el derecho a la vida privada se considera en la mayoría de los sistemas de derecho un derecho fundamental y por esta razón, los titulares-beneficiarios de este derecho son las personas físicas, en primer lugar. Es el caso de Alemania, las personas jurídicas de derecho público están excluidas del beneficio de este derecho, ya que el Estado no puede ser al mismo tiempo sujeto pasivo y beneficiario de los derechos fundamentales. En los últimos años, tanto los tribunales nacionales, como el T.E.D.H.[657] comenzaron a mostrar una marcada tendencia hacia el reconocimiento de ciertos componentes de este derecho y en favor de las personas jurídicas. Este reconocimiento es evidente especialmente en los casos que tienen como objeto uno de los atributos de identificación - el domicilio, respectivamente, la sede en el caso de las personas jurídicas. En este asunto, los dos tribunales supranacionales (Luxemburgo y Estrasburgo) inicialmente tenían opiniones diferentes, en el sentido de que el T.E.D.H. también otorgó protección a las personas jurídicas, a diferencia de la corte a nivel de la UE[658].

El cambio de esta visión ocurrió en el año 2002, con la decisión de T.J.U.E. en el caso Roquette[659], donde se alineó con la línea impuesta por el T.E.D.H. en el mismo año, por la sentencia del caso Société Colas Est. Consecuentemente, la interpretación dada a la noción de "domicilio" en casos relacionados con la aplicabilidad del artículo 8 del Convenio también incluye la de la oficina registrada de las personas jurídicas de derecho privado o de agencias u oficinas profesionales de éstas.

En Francia, la práctica del Consejo Constitucional es admitir la existencia de algunos derechos fundamentales también en el caso de personas jurídicas de derecho público (autoridades territoriales, partidos políticos) o privado (sindicatos, empresas, fundaciones), hecho por el cual en la doctrina se apreció que el derecho a la vida privada debe ser reconocido a su favor. Sin embargo, con respecto al derecho a la imagen, como un elemento del derecho a la vida privada, debido a la conexión intrínseca entre este derecho y la esfera íntima del individuo y su dignidad, dicho derecho solo puede admitirse en beneficio de las personas físicas (no de las jurídicas)[660].

---

[657] T.E.D.H. sentencia de 16 de diciembre de 1992, Niemietz c. Alemania, 13710/88, apdos. 29 y 31; sentencia de 16 de abril de 2002 Colas Est y otros c Francia, 37971/91).

[658] El TJUE consideraba en el asunto Hoescht que el domicilio empresarial no se incluía dentro del ámbito de protección del derecho al respeto del domicilio familiar recogido en el artículo 8 C.E.D.H. (TJUE sentencia de 21 de septiembre de 1989, Hoescht c. Comisión, ECLI: EU: C: 1989: 337, apdo. 17; sentencia de 17 de octubre de 1989, Dow Benelux c. Comisión, ECLI: EU: C: 1989: 379, apdo. 28).

[659] TJUE sentencia de 22 de octubre de 2002, Roquette Frères, ECLI: EU: C: 2002:C: 603, apdo. 29

[660] Burgorgue-Larsen, L. (2012) *La convention européenne des droits de l'homme*, Editorial LGDJ Paris.

En España, el derecho al honor de las personas jurídicas ha sido reconocido por la doctrina y la jurisprudencia constitucional (véase en este sentido la STC 139/1995, de 26 de septiembre, FJ 5[661]), pero el Tribunal Constitucional o ha tenido la misma opinión sobre el derecho a la vida privada de las empresas. En un debate sobre la existencia del derecho a la inviolabilidad del domicilio de la persona jurídica y sus garantías procesales, el Tribunal constitucional fallo que las empresas y otras organizaciones similares carecen de este derecho y no pueden ser amparadas por la garantía de la inviolabilidad domiciliaria reconocida en el art. 18.2 CE: "*el núcleo esencial del domicilio constitucionalmente protegido es el domicilio en cuanto morada de las personas físicas y reducto último de su intimidad personal y familiar. Si bien existen otros ámbitos que gozan de una intensidad menor de protección, como ocurre en el caso de las personas jurídicas, precisamente por faltar esa estrecha vinculación con un ámbito de intimidad en su sentido originario; esto es, el referido a la vida personal y familiar, sólo predicable de las personas físicas*" (la STC 69/1999, de 26 de abril, FJ 2)[662].

Aunque las personas jurídicas pueden invocar la garantía constitucional mencionada en el art. 18.2 CE, usando una interpretación del sede social visto como domicilio de la empresa, los jueces constitucionales niegan la existencia de un derecho a la intimidad puro de las personas jurídicas, motivando que este derecho deriva del derecho a la vida personal y familiar[663], una noción incompatible con la naturaleza jurídica de la persona jurídica.

Los titulares y beneficiarios del derecho a la vida privada pueden ser ciudadanos de un estado, así como ciudadanos extranjeros y apátridas, siendo reconocidos equitativamente, sin discriminación, a todas las personas, independientemente de su raza, nacionalidad, origen étnico, idioma, religión, sexo, opinión, pertenencia política, riqueza

[661] Sentencia 139/1995, de 26 de septiembre (BOE núm. 246, de 14 de octubre de 1995) ECLI:ES:TC:1995:139: "La compañía mercantil Lopesan Asfaltos y Construcciones, S.A. interpuso demanda en procedimiento especial de protección jurisdiccional civil del derecho fundamental al honor contra los ahora recurrentes en amparo Ediciones Zeta, S.A. La demandante entendía que, en un artículo publicado por Ediciones Zeta, S.A. se le realizaban una serie de imputaciones absolutamente falsas que implicaban una intromisión ilegítima en sus derechos al honor y a la imagen. Los demandados se opusieron a la demanda alegando varias excepciones de forma y de fondo; en concreto, y entre las mismas, se alegó la falta de legitimación activa de la actora y la inadecuación del procedimiento, al entender que las personas jurídicas no tienen honor como derecho de la personalidad amparado en el art. 18 C.E., sino que merecen protección por lo que establece el art. 38 del mismo texto".

[662] Sentencia 69/1999, de 26 de abril, (BOE núm. 130, de 01 de junio de 1999), ECLI:ES:TC:1999:69.

[663] EPRS - Servicio de Estudios del Parlamento Europeo, Pedro González-Trevijano Sánchez (2018) *El derecho al respeto de la vida privada: los retos digitales, una perspectiva de derecho comparado*, Unidad Biblioteca de Derecho Comparado, Recuperado de:
https://www.europarl.europa.eu/RegData/etudes/STUD/2018/628260/EPRS_STU(2018)628260_ES.pdf

u origen social. El lenguaje utilizado por la C.E.D.H. se refiere al reconocimiento del derecho a la vida privada y familiar a favor de cualquier persona bajo la jurisdicción de los Estados signatarios de la Convención. Asimismo, la Carta de los Derechos Fundamentales de la Unión Europea establece a favor de cualquier persona el derecho a la vida privada, a los ciudadanos de la U.E. están reservados exclusivamente los derechos políticos y, con algunos matices, el derecho al trabajo. En el caso del derecho de petición o el derecho a una buena administración, por ejemplo, sus titulares pueden ser ciudadanos europeos, así como otras personas físicas o jurídicas que residan o tengan su sede en el territorio de un Estado miembro.

En Francia, el reconocimiento del derecho a la vida privada y en favor de otros individuos fuera de los ciudadanos franceses se ha logrado a través de la jurisprudencia. En la Resolución número 93-325 DC de 13 de agosto de 1993, del Consejo constitucional ha declarado inconstitucionales las disposiciones del artículo 23 de la Ley de control de la inmigración y condiciones de entrada, recepción y estancia de extranjeros en Francia: "*Los extranjeros que residen en Francia bajo la apariencia de un permiso de residencia marcado como estudiante no pueden beneficiarse de la reunificación familiar",* y las palabras: *"Cuando el matrimonio entre un extranjero residente en Francia y su cónyuge que ha sido admitido permanecer como miembro de la familia ha sido disuelto o anulado al final de un procedimiento legal, este extranjero no puede traerle un nuevo cónyuge bajo la reunificación familiar hasta dos años después de la disolución o nulidad matrimonial*";

En los Estados Unidos, la ley sobre el derecho a la privacidad (1974)[664] define el término "individuo" (art. 552a) en el sentido del ciudadano de los Estados Unidos o de un extranjero que ha sido admitido a la residencia permanente en el territorio de este estado, de acuerdo con la ley. Luego, la ley estadounidense excluye del beneficio del derecho a la vida privada a otras personas, ciudadanos de terceros países o apátridas, que no residen legalmente en los EE. UU.

La dicotomía pública-privada también se aplica en el ámbito de los sujetos de derecho, titulares del derecho a la vida privada. Como hemos presentado más arriba, las personas públicas, aunque no pueden ser privadas del ejercicio de este derecho, están sujetas a limitaciones naturales, debido a su calidad. Estas limitaciones están impuestas

[664] The Privacy Act of 1974: 552 (a) the term "individual" means a citizen of the United States or an alien lawfully admitted for permanent residence.

por el requisito de transparencia en el ejercicio de una función pública, una condición necesaria en algunos casos incluso antes del nombramiento o elección en el cargo o dignidad respectiva. Así, por ejemplo, para la admisión de la candidatura en algunos puestos se requiere una buena reputación cívica (aunque como condición sine qua non, no todos los estados realmente proceden a verificar y tener en cuenta este criterio). Los límites y las restricciones impuestas sobre el contenido del derecho a la vida privada difieren según el momento del nombramiento/elección, siendo más estrictos durante el mandato, cuando están *bajo la mirada* de la opinión pública, los votantes y los medios de comunicación[665].

En la doctrina francesa se hace una distinción entre las "personas públicas por su naturaleza", cuya imagen y vida "pertenecen a la historia contemporánea" (dignatarios, funcionarios, pero también varias celebridades artísticas o deportivas) y "personas públicas por casualidad" que están en la atención pública debido a hechos en los que están involucradas accidentalmente (por ejemplo, delincuentes o sospechosos de cometer actos con un eco público, emocional, a menudo importante)[666]. Las personas en la segunda situación se benefician del "derecho al olvido", tan pronto como cesa su participación en eventos públicos, cuando se convierten en personas exclusivamente privadas. Recordando en este contexto la teoría de las esferas de las que hablamos anteriormente, se puede argumentar que a las personas públicas se le reconoce un derecho abierto e inequívoco a la vida íntima y privada, cuando su vida familiar, sus propias creencias o creencias religiosas están involucradas, o "la intimidad de la vida privada".

El alcance de la protección legal otorgada al derecho a la vida privada no está temporalmente limitado, teniendo en cuenta que los elementos de este derecho, como la integridad física, pueden comenzar desde el momento de la concepción, desde la fase embrionaria y otros, como el derecho a la imagen o el derecho a disponer del propio cuerpo (la donación de órganos, incineración, etc.) continúa después de la muerte de la persona. Una de las cuestiones planteadas por la jurisprudencia y la doctrina se refiere a la calidad del titular del derecho a la vida privada de las personas fallecidas (incluso si a primera vista sería una contradicción de términos). A pesar de las opiniones divergentes en este asunto, existe, sin embargo, una opinión mayoritaria sobre el reconocimiento del

[665] Gómez Montoro, Á. (2001) *Titularidad de derechos fundamentales», en Manuel Aragon Reyes (coord.), Temas de Derecho Constitucional*, t. III (Tribunal Constitucional y derechos fundamentales, Editorial Cívitas, Madrid, pp. 116 ss.
[666] Bertrand, A. (1999) *Droit à la vie privée et droit à l'image*, Editorial Litec.

derecho al honor y el derecho a la imagen, un derecho no transferible no patrimonial, pero que da legitimidad a la voluntad expresada por los herederos de algunas personas para defender este derecho en los tribunales, para reparar el daño de "imagen".

El Nuevo Código Civil rumano, por ejemplo, admite un respeto equivalente por el cuerpo y la memoria de la persona fallecida, en condiciones iguales a la protección de la imagen y la reputación de una persona viva (artículos 78 y 79). Por otro lado, el T.E.D.H. no admitió que se tratara de una violación del art. 8 de la Convención la exhumación y el análisis del ADN de un cadáver, considerando que no se puede hablar de un "*derecho a la vida privada del difunto*"[667].

Como hemos mostrado en las consideraciones iniciales de esta sección, los sujetos de derecho relacionados con el respeto del derecho a la vida privada pueden clasificarse en dos categorías: los sujetos de derecho activo, respectivamente, los beneficiarios del derecho y los sujetos pasivos de derecho, es decir, las personas a quienes corresponde la obligación de respetar el derecho a la vida privada de los primeros, quedando así restringidos por el poder público. En esta segunda categoría están las autoridades (dentro de los "efectos verticales" producidos por los derechos fundamentales[668]), pero también las personas jurídicas de derecho privado y las personas físicas (dentro de los "efectos horizontales indirectos" producidos por los derechos fundamentales que "irradian" en todas las ramas del derecho, también las del derecho privado)[669]. La admisión de efectos horizontales en relación con el derecho a la vida privada se verifica en el caso de disputas que surjan del incumplimiento del derecho a la imagen o al honor y la reputación, en el que las partes son particulares, ya sean personas jurídicas (por ejemplo, publicaciones) u otras personas físicas.

Los sujetos pasivos están sujetos principalmente a obligaciones negativas, pero también positivas. Por lo tanto, la regla básica establecida en relación con la protección del derecho a la vida consiste en la posibilidad de revelar ciertos hechos relacionados con la vida privada solo con el consentimiento del titular de este derecho, expreso o tácito. Por lo tanto, los demás sujetos de derecho tienen la obligación de abstenerse de realizar

[667] T.E.D.H., Sentencia de 15 de mayo 2006, demanda no. 1338/03, Kresten Filtenborg Mortensen v. Denmark.
[668] Sentencia del Tribunal Constitucional Español no. 101/1983, 13 de noviembre y Sentencia no. 18/1994, 7 de febrero.
[669] Sentencia del Tribunal Constitucional Español no. 80/1982, 20 de diciembre.

actos o acciones que puedan afectar la esfera de la vida privada de una persona, en ausencia del acuerdo de voluntad expresado por él o de una obligación legal[670].

La forma de regular el derecho a la vida privada a nivel constitucional y convencional implica esencialmente la obligación negativa de parte de las autoridades competentes de abstenerse de cualquier acto o acción que pueda socavar el derecho a la vida privada[671]. De la jurisprudencia de los tribunales nacionales resultó que el estado también tiene obligaciones positivas (los sujetos de las autoridades estatales tienen la obligación de actuar en el sentido de adoptar medidas legislativas y administrativas que creen el marco jurídico apropiado para el libre ejercicio del derecho a la vida privada).

Asimismo, el T.E.D.H., en su jurisprudencia constante, reconoció, a través de la interpretación teleológica del término "cumplimiento" en el párrafo 1 del Artículo 8, la existencia incluso de algunas obligaciones positivas (que hacer) que los estados deben cumplir, en el significado de la adoptar expresamente medidas razonables y adecuadas, teniendo como objetivo la protección efectiva del derecho a la vida privada y familiar, a través de un marco jurídico adecuado y suficiente[672]. El objetivo por alcanzar respetando el art. 8 de la Convención es garantizar la protección efectiva de las personas contra cualquier injerencia arbitraria de los poderes públicos de un estado.

En el caso extremo del incumplimiento de las obligaciones de estos sujetos pasivos, la realización efectiva del derecho a la vida privada está garantizada por medios judiciales (un aspecto que se analizará a continuación). Por otro lado, los beneficiarios de este derecho también tienen la obligación de ejercer su derecho sin exceder los límites permitidos por la ley, con respecto al orden público, las buenas costumbres o los derechos y libertades de los demás[673].

---

[670] Aguila-Real, J. A. (1993) *Autonomía privada y derechos fundamentales*. Anuario de derecho civil, ISSN 0210-301X, Vol. 46, Nº 1, págs. 57-122

[671] Peces-Barba Martínez, G. (1993) *Derecho y derechos fundamentales*. Madrid: Centro de Estudios Constitucionales.

[672] Bogdan, D. y Selegean, M. (2005) *Drepturi şi libertăţi în jurisprudenţa Curţii Europene a Drepturilor Omului (Derechos y libertades en la jurisprudencia del Tribunal Europeo de Derechos Humanos),* Editorial All Beck Publishing House, Bucarest, pág. 366;

[673] Azpitarte Sánchez, M. (2015) *Los derechos fundamentales de la Unión en busca de un nuevo equilibrio*, Revista Española de Derecho Constitucional n.º 104/2015, pp. 243-268;

7.6. El derecho a la vida privada y otros derechos fundamentales

Como hemos visto anterior, el derecho a la vida privada goza de una protección jurídica efectiva en el sistema legal internacional, regional y de los estados modernos. La doctrina sigue analizando sus elementos en conexión con la realidad sociocultural de nuestro continente que cambia de una década a otra. Al mismo tiempo, las disposiciones constitucionales de algunos estados, así como las disposiciones de algunos convenios internacionales en el campo de los derechos humanos, suman al derecho a la vida privada otros derechos complementarios, a través de disposiciones unitarias o distintas, como el derecho a la vida familiar, la inviolabilidad del domicilio o el secreto de la correspondencia.

En el campo de la aplicación efectiva de la ley, hay situaciones en las que la protección legal que se atribuye al derecho a la vida privada debe acordarse con otros derechos igualmente significativos o incluso con un mayor valor social, con referencia particular a la libertad de expresión o con el derecho a la información. Para comprender el impacto de las medidas de seguridad cibernética sobre los derechos humanos fundamentales a continuación, analizaremos el proceso de transformación de la vida privada de una persona bajo la influencia del desarrollo tecnológico a nivel global.

Algunos autores[674] opinan que el derecho a la vida privada incluye casi todos los derechos humanos, pero se necesita un análisis separado sobre las correlaciones identificadas entre este derecho y otros derechos fundamentales igualmente importantes, como: el derecho a la vida familiar, el secreto de la correspondencia o la inviolabilidad del domicilio. El derecho a la vida privada es el que asegura una garantía legal efectiva de estos derechos, es decir que estos derechos no pueden considerarse protegidos si este derecho está limitado por algunos actos con carácter intrusivo en la vida privada de una persona.

De acuerdo con el artículo 8 del C.E.D.H. y las interpretaciones de las normas constitucionales de algunos estados miembros, el contenido del derecho a la vida privada está conectado con el contenido de otros derechos:

> *"1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.*

[674] García Moriyon, F. (1983): *Enseñar los derechos humanos*. Editorial: Zero Madrid.; Arbós, T. y otros. (1998): *Los fundamentos de los derechos humanos desde la filosofía y el derecho*. Editorial EDAI, Barcelona.

2. No podrá haber injerencia de la autoridad en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

En algunas situaciones aparece la necesidad de elegir entre el derecho a la privacidad y otros derechos, como la libertad de expresión, la libertad de conciencia o el derecho a la información. En estas situaciones, el legislador o, según el caso, el juez tiene la tarea de determinar, para cada caso determinado, a qué derecho fundamental se le puede otorgar preeminencia. En este contexto analizaremos estos derechos, clasificados en dos niveles: los derechos complementarios al derecho a la privacidad, que por lo tanto convergen en la protección legal de los valores comunes y los derechos opuestos al derecho a la privacidad, ya que la realización de algunos excluye el ejercicio completo del otro.

7.6.1. Derechos complementarios al derecho a la privacidad

7.6.1.1. El derecho a la vida familiar

Este derecho protegido por todas las constituciones de los estados está también enmarcado por el C.E.D.H. en el contexto del derecho a la privacidad provisto por el art. 8, junto con el respeto del domicilio y la correspondencia. Al mismo tiempo, el artículo 7 de Carta de los derechos fundamentales de la Unión Europea, intitulado "*Respeto de la vida privada y familiar*" enuncia que: *"*Toda *persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones*".

Esta forma de regulación común del derecho a la vida privada y familiar también es común para diferentes constituciones nacionales de los estados europeos (por ejemplo: Bélgica, España, Rumania). La doctrina francesa[675] ha identificado tres componentes del derecho a la vida familiar: el derecho a establecer una familia (implica el derecho a casarse entre personas de diferente sexo, pero también la prohibición de la poligamia o el matrimonio ficticio), el derecho a vivir en la familia (reconocido en la jurisprudencia del Consejo Constitucional francés, pero también en la del T.E.D.H., incluso en el caso de inmigrantes que desean reunir a su familia) y el derecho a respetar la privacidad de la vida

[675] Favoreu, L. y otros (2008) *Droit constitutionnel*, Editorial : Dalloz, Paris, 11e édition

familiar (interfiere con el derecho al secreto, el derecho a oponerse a la captura y divulgación de imágenes o información íntima, sorprendido desde dentro de la vida familiar).

Las decisiones del T.E.D.H. sobre el derecho a la vida familiar han reconocido el derecho a respetar la decisión de ser o no el padre de un niño dentro o fuera del matrimonio, así como los derechos específicos a favor de los padres o hijos, en casos que involucren, entre otros, confiar a los menores[676], su adopción[677], reunir a los padres con sus hijos[678], el derecho de herencia[679].

La jurisprudencia de la Corte Suprema de los Estados Unidos ha sostenido que el derecho a usar anticonceptivos pertenece a la privacidad de la vida familiar y debe protegerse adecuadamente. En el caso *Griswold vs. Connecticut* se invocó el derecho a la vida privada de las personas casadas para pedir la anulación de una ley que prohibía la anticoncepción.

La jurisprudencia ulterior intentó ampliar el contenido de derecho fundamental, y con el caso *Roe vs. Wade*[680], se creó el precedente que conecta definitivamente el derecho de privacidad con la cláusula de debido proceso previsto en la decimocuarta enmienda[681]. La Corte Suprema introduce el derecho a la vida familiar en la categoría de derechos fundamentales y requiere una justificación motivada por razones de seguridad nacional a la hora de limitar de su alcance o para autorizar injerencias de las autoridades en la vida familiar de una persona. En el caso Roe se demostró que el interés del estado en evitar el aborto y proteger la vida de la madre era más importante que su autonomía personal únicamente después de que el feto fuese viable. Según la Corte, si no se puede probar la viabilidad del feto, la intervención del estado queda limitada por el derecho fundamental a la privacidad de la madre porque no se puede demonstrar que existe otro interés prioritario.

---

[676] T.E.D.H., Sentencia de 6 de abril de 2010, Caso Mustafa y Armağan Akin c. Turquía (núm. 4694/03).
[677] T.E.D.H., Sentencia de 22 de junio de 2004, Caso Pini y otros c. Rumania (núm. 78028/01 y 78030/01)
[678] T.E.D.H., Sentencia de 26 de febrero de 2006, Caso Kutzner c. Alemania (núm. 46544/99)
[679] T.E.D.H., Sentencia de 13 de junio de 1979, Caso Marckx c. Bélgica (No 6833/74)
[680] Corte Suprema de los Estados Unidos Caso Roe v. Wade, 410 U.S. 113 (1973)
[681] La enmienda provee una amplia definición de ciudadanía nacional, que anula la decisión de *Dred Scott v. Sandford* (1857), que había excluido a los esclavos y sus descendientes, de poseer derechos constitucionales. Se requiere que los estados ofrezcan una protección igualitaria ante la ley para todas las *personas* (no solo a los *ciudadanos*) dentro de sus jurisdicciones. La importancia de la Decimocuarta Enmienda fue ejemplificada cuando se interpretó para prohibir la segregación racial en los colegios públicos en el caso *Brown v. Board of Education.*

El juez constitucional español y profesor Pedro González-Trevijano Sánchez, sostiene que "*el derecho a la intimidad familiar reconocido en el art. 18.1. de la Constitución Española no incorpora la faceta propia del derecho a la vida familiar que reconoce el citado art. 8.1*"[682]. indicado que, según doctrina del T.E.D.H., correspondería como uno de sus elementos fundamentales, al "*disfrute por padres e hijos de su mutua compañía*"[683].

A diferencia del caso de la vida privada, la doctrina constitucional española no ha ofrecido una definición clara del concepto de vida privada familiar o intimidad familiar, aspecto que demuestra que el Tribunal Constitucional no haya identificado con claridad los aspectos relacionados con este derecho a la hora de analizar y fallar sobre determinados supuestos sometidos a su enjuiciamiento. Por ejemplo, en la STC 115/2000, de 5 de mayo, FJ 5[684], El Tribunal consideró que la elaboración y presentación pública de un reportaje sobre la familia y el hogar de una persona pública, usando datos con carácter personal ofrecidos por una antigua empleada, representa una intromisión no autorizada en la vida familiar del sujeto. En el artículo de la revista se presentaron informaciones confidenciales sobre las relaciones de familia, sobre bienes y recursos económicos, sobre la vida de los hijos menores, aspectos considerados por el Tribunal como invasivos para la intimidad familiar.

El problema de la violación de la intimidad familiar fue tratado también en el ámbito tributario, donde a base de la antigua Ley 44/1978, existía una obligación legal de los cónyuges a presentar una declaración del Impuesto sobre la Renta de las Personas Físicas (IRPF) única y conjunta. La vulneración se producía cuando uno de los esposos no acordaba con la publicación de sus ingresos por parte de su pareja u ofrecía datos financieros incorrectos. En este caso, el cónyuge "correcto" tenía la obligación de

---

[682] Trevijano Sánchez, P.G. (2018) *El derecho al respeto de la vida privada: los retos digitales, una perspectiva de derecho comparado*, EPRS-Servicio de Estudios del Parlamento Europeo, Unidad Biblioteca de Derecho Comparado, pág. 37, Recuperado de: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/628260/EPRS_STU(2018)628260_ES.pdf.

[683] Sentencia T.E.D.H. en el caso Johansen, de 27 de junio de 1996; SSTC 236/2007, de 7 de noviembre, FJ 11; SSTC 60/2010, de 7 de octubre, FJ 8 c; y SSTC 186/2013, de 4 de noviembre, FJ 6;

[684] Sentencia 115/2000, de 5 de mayo (BOE núm. 136 de 07 de junio de 2000): "Recurso de amparo 640-1997 promovido por doña María Isabel Preysler Arrastia frente a la Sentencia de la Sala Primera del Tribunal Supremo que, tras casar la dictada por la Audiencia Provincial de Barcelona, desestimó su demanda contra Hogar y Moda, S.A., y otras personas por la publicación de un reportaje en la revista Lecturas titulado *La cara oculta de Isabel Preysler*. Vulneración del derecho a la intimidad personal y familiar: reportaje sobre el hogar y la vida en familia de una persona con notoriedad pública, con datos proporcionados por una antigua niñera vulnerando su deber de secreto profesional, que carecen de relevancia pública y cuya veracidad y entidad resultan intrascendentes".

denunciar el cónyuge discorde si sospechaba que este ultimo ha cometido alguna irregularidad financiera que pueda perjudicar los intereses económicos del estado, obligación considerada por el Tribunal como una grave injerencia en el derecho a la intimidad: "*en su forma actual la regulación de la declaración única y conjunta de los esposos impone a cada uno de ellos el deber de denunciar ante la Hacienda Pública las incorrecciones en que, a su juicio, incurre su respectivo cónyuge en la estimación de sus propias rentas. La obligada manifestación pública de una discordia en el seno de la familia no es tampoco compatible con la intimidad familiar*"[685].

En Rumania, la vida familiar está protegida por el artículo 26.1. de la Constitución: "*las autoridades respetan y protegen la vida íntima, familiar y privada*". La noción de vida familiar puede incluir las relaciones entre los miembros de la familia y también aspectos de su vida íntima y su vida privada. Desde este punto de vista, la vida íntima, la vida familiar y la vida privada pueden ser complementarias. Sin embargo, los miembros de una familia también pueden tener su propia vida íntima privada, teniendo en esta posición el derecho protegido por el art. 26 párr. (1) de la Constitución, para reclamarles la total confidencialidad a las autoridades, a otros sujetos de derecho, distintos de sus familiares, así como a sus familiares cercanos.

En este sentido, el Código Penal rumano, en el artículo 226.2 admite la exoneración de responsabilidad para el miembro de familia que no denuncia las infracciones cometidas por un familiar, aunque los efectos de la infracción son de una alta gravedad: muerte de la víctima, lesiones físicas graves, enfermedades físicas o psíquicas. En estos casos el derecho a la vida familiar sobrepasa la importancia de la justicia y de la paz social.

7.6.1.2. La inviolabilidad del domicilio (hogar)

Al nivel internacional, el domicilio de la persona goza de la protección del *soft law*. La inviolabilidad del hogar está mencionada en el artículo 12 de la Declaración Universal de los Derechos Humanos: "*nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a*

[685] Sentencia 45/1989, de 20 de febrero (BOE núm. 52 de 02 de marzo de 1989), Cuestión de inconstitucionalidad 1837-1988 en relación con determinados preceptos de la Ley 44/1978, de 8 de septiembre, de normas reguladoras del Impuesto sobre la Renta de las Personas Físicas, teniendo en cuenta la reforma operada por la Ley 48/1983;

su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

Al mismo tiempo, el Pacto Internacional de Derechos Civiles y Políticos dispone: "*1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques"*, otorgando al derecho del hogar las mismas garantías y protección como al derecho de la vida privada.

Consagrada en el artículo 8.1 del C.E.D.H., la inviolabilidad del domicilio (hogar) está protegida también por la jurisprudencia del T.E.D.H., que otorga a la noción de "domicilio" un contenido extendido, incluyendo la residencia principal o secundaria de la persona, el lugar de actividad profesional, embarcaciones de recreo, caravanas, etc., siendo así una noción "autónoma", por referencia a el de "domicilio" en la legislación nacional de los estados, donde se limita a la residencia principal y permanente del individuo[686].

Según esta interpretación el domicilio no se limita a la propiedad de la cual el solicitante es el propietario o inquilino. Puede extenderse a la ocupación a largo plazo, anualmente o durante largos períodos, de una casa que pertenece a un familiar *(Menteş y otros v. Turquía, § 73)*. Domicilio no se limita a aquellos espacios que están legalmente establecidos como tal *(Buckley v. Reino Unido, § 54)* y puede ser reclamado por una persona que vive en un piso, con el acepto de los propietarios, aunque el contrato de arrendamiento no está a su nombre *(Prokopovich v. Rusia, § 36)* o si está registrada como residente en otro lugar *(Yevgeniy Zakharov v. Rusia, § 32)*. La noción es aplicable también para una casa social ocupada por el solicitante como inquilino, incluso si, de conformidad con la legislación nacional, el derecho de ocupación hubiera terminado *(McCann v. Reino Unido, § 46)*.

El domicilio no se limita a las residencias tradicionales. Por lo tanto, incluye, entre otras cosas, caravanas y otras residencias non fijas *(Chapman v. the United Kingdom [GC], §§ 71-74)*. También puede incluir cabañas o bungalows fijados en el suelo,

[686] T.E.D.H. (2020) *Guide on Article 8 of the European Convention on Human Rights. Right to respect for private and family life, home and correspondence,* Recuperado de: https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf

independientemente si la ocupación es legal o no según el derecho interno *(Winterstein y otros v. Francia, § 141; Yordanova y otros v. Bulgaria, § 103).*

Aunque el vínculo entre una persona y un lugar donde habita sólo ocasionalmente puede ser más débil, el artículo 8 también puede aplicarse a las segundas residencias o casas de vacaciones *(Demades v. Turquía, §§ 32-34; Fägerskiöld v. Suecia (dec.); Sagan v. Ucrania, §§ 51-54)* o a los locales residenciales en time-sharing *(Halabi v. Francia, §§ 41-43).* El concepto también se extiende a las instalaciones comerciales de un individuo, como la oficina de un miembro de una profesión *(Buck v. Alemania, § 31; Niemietz v. Alemania, §§ 29-31),* a las instalaciones de una editora *(SaintPaul Luxembourg SA v. Luxemburgo, § 37),* a la oficina de un notario *(Popovi v. Bulgaria, § 103),* o el despacho de un profesor universitario *(Steeg v. Alemania (dec.)).*

Un aspecto muy interesante es que la protección legal del domicilio se aplica también a un domicilio social y a las sucursales u otros locales comerciales de una empresa *(Société Colas Est y otros c. Francia, § 41; Kent Pharmaceuticals Limited y otros contra el Reino Unido (dec.)).*

La libertad de residencia implica tres derechos distintos pero complementarios al mismo tiempo:

- el derecho a elegir el domicilio propio y cambiar este domicilio cuando se considera necesario;
- el derecho a utilizar el domicilio de acuerdo con la voluntad propia, pero de conformidad con la ley;
- el derecho a ser protegido contra posibles violaciones del domicilio.

Este último derecho beneficia de la intervención del estado (garantías legales constitucionales y penales), el domicilio considerándose "no solo una fortaleza del individuo, pero también la extensión de la persona misma, sin la cual ninguna vida privada no es posible en concreto"[687]. Por consiguiente, este derecho está considerado un derecho fundamental que goza de garantías legales, provisto por la Constitución, tanto en el sistema de leyes americanas como europeas, ya sea dentro del derecho a la vida privada (España – articulo 18.2.) o como un derecho propio (Alemania, Bélgica, Rumania). La doctrina y la jurisprudencia estadounidenses otorgan una importancia fundamental a la inviolabilidad del hogar contra cualquier interferencia abusiva por parte de las autoridades

[687] Lebreton, G. (2008) *Libertés publiques et droits de l'homme*, Editorial Sirey.

estatales, como un elemento esencial de la esfera de la privacidad, en su dimensión espacial, defendida por la Cuarta Enmienda a la Constitución de los Estados Unidos[688].

Como plantea el Código Penal rumano (artículo 224): *"La entrada sin derecho, de cualquier forma, a una vivienda, habitación, dependencia o lugar cercado que les pertenezca, sin el consentimiento de quien los utilice, o rechazar la invitación a abandonarlos a la petición del ocupante, será sancionada con una pena privativa de libertad de 3 meses hasta 2 años o con una multa. Si el hecho es cometido por una persona armada, durante la noche o utilizando cualidades falsas, la pena es de prisión de 6 meses a 3 años o multa".* En consecuencia, la inviolabilidad de domicilio queda protegida por el derecho penal como también por la Constitución que en su artículo 27 dispone:

"(1) El domicilio y la residencia son inviolables. Nadie puede entrar o permanecer en el hogar o la residencia de una persona sin su consentimiento.

(2) Las disposiciones del párrafo (1) pueden ser derogadas por ley para las siguientes situaciones:

a) ejecución de una orden de detención o una decisión judicial;

b) la eliminación de un peligro relacionado con la vida, la integridad física o la propiedad de una persona;

c) defensa de la seguridad nacional o del orden público;

d) prevenir la propagación de una epidemia.

(3) El registro será ordenado por el juez y se llevará a cabo en las condiciones y formas previstas por la ley.

(4) Se prohíben los registros durante la noche, excepto en el caso de faltas flagrantes".

En lo que concierne el domicilio de la persona jurídica, el legislador rumano ha elegido protegerlo de modo similar. Según el artículo 225 del Código Penal:

"(1) La entrada sin derecho, de cualquier forma, en cualquiera de los locales donde una persona física o jurídica desarrolla su actividad profesional o el rechazo a abandonarlos a la solicitud del titular será sancionada con pena privativa de libertad desde 3 meses a 2 años o con multa.

(2) Si el hecho es cometido por una persona armada, durante la noche o utilizando cualidades falsas, la pena es de prisión de 6 meses a 3 años o multa".

[688] Amendment IV: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized".

La Constitución Española dispone en su artículo 18. 2. que: *"El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito".*

Como expresa la jurisprudencia del Tribunal Constitucional Español: "*en el caso del domicilio de una persona jurídica la inviolabilidad sólo se extiende a los espacios físicos que son indispensables para que puedan desarrollar su actividad sin intromisiones ajenas, por constituir el centro de dirección de la sociedad o de un establecimiento dependiente de la misma o servir a la custodia de los documentos u otros soportes de la vida diaria de la sociedad que quedan reservados al conocimiento de terceros, pero no a cualquier espacio en el que se desarrolle la vida reservada de un ente que carece de intimidad*"[689].

7.6.1.3. El secreto de la correspondencia

El secreto de las comunicaciones privadas entre personas ha sido siempre una preocupación importante para los juristas y casi todos los ordenamientos jurídicos han establecido garantías para proteger el contenido de las conversaciones privadas frente a los terceros. En todos los ordenamientos jurídicos está prohibida la interceptación de comunicaciones salvo en los casos autorizados por la ley, en situaciones excepcionales y solo en beneficio de las autoridades estatales. Las actividades de interceptación afectan a un derecho fundamental y solo el cumplimiento de estos requisitos y garantías permitirá que esta violación no se convierta en en *vulneración*.[690]

Como derecho fundamental, el secreto de las comunicaciones está reconocido en la Declaración Universal de Derechos Humanos de 1948 (artículo 12) y en algunos tratados internacionales, como el Pacto Internacional de Derechos Civiles y Políticos de 1966 (artículo 17), o el Convenio de Roma de 1950, para la protección de los Derechos Humanos y de las Libertades Fundamentales (artículo 8). Si bien estos textos prefieren

[689] Sentencia 137/1985, de 17 de octubre, (BOE núm. 268, de 08 de noviembre de 1985), ECLI:ES:TC:1985:137 - "Derivados de Hojalata, Sociedad Anónima" interpuso recurso de amparo, mediante escrito el día de 18 de febrero de 1985, solicitando que declarándose «la inconstitucionalidad del art. 117 de la Ley General Tributaria y de los arts. 103 y 107 del Reglamento General de Recaudación» y amparándose «la inviolabilidad de domicilio del art. 18.2 de la Constitución», se ordene «reponer las actuaciones judiciales al momento procesal en que el Juez de Distrito debe resolver si autoriza con plena jurisdicción y por tanto pueda acceder o denegar la entrada al Recaudador de Hacienda en el domicilio» de la solicitante de amparo.

[690] Díaz Revorio, F. J. (2006) *El derecho fundamental al secreto de las comunicaciones*, Derecho PUCP: Revista de la Facultad de Derecho, no. 59, pp. 159-175

referirse al respeto a la correspondencia, el artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea afirma, en términos similares, que "toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y del secreto de sus comunicaciones".

El secreto de la correspondencia aparece en algunas constituciones de los estados como un derecho fundamental distinto (Alemania, Rumania) o como anexado al contenido del derecho a la vida privada (España) u de otros derechos. Es el caso de la Constitución de Portugal, que regula el derecho a la inviolabilidad del domicilio y la correspondencia en el mismo artículo 34:

"*1. El domicilio y el secreto de la correspondencia y de otros medios de comunicación privada son inviolables [...]*

4. Se prohíbe toda injerencia de las autoridades en la correspondencia, en las telecomunicaciones y en los demás medios de comunicación, salvo en los casos previstos en la ley en materia de procedimiento penal".

Al nivel europeo, este derecho está reconocido y garantizado independientemente de la calidad del titular o de las circunstancias de hecho. El T.E.D.H. ha admitido la existencia de una interferencia no permitida en el secreto de la correspondencia, regido en el Convenio también por el artículo 8, en caso de que el control de la correspondencia de los prisioneros en los centros penitenciarios no esté claramente regulado[691], así como en la situación en la que se supervisa la correspondencia electrónica en el lugar de trabajo[692], sin el conocimiento de la persona sujeta a dicha medida.

Las limitaciones a este derecho, por ejemplo, a través de la vigilancia y la intercepción[693], solo se permiten si son autorizados por un juez independiente, en casos limitados y previstos por la ley, para la defensa de objetivos esenciales para el estado y la sociedad (seguridad nacional, prevención o lucha contra el terrorismo o crimen organizado), por un período de tiempo limitado y con la provisión de medidas estrictas para la preservación y vigilancia del uso de la información así obtenida. El T.E.D.H.

[691] T.E.D.H., Sentencia de 15 de noviembre de 2006, *Caso Domenichini c. Italia (núm. 15943/90);*
[692] T.E.D.H., Sentencia de 3 de abril de 2007, Caso *Copland c. Reino Unido (núm. 62617/00);*
[693] El primer juicio del T.E.D.H. en este asunto es el del 6 de septiembre de 1978, en el caso *Klass y otros c. Alemania (n. ° 5029/71)*, en el que se declaró que, si bien el art. 8 de la Convención no menciona las conversaciones telefónicas, deben incluirse en el ámbito de la noción de "correspondencia" y "vida privada".

considera que el incumplimiento de los requisitos legales al realizar intercepciones de comunicaciones puede producir consecuencias nocivas no solo para una determinada persona, sino que puede tener consecuencias negativas para la sociedad democrática en su conjunto. También especifica que *"un sistema secreto de vigilancia implementado para proteger la seguridad nacional presenta el riesgo de socavar o incluso destruir la democracia con el pretexto de su defensa"*[694].

En Francia, bajo el efecto de las sentencias del T.E.D.H.[695], que apreciaron que la ley francesa no preveía el alcance y las modalidades de ejercicio del poder discrecional de las autoridades, las disposiciones procesales penales se modificaron para garantizar la legitimidad y la transparencia del procedimiento de la interceptación de las comunicaciones.

En los Estados Unidos, violar el secreto de la correspondencia, en particular las comunicaciones telefónicas o electrónicas, es uno de los temas más debatidos, comenzando con el "*negocio Watergate*"[696] y hasta el tema de las escuchas de cientos de llamadas telefónicas de los ciudadanos estadounidenses bajo la Ley Patriota[697] (*Patriot Act*). El más reciente escándalo mediático fue determinado por la utilización de los programas de monitoreo de comunicaciones electrónicas desarrollados por la Agencia de Seguridad Nacional (NSA), revelados por Edward Snowden. Las operaciones fueron llevadas a cabo con el pretexto de identificar a las personas sospechosas de terrorismo, bajo las amenazas actuales representadas por los actos del crimen organizado. Con este delicado asunto se lanzó la cuestión de cómo encontrar un equilibrio entre la necesidad de aplicar medidas de vigilancia secretas y el respeto a la intimidad, así como lo protege la Cuarta Enmienda a la Constitución de los Estados Unidos.

En España, la constitución garantiza el derecho al secreto de las comunicaciones en el artículo 18 (parágrafo 3 y 4): "*Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*". La única brecha en la

---

[694] Ibidem.
[695] T.E.D.H., Sentencias de 24 de abril de 1990 en los casos *Kruslin c. Francia* (no. 11801/85) y *Huvig c. Francia* (no. 11105/84);
[696] El nombre pertenece a un escándalo político estadounidense de la década de 1970 generado por la instalación de dispositivos de escucha en las oficinas (del Hotel Watergate) del partido de oposición, que culminó con la dimisión del presidente estadounidense Richard Nixon.
[697] El texto de la ley, en español, está disponible en: http://interamerican-usa.com/articulos/Leyes/US-Patriot%20Act.htm

inviolabilidad de este derecho fundamental relativo es la resolución judicial, cuando un juez decide permitir algunas injerencias en la esfera de las comunicaciones de una persona en el nombre y por el cumplimiento de otros derechos fundamentales, solo después de un análisis sobre la proporcionalidad de los efectos.

La jurisprudencia del T.E.D.H., del Tribunal Constitucional y del Tribunal Supremo español ha señalado la necesidad de verificar la existencia de determinadas condiciones formales y legales que debe cumplir la resolución judicial que autoriza la interceptación de las comunicaciones de una persona. Estos requisitos no pueden tener un carácter formal, simple, sino que deben correlacionarse con la importancia de este derecho fundamental, de manera que se justifique la legalidad y legitimidad del enfoque.

En síntesis, esos requisitos serían los siguientes[698]:

1) La existencia de una motivación de la resolución judicial. Es un requisito para fundamentar la existencia de las circunstancias o motivos que justifican la admisibilidad de las actividades de injerencia en el derecho fundamental. Teniendo en cuenta estos aspectos, el requisito de la motivación no supone una fundamentación formal, sino una presentación de determinadas exigencias que cumplen, a su vez, con ciertos parámetros, como:

> a. La motivación judicial debe ser expresa. La solicitud policial no representa una motivación judicial pero los aspectos señalados pueden ser integrados por el juez en su informe, junto con los demás requisitos para la motivación. Rellenar unos formularios predeterminados no representa una verdadera motivación según la jurisprudencia del Tribunal Constitucional.
>
> b. El criterio de la proporcionalidad debe ser un punto focal de la motivación judicial porque es necesario demonstrar que la intervención es necesaria y su finalidad tiene la importancia necesaria para adoptar una medida de este alcance.
>
> c. El informe judicial debe presentar en detalle el alcance de la medida, el procedimiento de la intervención, los derechos afectados, los efectos y los límites de acción por parte de las autoridades.
>
> d. Si la interceptación se produce en el curso de un proceso penal, la motivación debe presentar en detalle los indicios existentes, los delitos que están al punto de cometerse, la ley con carácter penal aplicable y las personas consideradas

[698] Díaz Revorio, F. J. (2006) *El derecho fundamental al secreto de las comunicaciones*, Derecho PUCP: Revista de la Facultad de Derecho, no. 59, pp. 159-175

culpables. Las simples sospechas no pueden constituir un motivo de autorización para la intervención.

2) Establecer un plazo determinado para la intromisión en la vida privada del perseguido. El juez debe mencionar en detalle las fechas y las horas entre cuales están autorizadas las medidas de vigilancia. No importa el momento de la efectiva intervención, el plazo establecido por el juez no se puede prolongar a base de retrasos causados por motivos técnicos o de otra naturaleza *(STC 205/2005, del 18 de julio)*.

3) La resolución judicial debe precisar, en concreto, las personas determinadas y los delitos concretos que representan el objeto de la intervención. No son admisibles las autorizaciones genéricas ni la disociación entre la autorización y la investigación posterior.

4) La necesidad de la comunicación de las medidas a los afectados, una vez terminada la observación o intervención.

En el sistema de derecho rumano, la violación del secreto de la correspondencia representa una infracción prevista por el artículo 302 del Código penal: *"(1) La apertura, el robo, la destrucción o retención, sin derecho, de una correspondencia dirigida a otro, así como la divulgación sin derecho del contenido de dicha correspondencia, aun cuando haya sido enviada abierta o haya sido abierta por error, será sancionada con pena privativa de la libertad desde 3 meses a un año o con multa. (2) La interceptación, sin derecho, de una conversación o comunicación efectuada por teléfono o por cualquier medio electrónico de comunicación, será sancionada con pena privativa de libertad desde 6 meses a 3 años o con multa*".

Además de esta protección general, la ley penal añadió una agravante para la situación cuando los hechos previstos en los parágrafos mencionados más arriba fueron cometidos "*por un funcionario que tiene la obligación legal de respetar el secreto profesional y la confidencialidad de la información a la que tiene acceso*". En tal caso la pena es de prisión de uno a 5 años y la prohibición de ciertos derechos. También la divulgación, difusión, presentación o transmisión, a otra persona o al público, sin derecho, del contenido de una conversación o comunicación interceptada, aunque el autor haya tenido conocimiento de ella por error o accidente, será sancionada con prisión desde 3 meses a 2 años o con multa.

En lo que atañe las limitaciones del derecho al secreto de las comunicaciones el legislador rumano ha previsto dos situaciones de exoneración de responsabilidad penal. Así, el hecho cometido no constituye delito:

a) si el culpable descubre la comisión de un delito o contribuye a la divulgación de la comisión de un delito;

b) si el culpable capta hechos de interés público, que tienen interés para la vida de la comunidad y cuya divulgación tiene mayores ventajas públicas que el daño causado a la persona lesionada.

Analizando estas causas nos damos cuenta de que el interés de la comunidad y la seguridad de los demás ciudadanos son motivos pertinentes para restringir el derecho al secreto. Las situaciones mencionadas por el código penal son limitativas y no exhaustivas y son de estricta interpretación. Para subrayar la importancia de este derecho fundamental de la persona, la ley penal incrimina incluso algunos actos preparatorios de la infracción. Con base en el artículo 302.6.: "*La posesión o manufacturación, sin derecho, de medios específicos de interceptación o grabación de comunicaciones será sancionada con pena privativa de libertad desde 3 meses a 2 años o con multa*".

En conclusión, el único control efectivo sobre el respeto este derecho, sujeto a una intervención insidiosa del estado, sigue siendo el poder judicial, realizado por jueces independientes.

7.6.2. Derechos opuestos al derecho a la privacidad.

Garantizar el derecho a la vida privada o, por el contrario, limitarlo, también depende de otros derechos fundamentales, como la libertad de expresión o el derecho a la información. Si el juez debe analizar la invocación del derecho a la vida privada en contradicción con cualquiera de los dos derechos mencionados anteriormente, está obligado a aplicar el método de ponderación entre los derechos respectivos y hacer cumplir la ley en concreto, al declarar uno de los derechos como predominante.

7.6.2.1. La libertad de expresión

El creciente interés de la opinión pública sobre los asuntos cotidianos y los chismes ha sido profundamente influenciado y alimentado por los medios de la

comunicación, un aspecto observado e incluso criticado por los *padres* del derecho a la privacidad, S. Warren y L. Brandeis en su artículo de 1890. Este fenómeno fue analizado por el profesor Rodríguez Uribes que sorprende la esencia de esta transformación de la prensa: "*Esta mayor trascendencia de la imprenta, que supera los instrumentos tradicionales de difusión del pensamiento, el lenguaje oral y la escritura, explicará que se hable, a partir de la segunda mitad del siglo XV, sobre todo de «libertad de imprenta» y no tanto de «libertad de expresión*»"[699].

A veces, la divulgación de hechos personales puede legitimarse por la necesidad de satisfacer el interés público, especialmente cuando se trata de líderes políticos y sus acciones. Pero hay muchas situaciones en las que la prensa abunda en materiales, acompañados o no de imágenes, sobre personas privadas, cuyo derecho a la vida privada se viola sin un interés público a este respecto[700].

Para determinar en qué medida una noticia permite limitar el derecho a la privacidad, el contenido de la información debe analizarse en el sentido más amplio posible, respectivamente, se necesita evaluar si tiene un valor periodístico para los destinatarios o si es de interés público. En este sentido, se propone tener en cuenta el interés que una información puede presentar para un lector con una capacidad intelectual media, similar al enfoque del *consumidor medio informado*. Según la doctrina estadounidense "restatement of torts", una información no tiene ningún valor informativo cuando deja de aportar la información al público y cuando su único propósito es penetrar de manera morbosa y sensacionalista la privacidad de las personas[701].

Existen varias opiniones sobre la relación entre la libertad de expresión (en particular, la libertad de prensa, lato sensu, incluyendo aquí cualquier manifestación pública de ideas, no solo en la televisión, sino también en un foro de discusión en Internet, por ejemplo) y el derecho a la vida privada (visto en este contexto, en particular, desde el punto de vista del derecho a la imagen y/o del derecho al honor y la reputación).

---

[699] Rodríguez Uribes, J. M. (1999) *Opinión pública. Concepto y modelos históricos*. Editorial Marcial Pons, Madrid, pág. 97.

[700] En este sentido véase, Sentencia de T.E.D.H. de 24 de junio de 2004 en el caso *Von Hannover c. Alemania* (núm. 59320/2000).

[701] El *common law* hace una distinción entre la difamación oral, denominada *slander* y la difamación escrita, llamada *libel.* Hasta la invención de métodos de impresión a gran escala la regulación del libel era prácticamente inexistente, y es que la creación de la imprenta fue una de las razones más importantes que llevaron a la creación de la acción de *libel*. En épocas tempranas la difamación escrita (libel) debe haber sido relativamente rara e inocua; rara porque pocas personas podían escribir, inocua porque pocas podían leer. El primer caso en el que se utilizó la nueva ley de libel fue De libelis Famosis en 1609.

Sobre este asunto, la doctrina francesa[702] considera que la divulgación de los hechos o imágenes con carácter personal por parte del titular del derecho a la vida privada significa una renuncia al benéfico de este derecho y, como tal, la nueva publicación de la información hecha pública por otra persona no es ilegal.

No compartimos esta opinión, ya que, por un lado, es probable que es inalienable (sino que esté sujeto a restricciones en su ejercicio) y, por otro lado, la nueva publicación de la información debe realizarse con el mismo propósito y de buena fe para ser considerada legal y no abusiva. Por lo tanto, consideramos que la solución propuesta por el Código Civil rumano que estipula la presunción de consentimiento (artículo 76) es mucho más apropiada a la regla según la cual se presume el acuerdo sobre la divulgación de información, pero solo en relación con la persona física o jurídica en relación con el que el titular del derecho ejerció así su voluntad (siendo, por lo tanto, un consentimiento implícito y limitado a un acto legal bilateral):

> "*Cuando la persona a quien se refiere la información o material los pone a disposición de una persona física o jurídica de la que tenga conocimiento de que desarrolla su actividad en el ámbito de la información pública, se presume el consentimiento para su uso, no siendo necesario un acuerdo escrito".*

Además, el Código Civil rumano sanciona como violaciones del derecho a la vida privada aquellas manifestaciones de la libertad de expresión logradas sin el consentimiento de la persona interesada[703]. Analizando las disposiciones del Código Civil en este asunto, un autor[704] señala dos atributos de la correlación entre la libertad de expresión y el derecho a la vida privada: "*complementariedad (en el sentido de que los dos derechos son mutuamente integrales) y convergencia (en que ambos tienen, en finalmente, para lograr un equilibrio capaz de garantizar el respeto a la privacidad y la dignidad de la persona humana*".

---

[702] Bertrand A. (1999) *Droit à la vie privée et droit à l'image*, Editorial Litec.

[703] Artículo 74 lit. f) del Código Civil: "la difusión de noticias, los debates, las investigaciones o reportajes escritos o audiovisuales sobre vida íntima, personal o familiar, sin el consentimiento del interesado". Artículo 74 lit. g) del Código Civil: "difusión de materiales que contengan imágenes de una persona en tratamiento en unidades de salud, así como datos personales sobre el estado de salud, problemas de diagnóstico, pronóstico, tratamiento, circunstancias relacionadas con la enfermedad y con varios otros hechos, incluido el resultado de la autopsia, sin el consentimiento del interesado, y si el fallecido, sin el consentimiento de la familia o de los titulares".

[704] Dumitru, H. D. (2012*) La libertad de expresión y la vida privada. Conexiones constitucionales y civiles.* Revista Pandectele Romane, nr. 5/2012.

Superar los límites admitidos de libertad de expresión, al traer insultos o asociar a la persona con hechos o actos condenatorios o perjudiciales que no pasan *la prueba de la veracidad*, puede determinar una responsabilidad penal, en aquellos estados en los que el insulto y la calumnia reciben un mayor grado de peligro social. Al mismo tiempo el artículo 30 párr. (6) de la Constitución rumana regula expresamente el límite a la libertad de expresión: "*la libertad de expresión no puede dañar la dignidad, el honor, la vida privada de la persona o el derecho a la propia imagen*".

En España el derecho a la libertad de expresión fue reconocido por primera vez en la Constitución de Cádiz de 1812 (art. 371): "*Todos los españoles tienen libertad de escribir, imprimir y publicar sus ideas políticas sin necesidad de licencia, revisión o aprobación alguna anterior a la publicación, bajo las restricciones y responsabilidad que establezcan las leyes*". La Constitución de 1978 recoge este legado y consagra las libertades de expresión e información, como derecho fundamental, en el artículo 20, considerado la sede de la materia: "*el derecho a expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier medio de reproducción*" y "*a comunicar o recibir libremente información veraz por cualquier medio de difusión*".

La libertad de expresión, stricto sensu, es el núcleo básico de todos los derechos consagrados en el texto constitucional. Sin embargo, para una mejor comprensión del concepto, es necesario correlacionar la regulación nacional con las reglamentaciones internacionales, como la Declaración Universal de Derechos Humanos, el Pacto de Derechos Civiles y Políticos o la Convención para la Protección de los Derechos Humanos y las Libertades. Desde la perspectiva de estos tratados, la libertad de expresión se extiende también a la comunicación de hechos de interés general, así como al derecho a recibir y analizar libremente pensamientos, ideas y opiniones[705].

La jurisprudencia del Tribunal Constitucional español confirma el carácter fundamental de la libertad de expresión, de forma que: "*La libertad de expresión que proclama el art. 20.1 a) es un derecho fundamental del que gozan por igual todos los ciudadanos y que les protege frente a cualquier injerencia de los poderes públicos que no esté apoyada en la Ley, e incluso frente a la propia Ley en cuanto ésta intente fijar*

[705] López Acuña, C.R. (2016) *La evolución de la libertad de expresión y el derecho a la información en la España constitucional. Relevancia de la jurisprudencia en la profesión periodística*, Tesis doctoral, Universidad Complutense de Madrid, Facultad de Ciencias de la Información, recuperado de: http://eprints.ucm.es/42082/1/T38627.pdf.

otros límites que los que la propia Constitución (arts. 20.4 y 53.1) admite. Otro tanto cabe afirmar respecto del derecho a comunicar y recibir información veraz (art. 20.1 d), fórmula que, como es obvio, incluye dos derechos distintos, pero íntimamente conectados. El derecho a comunicar que, en cierto sentido, puede considerarse como una simple aplicación concreta de la libertad de expresión y cuya explicitación diferenciada sólo se encuentra en textos constitucionales recientes"[706].

En la mayoría de los casos, el T.E.D.H. ha fallado al favor de los periodistas, llamados los "*perros guardianes de la democracia*", especialmente en el periodismo de investigación, teniendo en cuenta que la protección de las fuentes de información es una de las piedras angulares de la libertad de prensa. Por otro lado, se condena el uso de cámaras ocultas o cámaras que violan el derecho a la imagen del individuo, esta práctica es "contraria al principio de rigor y honestidad que debe animar al periodista en la busca de información". Por esto, las limitaciones del derecho a la privacidad o a la libertad de expresión, en la situación de colisión entre estos dos derechos, están relacionado con la calidad del titular del derecho a la vida privada (pública o no), con el carácter de la información divulgada (si tiene un interés público legítimo[707]), con la forma de penetrar en la esfera de la vida privada de un individuo (por ejemplo, por medios ocultos o no, capturando imágenes internas de las propiedades privadas), respetando la voluntad del interesado, si corresponde.

Al nivel internacional la libertad de la expresión fue reconocida por el artículo 19 de la Declaración Universal de Derechos Humanos: "*todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión*"; así como por el artículo 10 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales: *"toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades y sin consideración de fronteras.*

[706] STC 6/1981, de 16 de marzo, BOE núm. 89, de 14 de abril de 1981, ECLI:ES:TC:1981:6;
[707] Por ejemplo, el TEHD en la Sentencia de 9 de noviembre de 2006, *caso Leempoel & S.A. ED. Revue c. Bélgica (núm. 64772/01)* consideró que la estrategia de defensa (presentada en la correspondencia privada) preparada por un juez para utilizarla durante una investigación parlamentaria no era de interés público general, sino íntimo de la vida de esa persona, y la confidencialidad de esos datos personales debía protegerse contra cualquier injerencia, como se consideraba la publicación de esa estrategia en un artículo de prensa.

El presente artículo no impide que los Estados sometan a las empresas de radiodifusión, de cinematografía o de televisión a un régimen de autorización previa". El párrafo 2 de este mismo artículo menciona la posibilidad de restringir el ejercicio de este derecho en algunas situaciones previstas por la ley. En un estado de derecho, se consideran como medidas necesarias la protección de la seguridad nacional y publica, la integridad de las fronteras, la prevención del delito y la lucha contra la criminalidad organizada, la protección de la salud, la preservación de los valores fundamentales, de los derechos y libertades de los ciudadanos, la imparcialidad del poder judicial.

También el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos reconoce la importancia del derecho a la libertad de expresión que comprende "la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección, y admite la posibilidad de limitar su ejercicio en algunas condiciones similares con las previstas en el convenio mencionado anterior".

No debemos perder de vista el hecho que todos estos textos legales fueron adoptados antes de la aparición de las redes sociales. Hay que admitir que Facebook determinó una revolución sociocultural de igual magnitud que en la que su día provocó Gutenberg[708] con la invención de la imprenta, pero en un periodo de tiempo bastante diferente. Marck Zuckerberg, el creador de Facebook necesitó solo 5 años para reunir miles de millones de personas de todo el mundo en su plataforma, mientras que para Gutenberg fueron necesarios 3 siglos para tener el mismo número de utilizadores de su invención. Pues, en nuestros días, la rapidez con cual se propagan al nivel mundial los productos de nuestro derecho a libre expresión y el impacto psicológico de los mensajes son superiores a las prácticas de los años sesenta.

La libertad de expresión debe limitarse por su mismo titular. La cláusula de conciencia consiste en la elección que puede hacer un profesional de la información entre obtener audiencia o notoriedad pública a cualquier precio o comunicar únicamente aquella información compatible con su código ético. Esta cláusula es una garantía de la independencia periodística frente a cualquier presión externa. El ordenamiento jurídico debe contener garantías suficientes para el cumplimiento de esta cláusula por parte de

[708] Johann Gutenberg inventó la imprenta moderna a mediados del siglo XIV.

todos los interesados, pero también para evitar daños o sanciones injustificadas[709]. Como indica Marc Carrillo: "*La vinculación del derecho a la cláusula de conciencia a una determinada forma de ejercer el derecho a la información que interesa no solamente al periodista, sino también a la sociedad, es lo que justifica su condición de derecho fundamental. La cláusula no es únicamente el derecho a una indemnización; es, esencialmente, el derecho a ejercer el periodismo en condiciones que colaboren a garantizar la objetividad y el pluralismo informativo"*[710].

La libertad de expresión es un derecho fundamental opuesto a la vida privada, pero sin su reconocimiento legal y social, tampoco es posible que este último derecho se manifieste. El profesor Rodríguez Uribes alude a este respecto: "*la libertad de expresión es la columna vertebral de nuestras sociedades democráticas y liberales, por lo que los límites siempre hay que justificarlos. Hay una presunción siempre a favor de la libertad de expresión"*[711]. Fuera de la democracia no hay derechos fundamentales.

7.6.2.2. El derecho a la información

"*Dadme la libertad de saber, de hablar y de argüir libremente según mi conciencia por encima de todas las libertades*" es el deseo expresado por John Milton en su célebre obra *Areopagitica* (1644), un discurso ante el Parlamento de Inglaterra sobre la libertad de impresión sin censura. La libertad de saber, es decir el derecho a la información, es la libertad humana que ha cambiado el mundo. Sin acceso a la información el ser humano no se puede desarrollar y evolucionar. Tampoco la sociedad en su conjunto.

Una vez que concientizaron la existencia de este derecho fundamental, los juristas empezaron el gran trabajo de la conceptualización y reglamentación, con el fin de proteger su contenido frente a las injerencias de institucionales o incluso sociales (hay sociedades donde el derecho a la información no pertenecía a ciertas categorías vulnerables: mujeres, niños, esclavos.).

---

[709] El legislador español ha cumplido el mandato constitucional de su regulación legal (Ley Orgánica 2/1997, reguladora de la cláusula de conciencia de las profesionales de la información, donde se regulan los detalles del ejercicio de este derecho).

[710] Carrillo, M. (1993). *La cláusula de conciencia y el secreto profesional de los periodistas*. Cuadernos Civitas, Editorial Civitas Madrid, p. 165.

[711] Debate sobre la libertad de la expresión con los profesores de la UC3M Juan José Tamayo, Miguel Satrústegui y José Manuel Rodríguez Uribes, *La tertulia jurídica*, organizada por la UC3M en colaboración con la editorial "Tirant lo Blanch".

Al nivel internacional, así como hemos visto en el capítulo seis de esta tesis, el derecho a la información está regulado en estrecha relación con la libertad de expresión: el artículo 19 de la Declaración Universal de Derechos Humanos, el artículo 10 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, artículo 19 del Pacto Internacional de Derechos Civiles y Políticos. Los instrumentos jurídicos internacionales confirman el carácter fundamental del derecho.

El derecho a la información se considera parte integrante de la libertad de expresión, pero en algunos sistemas jurídicos, este derecho se trata como un derecho fundamental autónomo. Independientemente de la forma en que esté regulado, su contenido denota la libertad de la persona para recibir o transmitir información o ideas sin interferencia, sin la interferencia de las autoridades. El titular de este derecho fundamental es todo ser humano, independiente de su nacionalidad, etnia, sexo, edad u otros rasgos. Por el otro lado, tenemos que subrayar un aspecto muy importante: el ejercicio de la libertad de expresión sólo corresponde a quien posea la capacidad natural o la edad necesarias para expresarse, mientras que el derecho a la información se puede ejercer solo por aquel que tiene la capacidad de recibir la información (leer, oír, comprender, analizar y sintetizar). Este último derecho implica responsabilidad y inteligencia para que cumpla con sus objetivos sociales.

El derecho a la información tiene dos aspectos: por un lado, cualquier persona tiene el derecho a recibir información de interés público, de parte de los titulares del poder público, y por el otro lado cualquier persona tiene el derecho a ser informado sobre aspectos que la interesa. En ambos sentidos, existen interferencias con la vida privada de los demás individuos.

El derecho a recibir información de interés público está reconocido en la mayoría de los estados democráticos y se beneficia de las garantías legislativas en los estados que pertenecen tanto al sistema de ley continental como a la ley anglosajona, que estipulan las condiciones bajo las cuales se permite el acceso a documentos de interés público. En este caso, el conflicto que podría surgir entre el derecho a la información y el derecho a la vida privada se refiere, en particular, al componente informativo de este último derecho, respectivamente, el derecho a la protección de datos personales, en caso de que el acceso a ciertos documentos públicos pudiera ser denegado por motivos de la necesidad de proteger cierta información personal incluida en los documentos respectivos. Por lo tanto, se excluye una tensión entre los dos derechos si los documentos públicos no

contienen datos personales o si los documentos respectivos, aunque contienen datos personales, no entran dentro del alcance del derecho fundamental a la información (lato sensu).

En el sistema legal rumano el derecho a la información de interés público está reglamentado de forma expresa, en la Ley 544/2001 sobre el libre acceso a las informaciones de interés público: *el acceso libre y sin restricciones*[712] *de la persona a cualquier información de interés público, así definida por esta ley, es uno de los principios fundamentales de las relaciones entre las personas y las autoridades públicas, de conformidad con la Constitución rumana*[713] *y los documentos internacionales ratificados por el Parlamento rumano*. Según esta ley, la información de interés público significa cualquier información relacionada con las actividades o resultado de las actividades de una autoridad o institución pública, independientemente del medio o la forma o manera de expresión de la información.

En España, el derecho a la información está reconocido como fundamental, junto al el derecho a libre expresión, en el artículo 20 de la Constitución Española (presentado en el capítulo anterior). En lo que concierne el derecho a información de interés público, el artículo 12 de la Ley orgánica 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno estipula que "*todas las personas tienen derecho*

---

[712] Aunque la Constitución otorga un carácter absoluto al derecho a la información, el artículo 12 de la Ley 544/2001 contiene disposiciones relativas a la información restringida para el público:
"a) información en el ámbito de la defensa nacional, la seguridad y el orden público, si forman parte de las categorías de información clasificada, de acuerdo con la ley;
b) información sobre las deliberaciones de las autoridades, así como las relativas a los intereses económicos y políticos de Rumanía, si forman parte de la categoría de información clasificada, de acuerdo con la ley;
c) información sobre actividades comerciales o financieras, si su publicidad infringe el derecho de propiedad intelectual o industrial, así como el principio de competencia leal, conforme a la ley;
d) información sobre datos personales, de acuerdo con la ley;
e) información sobre el procedimiento durante la investigación penal o disciplinaria, si se pone en peligro el resultado de la investigación, se divulgan fuentes confidenciales o se pone en peligro la vida, integridad física, salud de una persona luego de la investigación realizada o en curso;
f) información sobre procesos judiciales, si su publicidad es perjudicial para garantizar un juicio justo o el interés legítimo de alguna de las partes involucradas en el proceso;
g) información cuya publicación perjudique las medidas de protección de los jóvenes".

[713] *Artículo 31: "(1) El derecho de la persona a tener acceso a cualquier información de interés público no puede estar restringido.*
(2) Las autoridades públicas, según sus competencias, están obligadas a garantizar la correcta información de los ciudadanos sobre los asuntos públicos y sobre los problemas de interés personal.
(3) El derecho a la información no debe menoscabar las medidas para proteger a los jóvenes o la seguridad nacional.
(4) Los medios de comunicación, públicos y privados, están obligados a asegurar la correcta información de la opinión pública.
(5) Los servicios públicos de radio y televisión son autónomos. Deben garantizar a los grupos sociales y políticos el ejercicio del derecho a la emisión. La organización de estos servicios y el control parlamentario de su actividad están regulados por ley orgánica".

a acceder a la información pública, en los términos previstos en el artículo 105.b) de la Constitución Española, desarrollados por esta Ley". Según el siguiente artículo, "*se entiende por información pública los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de este título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones"*.

El sistema legal español permite limitar el acceso a la información en los casos previstos de forma limitativa en el artículo 14 de la Ley 19/2013[714]. Dependiendo de las circunstancias concretas de cada caso y especialmente cuando nos enfrentamos a un interés público o privado superior que justifique la injerencia, fijar los límites de acceso es un paso obligatorio, justificado y relacionado con la finalidad legítima que se persigue.

Los titulares del derecho a la vida privada pueden ser personas públicas o naturales; en el primer caso, la divulgación de datos personales puede ser admitida si la información solicitada está directamente relacionada con la calidad de la persona pública del interesado. En las otras situaciones, para satisfacer el derecho a la información, es necesario identificar un interés legítimo del solicitante para recibir tal información, frente al derecho a la privacidad del propietario de los datos personales, basado en una prueba de proporcionalidad o el recurso a la información anónima que podría dañar la vida privada de un individuo, antes de divulgar un documento de interés público.

Aunque ambos derechos nacieron de la necesidad de garantizar la transparencia, debe hacerse una distinción entre el derecho fundamental a la información y el derecho subjetivo a la información, un elemento componente del derecho a la protección de datos personales, cuyo contenido está restringido a una serie de información. que un operador

[714] Artículo 14. Límites al derecho de acceso:
"1. El derecho de acceso podrá ser limitado cuando acceder a la información suponga un perjuicio para:
a) La seguridad nacional.
b) La defensa.
c) Las relaciones exteriores.
d) La seguridad pública.
e) La prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios.
f) La igualdad de las partes en los procesos judiciales y la tutela judicial efectiva.
g) Las funciones administrativas de vigilancia, inspección y control.
h) Los intereses económicos y comerciales.
i) La política económica y monetaria.
j) El secreto profesional y la propiedad intelectual e industrial.
k) La garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión.
l) La protección del medio ambiente".

de datos personales (derecho público o privado) está obligado a proporcionar a la persona cuyos datos personales procesa (artículo 13.2 del Reglamento UE 2016/679).

El Tribunal de Justicia de Luxemburgo ha tenido la oportunidad en varias ocasiones[715] de pronunciarse sobre la importancia de uno u otro de los dos derechos, pero dejando a la discreción de los tribunales nacionales encontrar un equilibrio justo en los casos particulares. De acuerdo con las autoridades de protección de datos personales en los Estados miembros de la UE, ambos derechos son de la misma naturaleza, importancia y grado, por lo que es necesario identificar un equilibrio razonable en el caso de una solicitud de acceso a los documentos públicos, basado en un análisis personalizado.

A partir de otro principio básico, el de la igualdad, todo ciudadano tiene derecho a recibir información y acceder a los canales de los medios. Sin la información correcta y en tiempo real, ningún ciudadano puede participar en el acto de gobernar y no puede involucrarse en la vida comunitaria. Por estos motivos, todos los ciudadanos deben estar correctamente informados, en tiempo real y de acuerdo con su nivel de comprensión. Solo cuando comprende el verdadero significado del derecho a la información y el hecho de que éste le otorga el derecho a participar en las principales decisiones políticas, económicas, culturales o sociales, el ciudadano exige su reconocimiento y efectivo ejercicio. En conclusión, el derecho a recibir información se basa, por tanto, en un interés colectivo por la información y tiene una razón para tener derecho a emitir información[716].

En su libro *Opinión Publica. Concepto y modelos históricos*, el profesor Rodrigue Uribes, propone una perspectiva interesante y realista sobre el derecho a la información y su alcance: *"[...] lo relevante es que exista (se reconozca y se garantice suficientemente) un régimen de libertad de expresión en sentido amplio, que hoy incluiría también el derecho a la información, es decir, no sólo la libertad de informarse, sino también el derecho a ser informado (información, naturalmente, que ha de ser veraz). Es decir: es necesario que se pueda opinar y discutir libremente, o en condiciones de suficiente libertad, lo que no debe confundirse con la obligación de que opinen todos, o*

[715] Por ejemplo, los asuntos C-465/00, C-138/01 y C-139/01, sentencia del Tribunal de 20 de mayo de 2003, Rechnungshof (C465 / 00) contra Österreichischer Rundfunk y otros y Christa Neukomm (C-138/01) y Joseph Lauermann (C139 / 01) v Österreichischer Rundfunk, publicadas en Rep. 2003 I-04989, ECLI: EU: C: 2003: 294.

[716] López Acuña, C. R. (2016) *La evolución de la libertad de expresión y el derecho a la información en la España constitucional. Relevancia de la jurisprudencia en la profesión periodística*, Tesis doctoral, Universidad Complutense de Madrid, Facultad de Ciencias de la Información, recuperado de: http://eprints.ucm.es/42082/1/T38627.pdf.

con que todos tengan reconocido el derecho a formar parte de la opinión pública"[717]. El profesor sorprende en su libro la esencia del derecho a ser informado correctamente que no se puede lograr sin un ejercicio responsable y consciente del derecho a opinar o a expresarse. El titular del derecho a la información puede ser la victima perfecta de las conductas abusivas de los titulares de la libertad de expresión y aquí es donde intervienen la educación y la inteligencia humana para preservar la espiritualidad de nuestra sociedad y no transformarnos en un mundo sin valores y sin cultura.

[717] Rodríguez Uribes, J. M. (1999) *Opinión pública. Concepto y modelos históricos*. Editorial Marcial Pons, Madrid, pp. 104-105.

Capitulo VIII. Las limitaciones de los derechos fundamentales

Entre los derechos fundamentales, sólo unos pocos han sido consagrados en las leyes de los Estados y en la doctrina teniendo un valor absoluto e intangible: el derecho a no ser sometido a tortura o a tratos inhumanos o degradantes, la prohibición de la esclavitud. Considerando que el reconocimiento de los derechos y de las libertades fundamentales es posible siempre que sean coherentes no sólo con los intereses individuales de los titulares, sino también con los intereses generales de la sociedad, la mayoría de ellos son derechos relativos o condicionales, sometidos a limitaciones establecidas únicamente en virtud de la ley y que no deben afectar a la esencia de los derechos en sí.

El acepto de la posibilidad de establecer limitaciones se origina en los primeros instrumentos internacionales de derechos humanos, como la Declaración Universal de Derechos Humanos[718], o en el Convenio Europeo de Derechos Humanos[719] y más tarde en la legislación nacional de los Estados parte.

La legislación de los Estados sigue el modelo internacional y europeo en la materia, teniendo en cuenta las condiciones establecidas para determinar "los límites de las limitaciones". Dentro de los diversos instrumentos jurídicos nacionales o internacionales, la determinación de las limitaciones de los derechos se lleva a cabo de manera general, aplicable a todos los derechos, o personalizada para cada derecho relativo. La terminología utilizada en relación con las limitaciones de los derechos es compleja, a menudo siendo utilizadas también nociones como "injerencias", "restricciones", "limitaciones", "afectaciones", todas siendo nociones equivalentes, como se observa en la doctrina, todas siendo limitaciones de los derechos para sus titulares[720].

En general, las actividades de limitar el ejercicio de un derecho se dividen en dos categorías: limitaciones derivadas de la necesidad de respetar los derechos de los demás y limitaciones impuestas por la protección de los objetivos del interés general. La competencia para establecer estas limitaciones pertenece únicamente al legislador

[718] Artículo 29.2: En el ejercicio de sus derechos y en el disfrute de sus libertades, toda persona estará solamente sujeta a las limitaciones establecidas por la ley con el único fin de asegurar el reconocimiento y el respeto de los derechos y libertades de los demás, y de satisfacer las justas exigencias de la moral, del orden público y del bienestar general en una sociedad democrática.
[719] Artículo 18: Las restricciones que, en los términos del presente Convenio, se impongan a los citados derechos y libertades no podrán ser aplicadas más que con la finalidad para la cual hayan sido previstas.
[720] Bîrsan, C. (2010) *Conventia europeana a drepturilor omului. Comentariu pe articole* (*El Convenio Europeo de Derechos Humanos. Comentarios sobre los artículos*), Edición 2, C.H. Beck, Bucarest.

(constitucional u ordinario) obligado para tener en cuenta una serie de criterios para no afectar al fondo los derechos sujetos a limitaciones. Algunas constituciones nacionales imponen que las leyes con tal objeto regulador tengan un carácter general y abstracto y que no produzca efectos retroactivos[721].

Para seguir en la zona legal y constitucional, los "límites de las limitaciones" deben ser reguladas por la ley y, al mismo tiempo, son necesarias garantías jurisdiccionales, a nivel de los tribunales ordinarios o contencioso constitucional. El incumplimiento de estos criterios se castiga con una apelación ante los tribunales supranacionales, si se necesita. De ellos, La Organización para la Cooperación y el Desarrollo Económico ha desarrollado una literatura jurídica muy rica en materia de injerencias. La necesidad de los "límites de las limitaciones" se basa en el postulado establecido por la doctrina del derecho constitucional, según el cual cualquier intromisión de un Estado en la vida privada del individuo llevada a cabo sin consentimiento es inconstitucional, ya que el poder del estado está intrínsecamente limitado, como resultado del reconocimiento del principio constitucional de la preeminencia del derecho sin el cual ningún "contrato social" ya no sería libre y democrático[722].

Consiguientemente, las consideraciones anteriores son válidas en el caso del derecho a la vida privada, que también es un derecho relativo, que puede estar sujeto a limitaciones (injerencias) por parte de las autoridades. Sobre la base de las reglamentaciones nacionales, pero también de la jurisprudencia del T.E.D.H[723]. Al respecto, se han determinado una serie de condiciones que deben cumplirse de manera acumulativa para que una injerencia se considere aceptable:

• *La injerencia debe estar prevista por la ley*. "La ley", en la interpretación dada por el T.E.D.H.[724], es una noción autónoma, que no se considera stricto sensu, formalmente, sino en sentido material, abarcando tanto en su contenido actos normativos con poder jurídico, como en jurisprudencia, con el fin de no crear discrepancias entre el sistema de *common law* y el sistema continental. Con respecto a la normativa escrita en el derecho

[721] Romboli, R. (2018) *La influencia del C.E.D.H. y de la jurisprudencia del T.E.D.H. en el ordenamiento constitucional italiano*. Revista Teoría y Realidad Constitucional, núm. 42/2018, pp. 187-220.
[722] Böckenförde, E. W. (1993*) Escritos sobre derechos fundamentales*, trad. de Juan Luis Requejo Pagés e Ignacio Villaverde Menéndez, 1.a ed., Editorial Nomos Verlagsgesellschaft, Baden-Baden.
[723] Bogdan, D. y Selegean, M. (2005) *Drepturi şi libertăţi în jurisprudenţa Curţii Europene a Drepturilor Omului (Derechos y libertades en la jurisprudencia del Tribunal Europeo de Derechos Humanos),* Editorial All Beck Publishing House, Bucarest, pp. 380-381
[724] T.E.D.H., Sentencia de 30 de julio de 1998, no. 27671/95, Caso Valenzuela Contreras contra España.

nacional, ésta contiene todos los actos jurídicos emanados de las autoridades competentes de un estado, a saber: Constitución, leyes, actos de reglamentación basados en leyes, actos de carácter normativo de la administración pública central y local, convenios internacionales aplicables en el derecho nacional.

Por otra parte, no basta con que una injerencia sea prevista por la ley, ésta debe satisfacer a su vez determinados requisitos que, en cada caso, se evalúan en función del contenido, el alcance, el número y la calidad de los destinatarios de la ley:

a) *Accesibilidad*. Esta calidad de la ley (o de la jurisprudencia relevante, si es necesario) implica su publicidad o al menos la disponibilidad hacia los destinatarios (poner en conocimiento), en el sentido de que éstos tenían la posibilidad de conocerla y consultarla[725];

b) *Predictibilidad*. A tal fin, la ley/la jurisprudencia debe tener suficiente precisión y claridad, de modo que los destinatarios a los que se dirigen sean conscientes de que están dirigidos por las normas que deben cumplir en su comportamiento. Este requisito se considera relativo, refiriéndose en particular a la comprensión que pueden manifestar los profesionales del derecho, los especialistas, que pueden aconsejar a los otros destinatarios "profanos";

c) *Garantías independientes*. A tal fin, se considera que los mecanismos más eficaces son los de control independiente, en particular, de carácter jurisdiccional.

• *La injerencia debe tener un propósito legítimo*. El objetivo legítimo está representado por las causas por las que el Estado puede interferir en la vida privada de un individuo y que figuran expresamente en algunas Constituciones (art. 53.1. de la Constitución de Rumanía o art. 55 de la Constitución Española) o en las convenciones internacionales: la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de delitos penales, la protección de la salud o de la moral, o la protección de los derechos y de las libertades de los demás, la prevención de las consecuencias de una calamidad natural, un desastre o un siniestro particularmente grave.

[725] Por ejemplo, en la sentencia T.E.D.H. de 12 de mayo de 2000, Khan c. Reino Unido (No. 35394/97), se consideró una violación del art. 8 de la Convención, 8 de la Convención, al no respetar la accesibilidad de la ley, ya que el reglamento del Ministerio del Interior británico, en ese momento, que regulaba las condiciones en las que se podían instalar y utilizar equipos para grabar y grabar conversaciones, no era accesible al público.

Estos motivos son circunstancias fácticas, que permanecen en primer lugar, del legislador, en el momento de la regulación de tales limitaciones y, en segundo lugar, a la apreciación del juez (nacional o europeo) en situaciones concretas, cuando las limitaciones se analizarán en función de las circunstancias, caso por caso.

• *La injerencia debe ser necesaria en una sociedad democrática*. Esta frase pretende establecer unos límites a la necesidad, por la configuración de una necesidad social imperiosa, a la que le corresponda su injerencia, y a la proporcionalidad de la necesidad con el fin legítimo perseguido[726]. La necesidad social imperiosa debe basarse en motivos pertinentes y suficientes, es decir, aquellas circunstancias que obliguen al Estado a adoptar una determinada medida de restricción del derecho a la vida privada, adecuada y eficaz para alcanzar la finalidad prevista[727].

La exigencia de respetar la proporcionalidad, un justo equilibrio entre propósito y derecho, de hecho, entre diferentes intereses, se examina en función de la naturaleza y la importancia del derecho, el objetivo legítimo perseguido, la gravedad de la injerencia, la existencia o no de un denominador común para los sistemas jurídicos de los Estados (consenso europeo). En relación con esta tercera condición, basada en la premisa del carácter subsidiario del control judicial europeo hacia los sistemas nacionales de garantía de los derechos humanos, el T.E.D.H. se ha dedicado *a la teoría de la límite de apreciación*[728], es decir, en la que el control judicial del Tribunal es uno sobre la oportunidad, basada en la presunción de que la injerencia de los Estados puede explicarse por la preocupación de garantizar el orden público y los intereses superiores de su nación.

No obstante, el T.E.D.H. puede intervenir si considera que se ha superado este margen, respectivamente, si las medidas adoptadas por el Estado se interpretan como arbitrarias, excesivas, fuera de los límites de su facultad discrecional.

A nivel de los organismos de las Naciones Unidas, se utilizan los mismos criterios identificados por el T.E.D.H., añadiendo que, si una injerencia esté prevista por la ley, ésta debe estar de acuerdo con las disposiciones, los propósitos y los objetivos

[726] Sentencia T.E.D.H. de 7 de diciembre de 1976 en *Handyside c. Reino Unido* (No. 5493/72), Sentencia T.E.D.H. de 24 de marzo de 1988, *Olsson c. Suecia* (No. 10465/83).
[727] Sentencia T.E.D.H. de 27 de septiembre de 1999, Caso Smith y Grady contra Reino Unido (No 33985/96 y 33986/96) - aunque ha reconocido el derecho del Estado a imponer ciertas restricciones al derecho a la vida privada en situaciones en las que existe una amenaza real a la efectividad operativa de las fuerzas armadas, sin embargo, la realización de investigaciones sobre las inclinaciones homosexuales de los militares constituye una interferencia incompatible con los requisitos del art. 8. 2. de la Convención.
[728] Sentencia T.E.D.H. de 18 de junio de 1971, De Wilde, Ooms And Versyp ("Vagrancy") c. Bélgica (No. 2832/66; 2835/66; 2899/6618).

establecidos en el Pacto Internacional de Derechos Civiles y Políticos. En cualquier caso, tiene que ser razonables en las circunstancias particulares, ser proporcionada al propósito perseguido y necesaria en esa situación específica[729].

Los "titulares" de las injerencias al derecho a la vida privada pueden ser cualesquiera de las autoridades pertenecientes a uno de los tres poderes clásicos (legislativo, ejecutivo, judicial) y la acción imputable puede ser cometida incluso por un agente de estas autoridades, actuando en su calidad oficial. A este respecto, la función del juez es de censurar el cumplimiento de los "límites de las limitaciones", equilibrando el límite *de apreciación* dejado a las autoridades estatales para establecer si existe una injerencia y que efectos jurídicos produce sobre el derecho del individuo a la vida privada.

Considerando que no es posible apoyar la existencia de una jerarquía entre los distintos derechos fundamentales en caso de "colisión" entre el derecho a la vida privada y el interés general u otros derechos, a fin de determinar si la injerencia en el derecho a la vida privada es o no es una permitida, es necesario tener en cuenta las circunstancias específicas de cada caso. Igualmente, a nivel supranacional, se puede decir que la jurisprudencia de los tribunales de este grado (como el T.E.D.H.) tiene por objeto regular la conducta de los estados, a fin de no exceder los límites que el poder de la injerencia permite en la vida privada, para evitar la adopción (o repetición) de medidas arbitrarias, en esencia, para contribuir de manera unificada e integrada a garantizar la supremacía del derecho.

8.1. El derecho a la seguridad y la vigilancia

La vigilancia y las restricciones de algunas libertades fundamentales que mejoran la seguridad de la persona no necesita ser demasiado invasiva o alterar la vida. No es como si los agentes del gobierno necesitaran buscar físicamente a todos y cada uno de los sospechosos o aquellos conectados a un sospechoso. Los avances en la tecnología digital han hecho que dicha vigilancia sea relativamente discreta. El video monitoreado, los sistemas de posicionamiento global (GPS), los escáneres corporales de aeropuertos y las tecnologías biométricas, junto con la vigilancia de datos, brindan a los funcionarios encargados de hacer cumplir la ley herramientas de vigilancia, sin sobrecargar demasiado a los observados. En contra de este punto de vista, hay personas que sostienen que

[729] Nicholas Toonen v. Australia, Comunicación No. 488/1992, U.N. Doc. CCPR/C/50/D/488/1992 (1994), recuperado de: http://hrlibrary.umn.edu/hrcommittee/spanish/488-1992.html.

deberíamos estar preocupados por esta propuesta de intercambio de la privacidad por la seguridad. Se argumenta que los delincuentes y terroristas no son tan peligrosos como los gobiernos.

Hay demasiados ejemplos para que podamos negar el dicho de Lord Acton[730] de que "*El poder tiende a corromper y el poder absoluto corrompe absolutamente*"[731]. Si el control de la información alimenta el poder y el conocimiento total de la información expande radicalmente ese poder, entonces tenemos buenas razones para meditar y analizar antes de cambiar la privacidad por la seguridad.

Como es de conocimiento público, los gobiernos y las corporaciones son notoriamente los más interesados para exigir acceso a la información. Un reciente contra movimiento a esta tendencia es la aparición de sitios de intercambio de información en línea dedicados a destacar las actividades internas de las agencias y corporaciones gubernamentales. Por ejemplo, los sitios web como WikiLeaks prometen cambiar el "panorama de responsabilidad" y sacar a la luz los abusos en contra los derechos y libertades de las personas.

Las personas tienen derecho al respeto de la vida privada que limitan a las actividades de vigilancia de los gobiernos. Si bien no es un derecho absoluto, el protege a las personas de las miradas indiscretas de los vecinos, las corporaciones y el estado. La pregunta que planteamos en este análisis es una cuestión de equilibrio: ¿cuándo son los intereses de seguridad lo suficientemente importantes como para limitar los derechos de privacidad de los ciudadanos? Hay varias teorías sobre la respuesta a esta pregunta.

Una forma de lograr un equilibrio entre la vida privada y la seguridad es dejar que las autoridades estatales decidan. En esta teoría, los ciudadanos deben confiar en las autoridades y en otros ciudadanos que tienen un cargo público con fines nobles: debemos dejarles decidir cómo proteger mejor la privacidad y la seguridad. Llamamos esta posición "solo confía en nosotros"[732].

Una segunda teoría minimiza los intereses de privacidad poniendo en duda las actividades que la privacidad puede proteger[733]. Este punto de vista, llamado "nada que

---

[730] John Emerich Edward Dalberg-Acton, 1.er Barón Acton, (10 de enero de 1834, Nápoles, Reino de Nápoles - 19 de junio de 1902, Tegernsee, Baviera, II Imperio alemán), conocido como Lord Acton, fue un historiador y político inglés

[731] Pezzimenti, R. (2001) *The Political Thought of Lord Acton: The English Catholics in the Nineteenth Century*, Editorial Millennium Romae 2000 AD.MM, p. 8

[732] Deeks, A. (2014) *An International Legal Framework for Surveillance*. Public Law and Legal Theory Research Paper Series 2014-53, vol. 52:2, pp. 292-368

[733] Margulies, P. (2014) *The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism*, Fordham Law Review vol.82, issue 5, recuperado de:

ocultar", sostiene que las personas no deben preocuparse por ser monitoreadas si no desarrollan actividades con potencial de afectar la vida, la seguridad o derechos de otras personas. Solo aquellos que participan en actividades inmorales e ilegales deben preocuparse por la vigilancia del gobierno. Similar a "nada que ocultar" es la opinión de que "la seguridad triunfa". Esta última cuenta sostiene que los intereses de seguridad son, por su naturaleza, más importantes que los derechos de privacidad.

Opiniones más recientes[734] argumentan que, para proteger tanto la vida privada del ser humano como su seguridad, es importante tener una supervisión pública del proceso y el razonamiento involucrados en el procedimiento judicial para emitir órdenes de arresto o de restricción de derechos fundamentales en el nombre de la seguridad colectiva.

El derecho a la vida privada, así como hemos analizado en el capítulo VII, empodera a cada individuo a controlar el acceso a la propia persona, a los datos de sus ubicaciones o a otras informaciones sobre el mismo y es una condición necesaria para el bienestar o el desarrollo humano. Es decir, existe bastante evidencia convincente de que las personas que carecen de este tipo de control sufren física y mentalmente.

La seguridad también es valiosa. Ya sea derivada de los derechos individuales de autodefensa o desde la filosofía del contrato social, una función legítima de cualquier gobierno es proteger los derechos de sus ciudadanos. En el nivel más básico, la seguridad brinda a las personas el control sobre sus vidas, proyectos y propiedades. Estar seguro supone tener soberanía sobre un dominio privado; es estar libre de interferencias injustificadas de otros individuos, corporaciones y gobiernos. La seguridad también protege a los proyectos y propiedades de los grupos, empresas y corporaciones de interferencias injustificadas. Sin este tipo de control, las empresas y corporaciones no podrían operar en un mercado libre por mucho tiempo[735].

Es difícil definir el derecho a la seguridad. Por ejemplo: Rhonda Powell expresa su preocupación por el hecho de que la doctrina y los textos sobre los derechos humanos no han ofrecido hasta ahora una definición clara del concepto de seguridad: "*simplemente se supone que la seguridad se entiende claramente y se puede dar por sentado"*[736]. En

https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=4980&context=flr

[734] Moore, A. D. (2010) *Privacy Rights: Moral and Legal Foundations*, Editorial University Park, PA: Penn State University Press.

[735] Whitmant, J. Q. (2004) *The Two Western Cultures of Privacy: Dignity Versus Liberty*. Liberty, 113 Yale L.J. Recuperado de: https://digitalcommons.law.yale.edu/ylj/vol113/iss6/1

[736] Powell, R. (2012) *The Concept of Security*, University of Oxford Socio-Legal Review, no.1, p. 6.

términos simples, Hein van Kempen manifiesta que la seguridad se describe como estar libre de amenaza, peligro, vulnerabilidad, amenaza, fuerza y ataque[737]. Pero la "naturaleza más bien básica de esta definición" no debe ocultar el hecho de que hay muchas formas diferentes de seguridad, y que el significado está en desarrollo y es muy controvertido.

Citando a Hein van Kempen, el derecho a la seguridad es un derecho de primera generación, un derecho "civil y político", "negativo"; un escudo ante una intromisión del Estado. Como se demostró, los derechos de primera generación protegen a las personas de asesinatos, torturas, esclavitud, actos arbitrarios, etc. El derecho *sustantivo a la seguridad* del individuo ante el poder del Estado, que lo distingue de su elemento "*procesal*"[738], está expresamente previsto en varios documentos internacionales y regionales de derechos humanos.

El artículo 5, apartado 1, del Convenio Europeo de Derechos Humanos se expresa en términos similares: *"1. Toda persona tiene derecho a la libertad y a la seguridad. Nadie puede ser privado de su libertad, salvo en los casos siguientes y con arreglo al procedimiento establecido por la ley: a) Si ha sido privado de libertad legalmente en virtud de una sentencia dictada por un tribunal competente; b) Si ha sido detenido o privado de libertad, conforme a derecho, por desobediencia a una orden judicial o para asegurar el cumplimiento de una obligación establecida por la ley; c) Si ha sido detenido y privado de libertad, conforme a derecho, para hacerle comparecer ante la autoridad judicial competente, cuando existan indicios racionales de que ha cometido una infracción o cuando se estime necesario para impedirle que cometa una infracción o que huya después de haberla cometido; d) Si se trata de la privación de libertad de un menor en virtud de una orden legalmente acordada con el fin de vigilar su educación o de su detención, conforme a derecho, con el fin de hacerle comparecer ante*

[737] Van Kempen, P. H. (2013) *Four Concepts of Security – A Human Rights Perspective*, Human Rights Law Review 13, no.1.

[738] El Artículo 9 del Pacto Internacional de Derechos Civiles y Políticos explica los elementos procesales del derecho: "1. Todo individuo tiene derecho a la libertad y a la seguridad personales. Nadie podrá ser sometido a detención o prisión arbitrarias. Nadie podrá ser privado de su libertad, salvo por las ***causas fijadas por ley y con arreglo al procedimiento establecido en ésta***. 2. Toda persona detenida será informada, en el momento de su detención, de las razones de la misma, y notificada, sin demora, de la acusación formulada contra ella. 3. Toda persona detenida o presa a causa de una infracción penal ***será llevada sin demora ante un juez u otro funcionario autorizado por la ley para ejercer funciones judiciales, y tendrá derecho a ser juzgada dentro de un plazo razonable o a ser puesta en libertad***. La prisión preventiva de las personas que hayan de ser juzgadas no debe ser la regla general, pero su libertad podrá estar subordinada a ***garantías que aseguren la comparecencia del acusado en el acto del juicio, o en cualquier momento de las diligencias procesales*** y, en su caso, para la ejecución del fallo. 4. Toda persona que sea privada de libertad en virtud de detención o prisión ***tendrá derecho a recurrir ante un tribunal, a fin de que éste decida a la brevedad posible sobre la legalidad*** de su prisión y ordene su libertad si la prisión fuera ilegal".

la autoridad competente; e) Si se trata de la privación de libertad, conforme a derecho, de una persona susceptible de propagar una enfermedad contagiosa, de en enajenado, de un alcohólico, de un toxicómano o de un vagabundo; f) Si se trata de la detención o de la privación de libertad, conforme a derecho, de una persona para impedir su entrada ilegal en el territorio o contra la cual esté en curso un procedimiento de expulsión o extradición."

Pero la mayoría de los autores e investigadores en el ámbito de los derechos humanos examinan solo el elemento de *libertad* previsto en el artículo 5 (1), sin tener en cuenta la *seguridad*. En el asunto *East African Asians v. United Kingdom*, el Tribunal Europeo de Derechos Humanos sugirió que, aunque los términos deben ser interpretados en directa relación uno con el otro, *la protección de la "seguridad", en contexto, se refiere a toda interferencia arbitraria, por parte de una autoridad, con la libertad personal de un individuo*[739]. En otras palabras, cualquier decisión basada en el artículo 5 debe asegurar el derecho de la persona a la seguridad.

Muchos derechos humanos individuales, sin diferenciar si estén o no garantizados por instrumentos internacionales, regionales y/o nacionales, pueden ser restringidos por el Estado (no importa si es el Estado de residencia u otro Estado que estamos transitando) con fines legítimos, uno de los cuales es salvaguardar la seguridad. Por ejemplo, a nivel internacional, es importante analizar el artículo 19 (2) del Pacto Internacional de Derechos Civiles y Políticos que establece la libertad de expresión y también de buscar, recibir y difundir informaciones en cualquier formato y por todos los canales.

Pero, de acuerdo con el Artículo 19 (3) hay límites expresos a esta libertad: *"El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para: ... (b) Para la protección de la seguridad nacional o del orden público"*. La seguridad nacional, como una extensión estatal del derecho a la seguridad de cada ciudadano, se transforma en una razón de restricción del ejercicio de este derecho fundamental.

A nivel regional, el artículo 10 (1) del Convenio Europeo de Derechos Humanos garantiza el derecho a la libertad de expresión: *"Toda persona tiene derecho a la libertad*

[739] Commission (Plenary) Report (31), D.R. 78 A/B/5; EAST AFRICAN ASIANS C. ROYAUME-UNI, p. 99, disponible en: http://hudoc.echr.coe.int/eng?i=001-193001

de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades y sin consideración de fronteras".

Pero el apartado 2 del mismo Artículo 10, impone los límites del ejercicio del mismo derecho, en el nombre del interés de la seguridad nacional, la integridad territorial o la seguridad pública, para la prevención del desorden o el delito, etc., suponiendo que tales interferencias son necesarias: "*El ejercicio de estas libertades, que entrañan deberes y responsabilidades, podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones, previstas por la ley, que constituyan medidas necesarias, en una sociedad democrática, para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad del poder judicial".*

Además de estas "calificaciones" de aplicabilidad general, los textos legales relativos a los derechos humanos también añaden excepciones, suspendiendo libertades específicas, por ejemplo, momentos de "*emergencia pública que amenaza la vida de la nación*"[740].

A juicio de algunas opiniones[741] expresadas en la doctrina de los derechos humanos, el derecho de un individuo a la seguridad también se puede interpretar como un ejemplo de un derecho de "segunda generación", "económico, social y cultural", "positivo" del individuo; un "derecho a…". Tal como, el artículo 9 del Pacto Internacional de Derechos Económicos, Sociales y Culturales (*el Pacto, en adelante*) establece: *"Los Estados Parte en el presente Pacto reconocen el derecho de toda persona a la seguridad social, incluso al seguro social".*

Al mismo tiempo, el derecho a la seguridad también se extiende a la "tercera generación"[742], es el derecho "colectivo" de los pueblos y grupos de individuos. Por ejemplo, el Artículo 23 (1) de la Carta Africana sobre los Derechos Humanos y de los

[740] Rosen, J, (2001) *The Purposes of Privacy: A Response*. Recuperado de: https://ssrn.com/abstract=283988.
[741] Bidart Campos, G. (1994) *La interpretación del sistema de derechos humanos*, Editorial Ediar, Buenos Aires, Argentina;
[742] Hitoshi, N. (2013) *The Place of Human Security in Collective Security*, Journal of Conflict and Security Law 18, no.1, p. 97.

Pueblos[743] (Carta de Banjul) establece que: *"Todos los pueblos tendrán derecho a la paz y a la seguridad nacional e internacional. Los principios de solidaridad y de relaciones amistosas implícitamente afirmados por la Carta de las Naciones Unidas y reafirmados por la de la Organización para la Unidad Africana gobernarán las relaciones entre Estados"*.

La Carta de las Naciones Unidas también reconoce los derechos colectivos a la seguridad: uno de los propósitos de la ONU, según el Artículo 1 (1), es "mantener la paz y la seguridad internacionales [...]". Además, el Artículo 2 de la Carta obliga a los miembros de la ONU a *"arreglar sus controversias internacionales por medios pacíficos de tal manera que no se pongan en peligro ni la paz y la seguridad internacionales ni la justicia"* y deben *"abstenerse de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado [...]"*.

El derecho a la seguridad está consagrado también en los cuatro Convenios de Ginebra del año 1949. El Convenio Ginebra IV, por ejemplo, protege a los civiles en los conflictos armados. Este principio es extendido por los Protocolos Primero y Segundo de los Convenios, 1977. El Artículo 48 del Protocolo I establece que las Partes en conflicto deberán distinguir en todo momento entre la población civil y los combatientes y entre los objetivos civiles y militares y, en consecuencia, dirigirán sus operaciones solo contra los militares. Por esto, los ciudadanos no serán objeto de ataque, de conformidad con el artículo 51 (2).

Los estados están obligados, legalmente, a tomar todas las precauciones posibles al elegir armas y métodos de guerra que eviten la pérdida incidental de vidas, lesiones a civiles y daños a objetos civiles como hogares, escuelas, hospitales y lugares de culto, según el Artículo 52. Aquí podemos mencionar que estas obligaciones son vigentes y aplicable incluso en los ataques cibernéticos, porque las normas no distinguen, así como hemos presentado en los primeros dos capítulos de esta tesis.

Los Estados como parte del Protocolo (y en los cuatro Convenios de Ginebra) tienen la obligación expresa de buscar presuntos delincuentes, independientemente de su nacionalidad y del lugar del delito, y llevarlos ante sus propios tribunales o entregarlos a otra parte para juicio. En derecho internacional, este principio se conoce como *jurisdicción universal*.

[743] Aprobada el 27 de julio de 1981, durante la XVIII Asamblea de Jefes de Estado y Gobierno de la Organización de la Unidad Africana, reunida en Nairobi, Kenya

La "*seguridad humana*" representa un tema de interés para los organismos internacionales y es uno de los principios internacionales adoptados en la Cumbre Mundial de 2005:

> *"Seguridad humana: […] 143. Subrayamos el derecho de las personas a vivir en libertad y con dignidad, libres de la pobreza y la desesperación. Reconocemos que todas las personas, en particular las que son vulnerables, tienen derecho a vivir libres del temor y la miseria, a disponer de iguales oportunidades para disfrutar de todos sus derechos y a desarrollar plenamente su potencial humano. Con este fin, nos comprometemos a examinar y definir el concepto de seguridad humana en la Asamblea General"*[744].

Posteriormente, el tema fue mencionado en una resolución de la Reunión Plenaria de Alto Nivel de la Asamblea General de la ONU en septiembre de 2005, pero sin desarrollar el concepto. A pesar de, no existe un consenso real sobre qué significa exactamente la seguridad humana.

El concepto final de seguridad, por lo tanto, requiere que los estados tomen medidas *positivas* para evitar daños cometidos por terceros. Al proteger a las personas de las violaciones de los derechos por parte de actores no estatales (asesinatos, torturas, desapariciones forzadas, esclavitud, por ejemplo), los Estados, a nivel general, deben penalizar tales abusos y tomar activamente medidas para investigar, enjuiciar, condenar y castigar adecuadamente los responsables de tales violaciones.

Como conclusión podemos decir que el derecho a la seguridad implica dos tipos de obligaciones para los estados:

1. *una obligación negativa* – de abstenerse (sus autoridades) interferir en modo arbitrario con la libertad personal de un individuo.
2. *una obligación positiva* – de elaborar e implementar medidas y garantías para investigar, prevenir, enjuiciar, condenar y castigar los actos que afectan las libertades y derechos individuales cometidos por terceros.

[744] Resolución aprobada por la Asamblea General el 16 de septiembre de 2005/60/1. Documento Final de la Cumbre Mundial 2005. Disponible en: https://undocs.org/es/A/RES/60/1.

8.2. La vigilancia digital y las garantías legales del derecho a la vida privada

Aunque las amenazas al derecho a la vida privada en el ciberespacio son cualitativa y cuantitativamente nuevas, esta área no ha quedado fuera de la regulación en el ámbito de protección de los derechos humanos. Por ejemplo, la Observación general numero 16 aprobada por el Comité de Derechos Humanos (CDH)[745] en 1988 ha sentado las bases para la protección de los derechos de privacidad. El texto mencionado establece que la vigilancia electrónica, la interceptación de comunicaciones telefónicas y otras formas de comunicación y las escuchas telefónicas deben estar prohibidas. También establece que la recopilación y conservación de información personal por parte de las autoridades y los particulares debe estar regulada por la ley y que el propósito y el contenido de los datos personales deben ser transparentes para la persona en cuestión:

> *"Debe prohibirse la vigilancia, por medios electrónicos o de otra índole, la intervención de las comunicaciones telefónicas, telegráficas o de otro tipo, así como la intervención y grabación de conversaciones. Los registros en el domicilio de una persona deben limitarse a la búsqueda de pruebas necesarias y no debe permitirse que constituyan un hostigamiento"*[746].

Con estos requisitos generales, el CDH ha proporcionado una base legal sólida para el tema de la vigilancia digital. Pero debido el aumento de la vigilancia en todo el mundo, no resulta sorprende el aumento considerable de los casos de abusos sobre la vida privada de los individuos que el Comité tuvo que lidiar en los últimos cinco años[747].

Desde 2014, el Comité ha podido abordar diversos temas relacionados con la protección de los derechos cibernéticos[748]. La mayoría de las observaciones estaban relacionados con medidas antiterroristas. En el cuarto informe periódico sobre los Estados Unidos[749], en 2014, el Comité no solo analizó el régimen jurídico norteamericano sobre

---

[745] Las Observaciones generales adoptadas por el Comité de Derechos Humanos (CDH) con arreglo al párrafo 4 del artículo 40 del Pacto Internacional de Derechos Civiles y Políticos, núm. 1 a núm. 32 son disponibles en:https://conf-dts1.unog.ch/1%20SPA/Tradutek/Derechos_hum_Base/CCPR/00_2_obs_grales_Cte%20DerHum%20%5BCCPR%5D.html#GEN16

[746] CDH, 32º período de sesiones (1988) Observación general núm. 16 - Derecho a la intimidad (artículo 17).

[747] CDH, 95º período de sesiones (2009) Examen de los Informes presentados por los Estados parte de conformidad con el Artículo 40 del Pacto - Observaciones finales del Comité de Derechos Humanos – SUECIA/CCPR/C/SWE/CO/6 7 de mayo de 2009;
disponible en: https://undocs.org/es/CCPR/C/SWE/CO/6

[748] Idem.

[749] CDH - CCPR/C/USA/CO/4 - Concluding observations on the fourth periodic report of the United States of America, 23 de Abril 2014,

la vigilancia, sino también el sistema de otros países de América, Europa, Asia, África y Oceanía[750]. La variedad de leyes de vigilancia de los estados y las políticas revisadas demuestran que este es un problema universal que requiere atención global.

En sus recomendaciones, el Comité parte de la premisa de que las medidas de seguridad deben apuntar a prevenir la violencia y el terrorismo[751]:

> *"El Comité es consciente de que el Estado parte considera que la intervención en las comunicaciones telegráficas y telefónicas es un importante instrumento de investigación, pero estima que el recurso a las grabaciones telegráficas y telefónicas debería reducirse al mínimo de manera que solo se reúnan pruebas pertinentes y que un juez debería supervisar el empleo de este medio. Inquieta además al Comité la conclusión de la Junta de Protección de Datos de que las grabaciones de conversaciones telefónicas en las que intervienen profesionales sujetos al deber de confidencialidad, en especial abogados, no están protegidas de manera que se preserve la confidencialidad entre el abogado y su cliente (art. 17)".*

Si un Estado Parte del Pacto adopta tales medidas, las autoridades deben ser conscientes que están obligadas a respetar los mismos estándares de protección sin importar el medio de acción, en línea o fuera de línea[752]:

"Tomando nota de los informes del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, presentados al Consejo de Derechos Humanos en su 17º período de sesiones y a la Asamblea General en su 66º período de sesiones, relativos a la libertad de expresión en Internet,

---

disponible en: https://www.refworld.org/docid/5374afcd4.html

[750] CDH - Concluding Observations on the Sixth Periodic Report of Canada, 13 de Agosto 2015, UN Doc CCPR/C/CAN/CO/6, para. 10; Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, 17 de Agosto 2015, UN Doc CCPR/C/GBR/CO/7, para. 24; Concluding Observations on the Second Periodic Report of Turkmenistan, 20 de Abril 2017, UN Doc CCPR/C/TKM/CO/2, paras. 36–37; HRC, Concluding Observations on the Second Report of Namibia, 22 de Abril 2016, UN Doc CCPR/C/NAM/CO/2, para 38; Concluding Observations on the Sixth Periodic Report of New Zealand, 28 de Abril 2016, UN Doc CCPR/C/NZL/CO/6, paras. 15–16.

[751] Para analizar las condiciones del reconocimiento de las escuchas telefónicas y la interceptación de mensajes de texto, como una herramienta de investigación, véase, por ejemplo, CDH, Examen de los informes presentados por los Estados parte de conformidad con el artículo 40 del Pacto, Observaciones finales del Comité de Derechos Humanos, Países Bajos, 25 de agosto de 2009, Doc. ONU CCPR / C / NLD / CO / 4, párr.14.

[752] CDH, 20º período de sesiones (2012) Tema 3 de la agenda - Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo, Promoción, protección y disfrute de los derechos humanos en Internet - 29 de junio de 2012, disponible en: https://documents-dds-ny.un.org/doc/UNDOC/LTD/G12/147/13/PDF/G1214713.pdf?OpenElement

1. Afirma que ***los derechos de las personas también deben estar protegidos en Internet****, en particular la libertad de expresión, que es aplicable sin consideración de fronteras y por cualquier procedimiento que se elija, de conformidad con el artículo 19 de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos;*

2. Reconoce ***la naturaleza mundial y abierta de Internet*** *como fuerza impulsora de la aceleración de los progresos hacia el desarrollo en sus distintas formas;*

3. Exhorta a los Estados a que ***promuevan y faciliten el acceso a Internet*** *y la cooperación internacional encaminada al desarrollo de los medios de comunicación y los servicios de información y comunicación en todos los países;*

4. ***Alienta a los procedimientos especiales*** *a que tengan estas cuestiones en cuenta en sus mandatos actuales, según proceda;*

5. Decide seguir examinando ***la promoción, la protección y el disfrute de los derechos humanos, incluido el derecho a la libertad de expresión, en Internet y en otras tecnologías****, así como la forma en que el internet puede ser un importante instrumento para el desarrollo y para el ejercicio de los derechos humanos, de conformidad con su programa de trabajo".*

Consecuentemente, cualquier medida antiterrorista debe cumplir con los requisitos establecidos en el artículo 17. El Comité ha criticado los programas de vigilancia masiva[753] y el desarrollo de amplios procesos de vigilancia de las comunicaciones electrónicas sin las garantías necesarias para proteger el derecho a la vida privada y a la correspondencia[754]:

> *"El Estado parte debería adoptar todas las medidas adecuadas para velar por que la reunión, el almacenamiento y el uso de datos personales no sean objeto de abuso, no se usen para fines contrarios al Pacto y estén en consonancia con las obligaciones impuestas por el artículo 17 del Pacto. A estos efectos, el Estado parte debería garantizar que el procesamiento y la reunión de esas*

[753] CDH, Concluding Observations on the Sixth Periodic Report of Canada, 13 de Agosto 2015, UN Doc CCPR/C/CAN/CO/6, para 10;
[754] CDH, 95º período de sesiones, Examen de los Informes presentados por los Estados parte de conformidad con el Artículo 40 del Pacto - Observaciones finales del Comité de Derechos Humanos – SUECIA/CCPR/C/SWE/CO/6 7 de mayo de 2009;

informaciones son objeto de examen y supervisión por un órgano independiente con las necesarias garantías de imparcialidad y eficacia".

Entre los temas más analizados, fue la cuestión de si los Estados parte pueden exigir a las partes privadas que almacenen los datos infinitamente, en qué circunstancias las autoridades pueden obtener acceso a dichos datos y en qué medida la comunicación recibida o enviada fuera del país está protegida contra la intercepción.

El alcance de la protección en virtud del artículo 17 del Pacto es amplio. No solo protege la información sustantiva contenida en cualquier comunicación, sino también los metadatos, es decir, los datos que proporcionan información sobre otros datos. Los metadatos, como parte del proceso de comunicación, pueden proporcionar información confidencial sobre la vida privada de un individuo, permitiendo la construcción de un perfil personal integral. Por ende, también merece protección legal[755].

Además, la comunicación y los datos considerados como no confidenciales deben estar protegidos, porque el intercambio público de datos e información no puede dejar desprotegida la sustancia de la correspondencia. Si tales datos se acumulan, pueden usarse para generar perfiles personales y esto permite al titular de los datos familiarizarse con la vida privada del interesado. Por lo tanto, la protección bajo el artículo 17 también se extiende a la información, que se comparte en áreas públicas, incluidas las redes sociales, como Facebook. Por eso, el Comité criticó a Colombia por excluir el dominio público de la protección legal de la privacidad solo por su libre acceso[756]:

"El Comité lamenta no haber recibido información actualizada acerca del avance de las investigaciones relativas a las presuntas actividades ilegales de seguimiento que habrían sido realizadas por funcionarios del antiguo Departamento Administrativo de Seguridad y nota con preocupación las alegaciones sobre actividades ilegales de vigilancia contra periodistas que habrían tenido lugar durante el período en estudio. Asimismo, al Comité le

[755] Naciones Unidas, Asamblea General - Septuagésimo primer período de sesiones Tercera Comisión Tema 68 b) del programa Promoción y protección de los derechos humanos: cuestiones de derechos humanos, incluidos otros medios de mejorar el goce efectivo de los derechos humanos y las libertades fundamentales, El derecho a la privacidad en la era digital, disponible en: https://www.acnur.org/fileadmin/Documentos/BDL/2017/10904.pdf

[756] CDH - Observaciones finales sobre el séptimo informe periódico de Colombia - 17 de noviembre de 2016, disponible en: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR/C/COL/CO/7&Lang=Sp

preocupa que en el desarrollo del «monitoreo del espectro electromagnético» contenido en el artículo 17 la Ley 1621 de 2013 pudieran presentarse en la práctica injerencias en las comunicaciones privadas realizadas a través del espectro electromagnético que no estén sujetas a una estricta evaluación de legalidad, necesidad y proporcionalidad. Le preocupa también que el nuevo Código de Policía, que entrará en vigor en enero de 2017, prevea una definición muy amplia de lo que es espacio público, que incluye el espectro electromagnético, y que toda la información y los datos recolectados en los espacios públicos sean considerados públicos y de libre acceso (art. 17)".

Cualquier interferencia con datos personales que sea relevante para la privacidad de un individuo debe ser probada según los estándares del artículo 17. La interferencia incluye cualquier vigilancia digital que incluya, tal como la vigilancia en línea, interceptación de comunicación digital, escuchas telefónicas, piratería informática, extracción de bases de datos, explotación de redes informáticas, recopilación de metadatos, procesamiento, almacenamiento y uso compartido, retención obligatoria de datos y acceso a los mismos. Dicha vigilancia digital puede tomar la forma de vigilancia dirigida con objetivos concretos basados en una sospecha individualizada o vigilancia general (masiva).

8.3. Estándares de protección del derecho a la vida privada frente a la vigilancia digital

Las normas clave de protección que el Comité ha reconocido hasta ahora son de naturaleza sustantiva y procesal.

A. Normas de protección de naturaleza sustantiva

En primer lugar, la interferencia no debe ser de naturaleza arbitraria[757]. Por lo tanto, cualquier intercepción ilimitada está prohibida por el Pacto. En la mayoría de sus informes y observaciones, el Comité ha expresado su preocupación por los poderes

[757] Según la Observación general no. 35 del Comité, el término arbitrario incluye elementos de razonabilidad, necesidad y proporcionalidad, véase ONU: Comité de Derechos Humanos (CDH), *Observación general Nº 35: Artículo 9 (Libertad y seguridad personales)*, 16 diciembre 2014, CCPR/C/GC/35, disponible en: https://www.refworld.org.es/docid/553e0fb84.html

excesivos o vagos[758] de las autoridades estatales[759] que conducen a la intercepción masiva[760] por culpa de la ausencia de un mecanismo de supervisión independiente. Por ejemplo, en sus Observaciones finales sobre el cuarto informe de los Estados Unidos, el Comité criticó el programa de vigilancia de metadatos de teléfonos en virtud de la Ley Patriota de los Estados Unidos, la vigilancia extranjera a través de PRISM, que permite la recopilación de comunicaciones de empresas de Internet con sede en EE. UU., como Google y Facebook, y el programa UPSTREAM que recoge comunicaciones de la red troncal de Internet (de los principales cables e switches)[761]:

> *"El Comité está preocupado por la vigilancia de las comunicaciones en aras de la protección de la seguridad nacional, tanto dentro como fuera de los Estados Unidos, llevada a cabo por la Agencia de Seguridad Nacional a través del programa general de vigilancia de metadatos telefónicos (artículo 215 de la Ley PATRIOTA) y, en particular, por la vigilancia que, en aplicación del artículo 702 de la Ley de enmienda de la Ley de Vigilancia de la Inteligencia Extranjera, se lleva a cabo a través del programa PRISM (recopilación de los contenidos de las comunicaciones de empresas de Internet con sede en los Estados Unidos), y el programa UPSTREAM (recopilación de los metadatos y los contenidos de comunicaciones mediante la intervención de cables de fibra óptica que transportan datos de Internet) y su adversa repercusión en el derecho a la intimidad de las personas".*

Para remediar los problemas relacionadas con el respeto de los derechos humanos y la falta de garantías efectivas para la protección jurídica de estos derechos, el Estado parte, es decir los E.E. U.U., deberá:

"a) Adoptar todas las medidas necesarias para garantizar que sus actividades de vigilancia, tanto dentro como fuera de los Estados Unidos, se ajusten a las obligaciones que le incumben en virtud del Pacto, incluido el artículo 17; en particular, deben

---

[758] CDH, Concluding Observations on the Sixth Periodic Report of New Zealand, 28 April 2016, UN Doc CCPR/C/NZL/CO/6, paras 15–16

[759] CDH, Concluding Observations on the Fifth Periodic Report of France, 17 August 2015, UN Doc CCPR/C/FRA/CO/5, para 12.

[760] CDH, Concluding Observations on the Initial Report of South Africa, 27 April 2016, UN Doc CCPR/C/ZAF/CO/1, paras. 42–43; CDH, Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, 17 August 2015, UN Doc CCPR/C/GBR/CO/7, para 24; CDH, Concluding Observations on the Sixth Periodic Report of Denmark, 15 August 2016, UN Doc CCPR/C/DNK/CO/6, para 27;

[761] CDH, Observaciones finales sobre el cuarto informe periódico de los Estados Unidos de América, 23 abril 2014, disponible en: https://undocs.org/es/CCPR/C/USA/CO/4

adoptarse medidas para que toda interferencia en el derecho a la intimidad se ajuste a los principios de legalidad, proporcionalidad y necesidad, con independencia de la nacionalidad o el emplazamiento de las personas cuyas comunicaciones estén bajo vigilancia directa;

b) Asegurarse de que cualquier interferencia en el derecho a la intimidad, la familia, el hogar o la correspondencia esté autorizada por leyes que: i) sean de acceso público; ii) contengan disposiciones que garanticen que la obtención, el acceso y la utilización de los datos de las comunicaciones obedezcan a objetivos específicos legítimos; iii) sean suficientemente precisas y especifiquen en detalle las circunstancias concretas en que estas interferencias pueden ser autorizadas, los procedimientos de autorización, las categorías de personas que pueden ser sometidas a vigilancia, el límite de la duración de la vigilancia y los procedimientos para el uso y el almacenamiento de los datos recopilados, y iv) proporcionen salvaguardias efectivas contra las violaciones;

c) Reformar el actual sistema de supervisión de las actividades de vigilancia para garantizar su eficacia, entre otras cosas disponiendo la intervención judicial en la autorización o supervisión de las medidas de vigilancia, y considerando la posibilidad de establecer mandatos de supervisión consistentes e independientes con el fin de evitar abusos;

d) Abstenerse de imponer la retención obligatoria de datos por terceros;

e) Asegurar que las personas afectadas tengan acceso a recursos efectivos en casos de abuso"[762].

Según la Observación general No. 16 del Comité, una interferencia con el derecho a la vida privada debe ser de conformidad con las disposiciones, fines y objetivos del Pacto y debe ser, en cualquier caso, razonable en las circunstancias particulares[763]. En otras palabras, la interceptación de la comunicación requiere un objetivo específico y legítimo[764]. En el caso de Suiza, el Comité consideró que la referencia al "interés nacional" era demasiado amplia[765]. Cualquier interferencia debe estar en línea con los

[762] Ibidem.
[763] CDH, CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honor and Reputation, 8 April 1988, disponible en: https://www.refworld.org/docid/453883f922.html
[764] UN Doc CCPR/C/FRA/CO/5 (n 23) para 12; CDH, Concluding Observations on the Fourth Periodic Report of Rwanda, 2 May 2016, UN Doc CCPR/C/RWA/CO/4, para 36.
[765] HRC, Concluding Observations on the Fourth Periodic Report of Switzerland, 22 August 2017, UN Doc CCPR/C/CHE/CO/4, para 46

principios de legalidad, necesidad y proporcionalidad[766] y de naturaleza no discriminatoria[767]. Información privilegiada, como la información que se aplica a las fuentes periodísticas y otras profesiones que requieren confidencialidad, como la correspondencia entre el abogado y el cliente y los registros médicos, requieren normas más estrictas de protección. Asimismo, se aplicarán las mismas garantías independientemente de la nacionalidad de la persona afectada por la medida de vigilancia.

Consiguientemente, el Comité criticó a Polonia por aplicar diferentes criterios para la interceptación de ciudadanos extranjeros[768].

En la misma línea, pidió a Nueva Zelanda que implemente suficientes garantías judiciales "independientemente de la nacionalidad" de la persona afectada[769]:

> *"El proyecto de ley sobre comunicaciones digitales perjudiciales tiene por objeto mitigar el daño que pudiera derivarse de las comunicaciones digitales y proporcionar a las víctimas un medio rápido y eficaz de obtener una reparación. Abarca todas las formas de comunicación electrónicas, como mensajes de correo electrónico, textos, observaciones en bitácoras y mensajes en redes sociales como Facebook y Twitter, que puedan utilizarse para acosar, hostigar e intimidar a otros. En el proyecto de ley se contempla como un nuevo delito causar daño mediante la publicación de una comunicación digital, delito que se castiga con una pena máxima de dos años de prisión".*

B. Normas de protección de naturaleza procesal

La mayoría de los pronunciamientos del Comité hasta la actualidad se han ocupado de garantías procesales. Dado que los recursos individuales ex ante contra las medidas de supervisión son limitados en lo que respecta a la vigilancia, la protección de la privacidad es esencialmente una cuestión de regulación, protección procesal, especialmente la autorización y la supervisión independiente adecuada. El secreto de los

---

[766] CDH, Observaciones finales sobre el quinto informe periódico de Francia, 17 de agosto de 2015, disponible en: http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsias1RuYOs%2BUFEMWGcUshNyuKpKH1Sf7QroKxWkQSQoBsMu4Atlmowwkq1WWb0X0cmW4RunM0nfJSdJn4a44ERwCJRaKetUhzgckbBtFyCgZ.

[767] CDH, Concluding Observations on the Seventh Periodic Report of Poland, 23 November 2016, UN Doc CCPR/C/POL/CO/7, para 39; UN Doc CCPR/C/NZL/CO/6 (n 22) para. 15.

[768] UN Doc. CCPR/C/POL/CO/7 (n 31) para. 39

[769] CDH, Examen de los informes presentados por los Estados parte en virtud del artículo 40 del Pacto con arreglo al procedimiento facultativo de presentación de informes Sexto informe periódico que los Estados parte debían presentar en 2015 Nueva Zelandia, 24 de julio de 2015, disponible en: https://undocs.org/es/CCPR/C/NZL/6

servicios de inteligencia requiere un marco de procedimiento detallado para proteger a las personas de la interferencia arbitraria con sus derechos de privacidad, independientemente de si conocen la supervisión[770]. En consecuencia, el Comité, en sus observaciones finales sobre Namibia, explicó que el Estado parte debería garantizar que la interceptación de las telecomunicaciones solo se justifique en circunstancias limitadas autorizadas por la ley, con las garantías procesales y judiciales necesarias contra el abuso[771]:

> *"El Comité observa con preocupación que los centros de interceptación parecen estar funcionando ya, a pesar de que la base jurídica en que se sustentan, la parte 6 de la Ley de Comunicaciones (Ley núm. 8 de 2009), aún no ha entrado en vigor. Si bien toma nota de la indicación hecha por la delegación en el sentido de que todas las interceptaciones deben ser autorizadas por un juez y no se retiene información privada, el Comité expresa su preocupación por la falta de claridad sobre el alcance de las posibilidades de interceptación legal, así como sobre las salvaguardias existentes para garantizar que se respete el derecho a la intimidad con arreglo al Pacto (arts. 17 y 21)".*

B. 1. La existencia de una base legal

En primer lugar, cualquier vigilancia, intercepción, acceso, recopilación, retención y difusión de información personal requiere una base legal. Cuando el Comité elaboró el sexto informe de Italia, el Comité observó críticamente que las agencias de inteligencia del estado estaban interceptando comunicaciones personales empleando técnicas de piratería sin autorización legal:

"Preocupan al Comité las denuncias en el sentido de que los organismos de inteligencia interceptan las comunicaciones personales y emplean técnicas de piratería informática

[770] Para una descripción general de las salvaguardas legales necesarias, véase el Doc. CCPR/C/USA/CO/4 (n 26) párrafo 22 de la ONU: "Cualquier interferencia con el derecho a la privacidad o con la correspondencia debe estar autorizada por leyes que sean públicas y accesibles, contienen disposiciones que aseguran que la recopilación, el acceso y el uso de datos de comunicaciones se adaptan a objetivos legítimos específicos, son lo suficientemente precisos y especifican en detalle las circunstancias precisas en las que se puede permitir dicha interferencia, los procedimientos de autorización, las categorías de personas que pueden estar bajo vigilancia, el límite de duración de la vigilancia y los procedimientos para el uso y almacenamiento de los datos recopilados y para salvaguardas efectivas contra el abuso".

[771] CDH - Observaciones finales sobre el segundo informe de Namibia, 22 de abril de 2016, disponible en: http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsh7Ph3KVs8zxwYZKnao5FA8MpfDWy%2FQGPY29QoZxc1OtOmGEp%2BDSlHNgsDjRvjLL6XP1zK0sxDFn1F7An7YwTI5IfSyDejP3nHmcKH%2F9hgLe

sin autorización legal expresa o salvaguardias claramente definidas contra los abusos. También le preocupa que el Decreto-ley de Lucha contra el Terrorismo núm. 21/2016 obligue a los proveedores de servicios de telecomunicaciones a conservar los datos más allá del período autorizado por el artículo 132 del Código de Protección de los Datos Personales, así como que las autoridades puedan acceder a esos datos sin el consentimiento de una autoridad judicial".[772]

La Observación general No. 16 estipula que la legislación que autoriza la interferencia con las comunicaciones privadas "*debe especificar en detalle las circunstancias precisas en las que se pueden permitir tales interferencias*". El Comité ha pedido a varios estados que adopten una ley dedicada a la regulación de las actividades de vigilancia. Dicha legislación debe especificar en detalle el alcance de las posibilidades de intercepción, incluidas las circunstancias en las que se puede autorizar la interferencia. Los objetivos de los servicios de vigilancia no deben ser demasiado amplios. La base legal debe ser precisa y definir claramente el mandato y los poderes de la agencia de inteligencia competente, incluidas las medidas de vigilancia. Se debe evitar el lenguaje vago para evitar interferencias y abusos. En consecuencia, el Comité criticó la ausencia de una definición clara de los términos seguridad nacional y comunicaciones privadas cuando redactó el sexto informe de Nueva Zelanda en 2016:

"Al Comité le preocupa que el derecho a la vida privada no esté contemplado en la Ley de la Carta de Derechos de 1990 y que el marco jurídico vigente establezca un mandato muy amplio de la Oficina Gubernamental para la Seguridad de las Comunicaciones. Le preocupa, además, la ausencia de una definición clara de los conceptos de "seguridad nacional" y "comunicación privada" en la Ley de Telecomunicaciones de 2013. También preocupan al Comité las deficiencias del proceso de autorización judicial para la interceptación de las comunicaciones de los neozelandeses y que no se requiera autorización judicial alguna para interceptar las comunicaciones de los extranjeros (art. 17)"[773].

---

[772] CDH - Observaciones finales sobre el sexto informe periódico de Italia, 1 de mayo de 2017, disponible en:http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhskwLPXK6lx3yNpCdqzah05gNGxS0RGWgUA0TG13aUZvgywezVW6PrWVBLLO%2FsHOjpucgVQxdqvPnwjLiDtho4gBQFMtjCoamJNfhqthEepTn

[773] CDH - Observaciones finales sobre el sexto informe periódico de Nueva Zelandia, CCPR/C/NZL/CO/6, 28 de abril de 2016, disponible en: http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhstky1HJJMM0R%2Bg124Xadhh68naPWV2k8dZAlFF8ilyRoMnuWaZwXPzS4G12gLHCuxiobcVAl5HicL4Dn6n%2Fl2UvlLz%2FoU9CzKStSxq6NUD6u

Además, los poderes deben adaptarse a un objetivo legítimo específico. Consiguientemente, la ley debe contener disposiciones que garanticen que la recopilación, el acceso y el uso de los datos de comunicaciones se adapten a las necesidades específicas de seguridad y se utilicen exclusivamente para este propósito[774].

La base legal también debe especificar la duración de la vigilancia y las instituciones que tienen acceso a los datos de comunicación recompilados. Además, la norma legal debe establecer claramente los motivos (objetivos permitidos) y las pruebas necesarias para obtener la autorización judicial para la vigilancia especificando la naturaleza del delito que puede dar lugar a órdenes de interceptación, las categorías de personas que pueden ser vigiladas o aquellas cuyas comunicaciones es probable que sean interceptadas, y las salvaguardas contra la interferencia arbitraria con el derecho a la privacidad, incluidas las salvaguardas para la información privilegiada. El procedimiento de autorización y los procedimientos para el acceso, uso, comunicación, almacenamiento y destrucción de datos interceptados deben especificarse en ley[775].

Dado que la vigilancia digital y la intercepción se llevan a cabo en secreto sin el conocimiento del individuo, es imperativo que las leyes que autorizan tales medidas sean transparentes para mejorar su legitimidad y permitir que cualquier persona potencialmente afectada conozca el marco legal y las condiciones bajo las cuales las autoridades puedan recurrir a medidas de vigilancia secretas[776]. Esto también es importante para determinar la responsabilidad legal. Por lo tanto, el Comité exige que las normas que regulan el alcance de los poderes de vigilancia y las garantías procesales relativas a su aplicación sean accesibles para el público[777]. También ha pedido a los Estados parte que aumenten el grado de transparencia de las autoridades de vigilancia y de presentar al público todas las medidas concretas de protección de los derechos fundamentales. En este sentido, las autoridades deben hacer públicas las pautas de política de vigilancia y las decisiones de las instituciones involucradas en la inteligencia,

---

[774] CDH - Observaciones finales sobre el séptimo informe periódico del Reino Unido de Gran Bretaña e Irlanda del Norte, CCPR/C/GBR/CO/7, 17 de agosto de 2015, disponible en: https://undocs.org/es/CCPR/C/GBR/CO/7

[775] En este sentido: T.E.D.H., Causa Roman Zakharov v. Russia 47143/06, 04/12/2015, disponible en: http://hudoc.echr.coe.int/eng?i=001-159324.

[776] European Union Agency for Fundamental Rights (2017) *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU*, Volume II: field perspectives and legal update, disponible en: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf

[777] CDH - Observaciones finales sobre el séptimo informe periódico del Reino Unido de Gran Bretaña e Irlanda del Norte, CCPR/C/GBR/CO/7, disponible en: https://undocs.org/es/CCPR/C/GBR/CO/7

buscando el punto de equilibrio entre las consideraciones de seguridad nacional y los intereses de privacidad de las preocupaciones individuales.

La transparencia no solo es relevante con respecto al marco regulatorio sino también con respecto a la práctica judicial. Por consiguiente, el Comité criticó[778]. que la interpretación de la Ley de Vigilancia de Inteligencia Extranjera (FISA) en los Estados Unidos de América y las decisiones del Tribunal de Vigilancia de Inteligencia Extranjera se mantuvieron en gran medida secretas, por lo que no permitía que la persona afectada conociera la ley con suficiente precisión[779]:

B. 2. Garantías de independencia, notificación y reparación

Para verificar la existencia de una sospecha razonable contra una persona y determinar si la medida de vigilancia aplicada es proporcional a los objetivos legítimos perseguidos, cualquier medida de este tipo requiere la autorización de una institución que sea independiente del servicio de inteligencia. El Comité ha indicado una preferencia por la participación judicial en la autorización, pero no ha eliminado la posibilidad de implicar un organismo cuasi judicial independiente que también es políticamente responsable:

> "*El Estado parte debe: […]*
>
> *c) Reformar el actual sistema de supervisión de las actividades de vigilancia para garantizar su eficacia, entre otras cosas disponiendo la intervención judicial en la autorización o supervisión de las medidas de vigilancia, y considerando la posibilidad de establecer mandatos de supervisión consistentes e independientes con el fin de evitar abusos"*[780].

---

[778] CDH, Observaciones finales sobre el cuarto informe periódico de los Estados Unidos de América, 23 abril 2014, disponible en: https://undocs.org/es/CCPR/C/USA/CO/4.

[779] *"Al Comité le preocupa que, hasta hace poco, las interpretaciones judiciales de la Ley de Vigilancia de la Inteligencia Extranjera y las resoluciones del Tribunal de Vigilancia de la Inteligencia Extranjera se hayan mantenido en gran parte en secreto, lo que ha impedido que las personas afectadas conozcan la Ley con suficiente precisión. Al Comité le preocupa que el actual sistema de supervisión de las actividades de la Agencia de Seguridad Nacional no proteja de manera efectiva los derechos de las personas afectadas. Aunque acoge con satisfacción la reciente Directiva de Política del presidente/PPD-28, que hace extensivas algunas garantías a ciudadanos no estadounidenses en la mayor medida posible de acuerdo con la seguridad nacional, el Comité sigue preocupado porque esas personas tengan únicamente una protección limitada contra la vigilancia excesiva. Por último, el Comité está preocupado por que las personas afectadas no tengan acceso a recursos efectivos en casos de abuso (arts. 2, 5 1) y 17)"*

[780] CDH, Observaciones finales sobre el cuarto informe periódico de los Estados Unidos de América, CCPR/C/USA/CO/4, 23 de abril de 2014, disponible en: https://undocs.org/es/CCPR/C/USA/CO/4

Además, para evitar abusos, la aplicación de la ley que permite medidas de vigilancia de la comunicación privada estará sujeta a un control legal ex post[781] general, continuo y apropiado, efectivo e independiente a través de un mecanismo de supervisión externo independiente y consolidado, que sea capaz a enfrentar los poderes y capacidades del servicio de inteligencia[782]. Al igual que la autorización, la supervisión independiente es necesaria para proteger los derechos de las personas afectadas por las medidas de inteligencia y, por lo tanto, funciona como un sustituto y una forma de compensación contra el secreto de las medidas de inteligencia, que impiden que los afectados defienden su privacidad contra tales medidas. Por consiguiente, el Comité solicita un sistema de supervisión robusto e independiente con respecto a la vigilancia, intercepción y piratería[783].

Los Estados deben garantizar que el procesamiento y la recopilación de información estén sujetos a revisión y supervisión por parte de un organismo independiente, bajo garantías necesarias de imparcialidad y eficacia. Por ejemplo, el Comité solicitó a Canadá que establezca mecanismos de supervisión de las agencias de seguridad e inteligencia que sean efectivos y adecuados, y que proporcione a estos mecanismos poderes apropiados y recursos suficientes para llevar a cabo su mandato:

"El Estado parte debe abstenerse de aprobar leyes que impongan restricciones indebidas al ejercicio de los derechos reconocidos por el Pacto. En particular, debe: a) asegurarse de que su legislación de lucha contra el terrorismo prevea salvaguardias legales adecuadas y no socave el ejercicio de los derechos protegidos por el Pacto; b) considerar la posibilidad de revisar el proyecto de ley C-51 para armonizarlo con el Pacto; c) ofrecer salvaguardias adecuadas para garantizar que la transmisión de información en virtud de la Ley de Intercambio de Información para Proteger la Seguridad del Canadá

[781] "El Estado parte debe adoptar las medidas legislativas y de otra índole necesarias para garantizar que toda injerencia en el derecho a la intimidad se ajuste a los principios de legalidad, proporcionalidad y necesidad. También debe garantizar que solamente se intercepten comunicaciones y se utilicen datos para alcanzar objetivos legítimos y precisos, y que se especifiquen detalladamente las circunstancias concretas en que se pueden autorizar esas injerencias y las categorías de personas cuyas comunicaciones puedan ser objeto de vigilancia. Asimismo, debe garantizar la eficacia e independencia del sistema de control de las interceptaciones, en particular disponiendo que el poder judicial intervenga en la autorización y el control de estas"- Observaciones finales sobre el cuarto informe periódico de Rwanda, CCPR/C/RWA/CO/4, 2 de mayo de 2016, texto disponible en: https://undocs.org/es/CCPR/C/RWA/CO/4

[782] CDH, Observaciones finales sobre el segundo informe periódico de Honduras, CCPR/C/HND/CO/2, 22 de agosto de 2017, disponible en: https://undocs.org/en/CCPR/C/HND/CO/2

[783] CDH, Observaciones finales sobre el sexto informe periódico de Italia, 1 de mayo de 2017, CCPR/C/ITA/CO/6, disponible en: https://undocs.org/es/CCPR/C/ITA/CO/6

no dé lugar a violaciones de los derechos humanos; d) establecer mecanismos de supervisión de los organismos de seguridad e inteligencia que sean eficaces y adecuados, y dotarlos de facultades adecuadas y recursos suficientes para el desempeño de su mandato; e) prever la participación del sistema judicial en la autorización de las medidas de vigilancia; y f) establecer un procedimiento claro para que las personas a las que se prohíba viajar en avión sean informadas sin demora y puedan impugnar esa decisión mediante revisión judicial, con la asistencia de un abogado"[784].

Finalmente, el Comité solicita que las personas que son monitoreadas ilegalmente sean informadas sistemáticamente al respecto y, por lo tanto, tengan acceso a recursos legales adecuados para cuestionar la legalidad de la medida de vigilancia. Donde sea posible, la notificación ex post también debe hacerse a todas las demás personas que fueron puestas bajo vigilancia. Tales remedios son una salvaguardia importante contra el uso indebido de medidas de vigilancia secretas. Por esto, si la notificación no pone en peligro el propósito de la medida, se debe proporcionar información sobre la vigilancia a las personas interesadas.

8.4. Retención y uso de datos personales en las actividades de inteligencia

Otro tema muy analizado, aparte de la vigilancia digital, es la permisibilidad de la retención de los datos. Esto no es un problema nuevo. En la Observación general No. 16[785], el Comité explicó que: para tener la protección más efectiva de su vida privada, cada individuo debe tener el derecho de saber con claridad cuál es el propósito y el procedimiento de almacenamiento de sus datos personales, si se almacenan en archivos de datos automáticos, y con qué fines. La protección también se aplica a los datos retenidos por las empresas privadas:

"La recopilación y el registro de información personal en computadoras, bancos de datos y otros dispositivos, tanto por las autoridades públicas como por las particulares o entidades privadas, deben estar reglamentados por la ley. Los Estados deben adoptar medidas eficaces para velar por que la información relativa a la vida privada de una persona no caiga en manos de personas no autorizadas por ley para recibirla, elaborarla

[784] CDH, Observaciones finales sobre el sexto informe periódico del Canadá, CCPR/C/CAN/CO/6, 13 de agosto de 2015, disponible en: https://undocs.org/es/CCPR/C/CAN/CO/6.
[785] Observación General No. 16, Comentarios generales adoptados por el Comité de los Derechos Humanos, Artículo 17 - Derecho a la intimidad, 32º período de sesiones, U.N. Doc. HRI/GEN/1/Rev.7 at 162 (1988).

y emplearla y porque nunca se la utilice para fines incompatibles con el Pacto. Para que la protección de la vida privada sea lo más eficaz posible, toda persona debe tener el derecho de verificar si hay datos personales suyos almacenados en archivos automáticos de datos y, en caso afirmativo, de obtener información inteligible sobre cuáles son esos datos y con qué fin se han almacenado. Asimismo, toda persona debe poder verificar qué autoridades o qué particulares u organismos privados controlan o pueden controlar esos archivos. Si esos archivos contienen datos personales incorrectos o se han compilado o elaborado en contravención de las disposiciones legales, toda persona debe tener derecho a pedir su rectificación o eliminación".

En consecuencia, en los últimos años, el Comité ha pedido a los Estados parte que limiten la retención obligatoria por parte de terceros. En el caso de Sudáfrica criticó el amplio alcance del régimen de retención de datos y pidió al estado adoptar medidas para: *"garantizar que la interceptación de las comunicaciones por las fuerzas del orden y de seguridad se realice únicamente con arreglo a la ley y bajo control judicial. El Estado parte debe aumentar la transparencia de su política de vigilancia y establecer cuanto antes mecanismos de supervisión independientes para evitar abusos y garantizar el acceso a recursos efectivos"*[786].

El acceso a los datos de comunicación retenidos, es decir, datos sobre llamadas telefónicas, correos electrónicos, visitas al sitio web, etc., estará sujeto a garantías estrictas y estándares en acuerdo con los principios de legalidad, necesidad y proporcionalidad. Para determinar si el acceso es necesario y proporcionado, se tendrán en cuenta las categorías de datos retenidos, los medios de comunicación utilizados y las personas interesadas. Las autoridades estatales solo pueden acceder a los datos retenidos solo en la medida estrictamente necesaria para el enjuiciamiento de los delitos más graves o, en situaciones particulares, donde la seguridad pública se ve amenazada por actividades terroristas, donde hay evidencia objetiva de que los datos podrían contribuir efectivamente para combatir tales actividades.

El acceso a los datos retenidos por los proveedores de servicios requiere la autorización de una autoridad judicial[787] y debe estar sujeto a mecanismos de supervisión

[786] CDH, Observaciones finales sobre el informe inicial de Sudáfrica, CCPR/C/ZAF/CO/1, 27 de abril de 2016, disponible en: https://undocs.org/es/CCPR/C/ZAF/CO/1

[787] Por ejemplo, Italia fue criticada por el acceso de las autoridades a los datos retenidos por los proveedores de servicios sin autorización de una autoridad judicial, véase UN Doc CCPR / C / ITA / CO / 6 (n 39) párr. 37.

efectivos e independientes. Es el caso de Australia, se le pidió que introdujera un control judicial sobre el acceso a los metadatos: *"Al tiempo que toma nota de la disponibilidad de mecanismos para la supervisión administrativa en relación con el acceso a los metadatos conservados por los proveedores de telecomunicaciones durante dos años, al Comité le preocupa la falta de autorización judicial para acceder a esos metadatos y de su amplio uso en la seguridad nacional, incluida la lucha contra el terrorismo, y en las investigaciones penales (art. 17). El Estado parte debe reforzar las salvaguardias contra la injerencia arbitraria en la vida privada de las personas con respecto al acceso a los metadatos, mediante la implantación de un control judicial sobre ese acceso"*[788].

Además, debe fijarse un límite aceptable de tiempo para la retención de datos que sea previsto por la ley y garantizar su respeto. En consecuencia, Italia fue criticada por retener datos más allá del período permitido por el estatuto aplicable. Una retención obligatoria de diez años por parte de los proveedores de servicios y el operador de la red se consideró excesiva en el caso de Camerún, y se le pidió al estado parte que se asegurara de que el período de tiempo para conservar los datos se reduzca en la medida necesaria:

"El Comité expresa su preocupación por la Ley núm. 2010/012, de 21 de diciembre de 2010, de la Ciberseguridad y la Ciberdelincuencia, y en particular por su artículo 25, que impone a los operadores de redes y los proveedores de servicios un período de retención de los datos de diez años, contrario a la privacidad de los datos (art. 17)"[789].

Si bien ha existido algunos avances en la promulgación de leyes nacionales que protegen a las personas de la vigilancia doméstica en los últimos años, las salvaguardas nacionales para las cooperaciones internacionales en el ámbito de la inteligencia siguen siendo significativamente más bajas. Por lo tanto, el Comité ha abordado la cuestión de si es necesario respetar el derecho a la privacidad cuando las personas, que se encuentran fuera del territorio de un Estado parte, son sometidas a interceptación o vigilancia. El tema de la aplicación transnacional es particularmente relevante para las redes sociales como Facebook y para los motores de búsqueda como Google porque los datos de

[788] CDH, Observaciones finales sobre el sexto informe periódico de Australia, CCPR/C/AUS/CO/6, disponible en: http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsoAl3%2FFsniSQx2VAmWrPA0uA3KW0KkpmSGOue15UG42EodNm2j%2FnCTyghc1kM8Y%2FLUfoagtkMTN0J7nKKHf5uR8rW8x8clZrKSWnND92qi5r

[789] CDH, Observaciones finales sobre el quinto informe periódico del Camerún, CCPR/C/CMR/CO/5, 30 de noviembre de 2017, disponible en: https://undocs.org/es/CCPR/C/CMR/CO/5.

comunicación generalmente se envían y se reciben desde fuera del país. El Comité extiende la protección para la comunicación transnacional también.

Con respecto al Reino Unido, el Comité criticó el tratamiento diferenciado entre las comunicaciones internas y externas y el régimen distinto de las órdenes la intercepción de las comunicaciones privadas externas y datos de comunicaciones que se envían o reciben fuera del Reino Unido, sin implementar las mismas garantías que se aplican para la comunicación interna[790].

Además, si un Estado parte, extiende su jurisdicción más allá de sus fronteras, las disposiciones legales del Pacto tienen carácter obligatorio y vinculante para el Estado parte. Esto significa que las salvaguardias para la interceptación de comunicaciones externas e internas deben ser idénticas o equivalentes. De conformidad con su enfoque tradicional[791], el Comité ha rechazado los argumentos planteados en contra la aplicación extraterritorial del Pacto en lo que concierne la vigilancia en el extranjero.

El Comité aclaró este tema en sus Observaciones finales sobre el Reino Unido, donde explicó que cualquier interferencia con el derecho a la privacidad debe cumplir con los principios de legalidad, proporcionalidad y necesidad, independientemente de la ubicación o nacionalidad de las personas cuya comunicación está bajo vigilancia directa:

"*El Comité toma nota, entre otras cosas, de las noticias según las cuales las comunicaciones de Amnesty International por correo electrónico fueron interceptadas por el Gobierno en virtud de una orden general. Al Comité le preocupa:*

a) que la Ley de Regulación de las Atribuciones de Investigación de 2000, que establece una distinción entre las comunicaciones internas y externas, permita emitir órdenes no selectivas de interceptación de comunicaciones privadas externas y de los datos de estas que son enviados o recibidos fuera del Reino Unido sin ofrecer las mismas garantías que se aplican a la interceptación de las comunicaciones internas; y

b) la falta de salvaguardias suficientes respecto de la obtención de comunicaciones privadas de organismos de seguridad extranjeros y el intercambio de datos de comunicaciones personales con esos organismos. Al Comité le preocupa además que la

[790] CDH, Observaciones finales sobre el séptimo informe periódico del Reino Unido de Gran Bretaña e Irlanda del Norte, CCPR/C/GBR/CO/7, disponible en: https://undocs.org/es/CCPR/C/GBR/CO/7

[791] CDH - Naturaleza de la obligación jurídica general impuesta a los Estados parte en el Pacto, Observación general No. 31; 26/05/2004, disponible en: http://www.cjslp.gob.mx/seminario/programa/Panel%20IV/PanelIV_Observaci%C3%B3nGeneral31_Comit%C3%A9DH.pdf

Ley de Atribuciones de Investigación y Retención de Datos de 2014 prevea amplias atribuciones de retención de datos de las comunicaciones y que el acceso a esos datos no parezca estar limitado a los delitos más graves (arts. 2, 17, 19 y 26)"[792].

El Comité adoptó el mismo enfoque cuando consideró los informes de Francia, Nueva Zelanda y los Estados Unidos.

En sus observaciones finales sobre los Estados Unidos[793], el Comité solicitó al gobierno garantizar que las actividades de vigilancia, tanto dentro como fuera del territorio de los Estados Unidos, cumplan con sus obligaciones impuestas por el Pacto, incluido el Artículo 17, independientemente de la nacionalidad o ubicación de las personas cuyas comunicaciones son bajo vigilancia directa. También, en sus observaciones finales sobre Nueva Zelanda[794], el Comité solicitó garantías judiciales suficientes para todas las personas afectadas en términos de interceptación de la comunicación y la recopilación, procesamiento e intercambio de metadatos, sin importar el territorio donde se encuentran.

Estas observaciones se basan en el entendimiento de que los Estados parte ejercen su jurisdicción de conformidad con el Artículo 2 (1) del Pacto siempre que ejerzan autoridad sobre la comunicación de una persona. En tales circunstancias, la jurisdicción se basa en el control virtual sobre los datos o la persona que los generó. En otras palabras, el significado del término jurisdicción depende del derecho afectado. Si bien, en virtud del artículo 9, el derecho a la libertad implica el control físico sobre un individuo, cuando se trata de la protección de la privacidad y la comunicación, el control físico no es importante. Es más bien la autoridad fáctica que se ejerce sobre la comunicación u otros datos lo que es decisivo.

Estrechamente relacionado con el tema de la vigilancia extraterritorial está el tema del intercambio de inteligencia digital con gobiernos extranjeros. Las garantías del artículo 17 se aplican también a tales formas de cooperación. Por esto, Pakistán fue criticado en julio de 2017 al compartir información y cooperar con gobiernos extranjeros

[792] CDH - Observaciones finales sobre el séptimo informe periódico del Reino Unido de Gran Bretaña e Irlanda del Norte, CCPR/C/GBR/CO/7, 17 de agosto de 2015, disponible en: https://undocs.org/es/CCPR/C/GBR/CO/7

[793] CDH, Observaciones finales sobre el cuarto informe periódico de los Estados Unidos de América, CCPR/C/USA/CO/4, 23 de abril de 2014, disponible en: https://undocs.org/es/CCPR/C/USA/CO/4

[794] CDH, Observaciones finales sobre el sexto informe periódico de Nueva Zelandia, CCPR/C/NZL/CO/6, 28 de abril de 2016, disponible en: https://undocs.org/es/CCPR/C/NZL/CO/6.

sin autorización ni supervisión judicial. Con respecto al Reino Unido, el Comité destacó la falta de garantías suficientes con respecto a la obtención de comunicaciones privadas de agencias de seguridad extranjeras y el intercambio de datos de comunicaciones con dichas agencias. En este sentido se recomendó que:

"El Estado parte debe revisar su legislación en materia de reunión de datos y vigilancia, en particular la Ley de Prevención de Delitos Electrónicos de 2016, para que se ajuste a sus obligaciones dimanantes del Pacto. También debe establecer mecanismos independientes de supervisión de la aplicación de la Ley, que incluyan el examen judicial de las actividades de vigilancia; revisar sus leyes y prácticas en materia de intercambio de información de los servicios de inteligencia con organismos extranjeros a fin de asegurar su conformidad con el Pacto"[795].

Preocupaciones similares se expresaron en el diálogo con Suecia. Por lo tanto, el Comité solicitó mecanismos de supervisión eficaces e independientes sobre el intercambio de inteligencia que implica manipulación y transferencia de datos personales.

Cuando hace unos años comenzaron los debates sobre cómo lidiar con la vigilancia digital y la cooperación de inteligencia internacional, proponiéndose varias soluciones, incluso la elaboración rápida de un nuevo instrumento legal[796]. Sin embargo, el análisis anterior de la interpretación del Comité de Derechos Humanos del artículo 17 del Pacto demuestra que este no es un punto ciego del derecho internacional, sino un área sujeta a estándares legales específicos[797]. Cualquier interferencia con este derecho debe estar en acuerdo perfeto con los principios de legalidad, necesidad y proporcionalidad. La vigilancia masiva no puede conciliarse con el derecho a la vida privada en ausencia de las garantías necesarias requeridas por estos principios. Los mecanismos de garantías juegan un papel central para equilibrar los intereses de seguridad con la protección de los derechos individuales.

Así pues, el principal desafío no es el desarrollo de nuevas reglas internacionales sino la aplicación e implementación de la ley existente. Lo más importante es el desarrollo de garantías legales nacionales que incluyan mecanismos efectivos de supervisión. El

[795] CDH, Observaciones finales sobre el informe inicial del Pakistán, CCPR/C/PAK/CO/1, 23 de agosto de 2017, disponible en: https://undocs.org/es/CCPR/C/PAK/CO/1
[796] Deeks, A. (2014) *An International Legal Framework for Surveillance*, Virginia Journal of International Law, vol. 55:2, pp. 292-367.
[797] Maurer, T. (2011) *Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security*, Belfer Center for Science and International Affairs Harvard Kennedy School;

Comité ha aclarado en varias recomendaciones que los Estados parte deben reconocer y regular al nivel nacional los desafíos derivados de las formas modernas de vigilancia digital. En este contexto, ha identificado una regulación insuficiente y no transparente de las actividades de vigilancia y la falta de responsabilidad de los servicios de inteligencia como obstáculos importantes para la protección efectiva del derecho a la privacidad.

Algunos estados se han basado en leyes obsoletas que fueron diseñadas para regular formas de vigilancia más rudimentarias para justificar la vigilancia masiva. Pero tales leyes no son adecuadas para hacer frente a la profunda intrusión en el ámbito privado que las nuevas tecnologías hacen posible:

"Cuando se utilizan programas de acceso masivo, no hay límites a las categorías de personas que pueden ser vigiladas ni a la duración de la vigilancia. Estas condiciones, por lo tanto, no pueden enunciarse detalladamente en la legislación. Los marcos jurídicos y administrativos detallados de la vigilancia a gran escala suelen ser confidenciales, y poco se sabe aun públicamente sobre el uso que se da a los datos recabados. Hasta ahora, en muy pocos Estados existe normativa del poder legislativo que autorice expresamente esos programas"[798].

Si bien recientemente se han logrado algunos avances a nivel nacional con respecto a la vigilancia nacional, las garantías existentes y los remedios disponibles siguen siendo insuficientes y el intercambio de inteligencia y la cooperación siguen sin tener una regulación suficiente. Con respecto a la vigilancia transnacional, se observa la necesidad de una regulación más concreta para el intercambio de inteligencia y la cooperación. Se pide a los Estados parte que promulguen una base legal que regule las condiciones para el intercambio de inteligencia, incluidas las normas de diligencia[799], que deben cumplirse para que la información se comparta respetando los derechos fundamentales. Además, la autorización y las garantías necesarias para todos los intercambios de inteligencia deben regularse a nivel nacional.

Los futuros análisis del Comité de Derechos Humanos deberán abordar con más detalle la distinción entre vigilancia específica, vigilancia general y las normas

[798] El informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Sr. Ben Emmerson, presentado de conformidad con la resolución 68/178 de la Asamblea General y la resolución 15/15 del Consejo de Derechos Humanos, diponible en: https://undocs.org/es/A/69/397.
[799] Kulesza, J. (2014) *Protecting Human Rights Online - An Obligation of Due Diligence*, Jean Monnet Working Paper 24/14.

respectivas. Muchos Estados parte parecen apartarse del supuesto de que la vigilancia especifica requiere un estándar de protección más alto que la vigilancia general, lo que supuestamente es menos invasivo. Es cierto que las consecuencias de la vigilancia selectiva para el enjuiciamiento penal son de mayor alcance para los sospechosos. Por otro lado, las garantías existentes estipulan que la vigilancia especifica requiere la existencia de una sospecha razonable de conducta ilegal y que tales medidas deben estar dirigidas y adaptadas a la recolección de evidencia relevante.

En lo que concierne la vigilancia general, las normas nacionales suelen ser menos exigentes. Sin embargo, no es importante si una persona está sujeta a vigilancia específica o si está sujeta a vigilancia general, su derecho a la privacidad será afectado en la misma medida. Por ejemplo, construir perfiles personales completos desde los datos compilados en un procedimiento de vigilancia masiva conduce a una grave intrusión en la privacidad de los afectados. Además, no debe subestimarse el efecto escalofriante de la vigilancia general. Es probable que la aprensión constante de la vigilancia tenga un efecto perjudicial en el ejercicio de los derechos y libertades en general. Por lo tanto, existen buenas razones para que el Comité especifique aún más las garantías del artículo 17 con respecto a la vigilancia general en el futuro y considere si y bajo qué circunstancias puede conciliarse con el principio de proporcionalidad[800].

Si bien el Comité ha enfatizado la protección procesal hasta el momento, en el futuro tendrá que tratar con más detalle las cuestiones sustantivas. Esto requerirá ante todo una consideración general del significado de la protección de la privacidad en la era digital. Al reconocer que el artículo 17 del Pacto se aplica también a la información compartida en áreas públicas, se ha reconocido también que la protección de la privacidad no se limita a proteger la intimidad, sino que se extiende a todos los aspectos del autodesarrollo y la personalidad del individuo. Este desarrollo personal se alimenta de la interacción social y la capacidad de comunicarse con los demás. No se limita a la comunicación, sino que también se extiende a otros aspectos del autodesarrollo, la autonomía individual y la personalidad[801]. Por lo tanto, el acceso no discriminatorio al ciberespacio, la protección contra la interferencia ilegal y el derecho a ejercer control

[800] James, J. (2006) *Digital Divide Complacency: Misconceptions and Dangers*, The Information Society International Journal, Vol. 24, pp. 54-61

[801] Milanovic, M. (2015) *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*. Harvard International Law Journal 56 (1). Recuperado de: http://www.harvardilj.org/wp-content/uploads/561Milanovic.pdf

sobre la información y los datos propios, incluido el derecho al olvido, son, posiblemente, una condición previa necesaria para el libre desarrollo de la personalidad.

Frente a los desafíos cada vez mayores para la protección de la vida privada y de las comunicaciones en la era digital, la interpretación del Comité también debería abordar otras innovaciones tecnológicas, como nuevas formas de vigilancia tipo IMSI-Catchers (utilizado para recibir tráfico de teléfonos móviles y para rastrear los datos de ubicación de los usuarios de teléfonos móviles), compilación de datos, malware y manipulación de datos, vulnerabilidades de almacenamiento, el uso de tecnología de reconocimiento biométrico para identificación y monitoreo de lugares públicos y las amenazas derivadas de las nuevas tecnologías[802]. También tendrá que lidiar con nuevos modos de interferencia.

Algunos estados, en un esfuerzo por obtener una supervisión completa sobre el ser humano, han comenzado a presionar para que se entreguen datos personales completos de las personas a cambio de beneficios económicos y de otro tipo, lo que les permite construir perfiles personales completos y ejercer la supervisión sobre bases supuestamente voluntarias. Esta práctica requiere una nueva reflexión sobre el concepto de interferencia con los derechos individuales y la noción de voluntariado[803].

Además, el Comité deberá analizar más atentamente las amenazas que surgen para la protección de la privacidad como consecuencias de las acciones de los actores no estatales. Teniendo en cuenta los crecientes riesgos causados por las empresas privadas, el Comité debe considerar con mayor profundidad las obligaciones de los Estados parte de proteger a las personas contra tales amenazas. En este sentido, en el sexto informe de Italia, el Comité, criticó que las empresas privadas vendieran equipos de vigilancia a los gobiernos con antecedentes de violaciones graves de los derechos humanos y se quejó de la ausencia de garantías legales o mecanismos de supervisión con respecto al exportación de equipos de vigilancia:

"Además, preocupan al Comité las denuncias de que algunas empresas con sede en un Estado parte han exportado equipo de vigilancia en línea a Gobiernos con antecedentes de graves violaciones de los derechos humanos, así como el hecho de que no haya

[802] Kris, D. (2013) *Thoughts on a Blue-Sky Overhaul of Surveillance Laws: Approach.* Lawfare. Recuperado de: https://www.lawfareblog.com/thoughts-blue-sky-overhaul-surveillance-laws-approach
[803] Milanovic, M. (2015) idem.

salvaguardias jurídicas ni mecanismos de supervisión en relación con la exportación de ese tipo de equipo (art. 17)"[804].

El Estado parte debe tomar medidas para garantizar que todas las empresas bajo su jurisdicción, como las corporaciones tecnológicas, respetan los derechos humanos cuando participan en operaciones en el extranjero. La observación final le recuerda a los Estados parte, que tienen funciones reguladoras frente a los actores privados y reafirma la aplicación transnacional del Pacto incluso en los casos en que las empresas actúan en el extranjero. De manera que, queda claro que los Estados parte deben tomar todas las medidas positivas de protección contra las amenazas a los derechos fundamentales que se originan en sus jurisdicciones.

En conclusión, es justo decir que, aunque el Comité no ha podido abordar todos los problemas relacionados con la vigilancia digital, nuestro análisis demuestra que su interpretación ha avanzado significativamente en los últimos años en un esfuerzo por mantenerse al día con los nuevos desafíos en lo que concierne el derecho a la vida privada. El Comité ha sentado importantes bases en el contexto del procedimiento de presentación de informes. En cualquier caso, en lo que concierne el derecho a la vida privada, ya se ha logrado aclarar las exigencias necesarias para su protección en el entorno digital, al especificar las normas legales aplicables a la cooperación, a los metadatos y a la cooperación en el ámbito de la inteligencia extranjera. El Comité ha realizado y continuará haciendo una contribución importante para el desarrollo del derecho internacional y su correlación con los nuevos desafíos resultados de la revolución tecnológica.

[804] CDH, Observaciones finales sobre el sexto informe periódico de Italia, CCPR/C/ITA/CO/6, 1 de mayo de 2017, disponible en: https://undocs.org/es/CCPR/C/ITA/CO/6

CONCLUSIONES

Nuestras vidas se han trasladado poco a poco en la red global donde los dispositivos interconectados que operan en el protocolo TCP/IP o los compatibles con el mismo pueden comunicar sin límites, creando lo que llamamos el Internet. El término "ciberespacio" que se originó en la literatura de ciencia ficción se ha materializado en una plataforma de interacción humano-computadora habilitada por los dispositivos interconectados TCP/IP. Con más del 60% de la población mundial utilizando Internet en nuestros días, la cuestión de los derechos y obligaciones individuales es cada vez más importante. Después de que casi 70 años de desarrollo de normas y principios en el ámbito de los derechos humanos podemos pensar que esta transición de la vida comunitaria del entorno offline a un entorno en línea puede ser una tarea muy fácil, pero en realidad no es un asunto tan sencillo. Las preguntas prácticas sobre los límites de la vigilancia estatal y el respeto de la vida privada o sobre la aplicabilidad de las diferentes leyes nacionales en los casos de difamación en línea han demostrado que se necesitan criterios universales y garantías para la protección efectiva de los derechos humanos, en lugar de un compromiso político ampliamente definido que domina el debate sobre los derechos humanos en el ciberespacio.

Pese a, que los derechos humanos no son el único dominio de las relaciones y el derecho internacionales significativamente alterado por las características del ciberespacio. Internet cambió algo más que la percepción de los derechos humanos. Con su naturaleza descentralizada y su gobernanza polivalente, también alteró el papel de los estados en lo que respecta a la protección de los derechos humanos. Mientras que dentro de sus territorios "físicos" los estados actúan a través de instituciones y órganos para la aplicación de la ley, en línea necesitan la ayuda de los proveedores de servicios de Internet (ISP), empresas o personas que alojan sitios web o prestan servicios, incluidos los que consisten en permitir el acceso a Internet, para poder ejecutar sus poderes y hacer cumplir sus leyes.

Con el carácter transnacional de la red y los ISP ubicados en varias jurisdicciones, que ofrecen sus servicios en todo el mundo, los estados encuentran cada vez más difícil ejecutar efectivamente sus leyes dentro de sus territorios nacionales cuando se trata de infracciones en línea o violaciones de la ley. Sin la ayuda de los organismos privados extranjeros, un Estado no puede hacer efectiva una sentencia de

eliminación de un contenido difamatorio, por ejemplo, aunque tal comportamiento está sancionado por sus leyes nacionales. Sin una cooperación internacional reforzada, es imposible configurar el alcance de los derechos humanos en línea, ya sea la libertad de expresión, la no discriminación o la privacidad. Sin embargo, una mayor cooperación internacional con respecto al entorno en línea se refiere no solo a los Estados parte. Los proveedores de internet juegan un papel crucial en la protección o limitación de los derechos humanos en línea, lo que se suma al debate sobre las obligaciones de derechos humanos de las corporaciones globales.

En este sentido, El Consejo de Derechos Humanos de las Naciones Unidas adoptaron, en su resolución 17/4, de 16 de junio de 2011, los *"Principios Rectores sobre las empresas y los derechos humanos: puesta en práctica del marco de las Naciones Unidas para proteger, respetar y remediar"*, que fueron elaborados por el Representante Especial del Secretario General para la cuestión de los derechos humanos y las empresas transnacionales y otras empresas. Según el documento, los principios rectores se aplican a todos los Estados y a todas las empresas, tanto transnacionales como de otro tipo, con independencia de su tamaño, sector, ubicación, propietarios y estructura, basándose en el reconocimiento de:

"*a) Las actuales obligaciones de los Estados de respetar, proteger y cumplir los derechos humanos y las libertades fundamentales;*

b) El papel de las empresas como órganos especializados de la sociedad que desempeñan funciones especializadas y que deben cumplir todas las leyes aplicables y respetar los derechos humanos;

c) La necesidad de que los derechos y obligaciones vayan acompañados de recursos adecuados y efectivos en caso de incumplimiento"[805].

La necesidad de encontrar una fórmula para de gestionar de forma unitaria el recurso digital global que es el ciberespacio ha llamado la atención de la comunidad internacional, pero el término "gobernanza de Internet" ha aparecido después del año 2003. De acuerdo con la Agenda de Túnez, la "gobernanza de Internet" [806] representa "*el desarrollo y aplicación por los gobiernos, el sector privado y la sociedad civil, en el*

[805] Naciones Unidas (2011) *Principios rectores sobre las empresas y los derechos humanos. Puesta en práctica del marco de las Naciones Unidas para "proteger, respetar y remediar"*, HR/PUB/11/04, Nueva York: Naciones Unidas

[806] Cumbre Mondial sobre la Sociedad de la Informacion (2006) *Agenda de Túnez para la Sociedad de la Información*, WSIS-05/TUNIS/DOC/6(Rev.1)-S, recuperado de: https://www.itu.int/net/wsis/docs2/tunis/off/6rev1-es.html.

desempeño de sus respectivos papeles, de principios, normas, reglas, procedimientos de toma de decisiones y programas comunes que dan forma a la evolución y a la utilización de Internet".

Esta definición concisa es un buen reflejo de las características específicas de la arquitectura de Internet, que se percibe como una estructura en capas. En general, se puede considerar que Internet se compone de al menos tres capas concéntricas: la capa física más central de hardware y cables de telecomunicaciones, la capa intermedia de código, incluido el software y que permite que el hardware participe en la comunicación y la capa de contenido exterior, donde la información y los servicios se proporcionan y comparten con el uso del hardware y software.

Cada una de las capas está gobernada por diferentes grupos de entidades. Si bien los elementos de la capa física pertenecen a empresas, generalmente operadores de telecomunicaciones de propiedad privada, la capa de software (o la capa de código) es desarrollada por individuos, generalmente informáticos, dentro de unos pocos foros informales autónomos, como Internet Engineering Task Force (IETF) o el World Wide Web Consortium (W3C). Los detalles de tales organismos de establecimiento de estándares y, en consecuencia, la organización de esta capa de código intermedia es una consecuencia directa de la génesis de la red: lo que una vez fue un ejercicio estrictamente académico sigue estando fuertemente influenciado por los estudiosos de la informática, que buscan formas más efectivas de transmitir paquetes de datos, menos consciente de las políticas nacionales o internacionales y las luchas de poder. Por lo tanto, el establecimiento de normas técnicas queda fuera del alcance de los estados o empresas por igual, como un asunto ajeno a las políticas.

El papel de las autoridades estatales es más fuerte en solo una de las tres capas complementarias: la capa de contenido. Los estados desean que el contenido disponible dentro de sus territorios obedezca a las leyes locales y tratan de influir en el alcance de la información disponible en línea mediante la ejecución y aplicación de las leyes nacionales. A pesar de que, a menudo fallan, debido al hecho de que todas las capas están fuertemente interconectadas: es imposible administrar de manera efectiva una de ellas sin interaccionar con las otras. Es imposible gobernar el contenido solo, ya que se ejecuta en código, creado por individuos en foros no gubernamentales y se transmite a través de redes de propiedad privada o cables submarinos.

Por mucho que los estados tuvieran la autoridad y la capacidad física para confiscar una edición impresa completa de un periódico que contiene una declaración

difamatoria, a menudo no pueden detener físicamente una publicación en línea, a pesar de que está disponible en sus territorios. Como se presentó en los primeros tres capítulos de esta tesis, esta especificidad transnacional única del ciberespacio requiere una cooperación efectiva de todas las partes interesadas, una característica de la gobernanza de Internet a la que se hace referencia como principio multisectorial y está redactada en la Agenda de Túnez citada anteriormente, refiriéndose a tres grupos de partes interesadas: el sector privado que ejecuta el hardware , sociedad civil, incluida la academia, diseñando el código y los estados, aplicando sus leyes sobre el contenido en línea y sus autores o usuarios.

La necesidad de cooperación de las diversas partes interesadas es particularmente visible cuando se trata de proteger los derechos humanos en el entorno digital. Con la necesidad de identificar las obligaciones individuales de los estados hacia todos los actores de Internet, tanto usuarios como proveedores de servicios digitales, parece que ha llegado el momento de introducir en el ciberespacio las obligaciones legales, derivadas del derecho internacional de derechos humanos desarrollado hasta ahora. Si bien existe una sólida experiencia en el derecho internacional de los contratos y la jurisprudencia, todos los principios de derechos humanos deben aplicarse "*de manera adecuada*" para reflejar las características específicas de este único medio que deben gobernar.

Teniendo esto en cuenta, se pueden identificar los principios básicos de lo que podría llamarse una ley internacional de Internet. Estos principios deben adaptarse al carácter multisectorial de la gobernanza de Internet, de manera especificada en la Agenda de Túnez de 2005, fomentando la cooperación entre todos los gestores de las áreas que interactúan en Internet, quitando el poder absoluto a los estados y dividiéndolo entre los tres grupos de partes interesadas para crear y mantener el equilibrio del ciberespacio. Los principios del derecho internacional aplicados al Internet[807] deben incluir, además del multi-sectorialismo, la diversidad cultural, la libertad de acceso, la apertura y la seguridad de la red.

Con los esfuerzos de legislar en el ámbito de la ciberseguridad depositados por las instituciones y agencias europeas, con las declaraciones de los representantes de las Naciones Unidas, podemos decir que ya se ha iniciado el camino hacia un único documento de derecho internacional, que inicialmente contiene principios de gobernanza

[807] Kulesza J. (2012*) International Internet law*, Revista: Global Change, Peace & Security 24(3), pp. 351 – 364

de Internet de tipo soft law, y que finalmente sigue el camino del derecho ambiental internacional, un dominio bien establecido del derecho público internacional.

La aplicabilidad legal de estos principios resulta fácilmente de la obligación impuesto por el derecho internacional a los Estados de tomar todas las medidas posibles para prevenir cualquier violación de los derechos humanos dentro de su jurisdicción, poder o control, donde el estándar internacional de diligencia debida servirá como una medida para identificar el alcance de los esfuerzos requeridos de cada Estado Parte individual.

En lo que concierne el desarrollo de las obligaciones de las empresas transnacionales en materia de respeto y protección de derechos humanos, así como se describe en los Principios Rectores sobre las empresas y los derechos humanos (mencionados más arriba), pensamos que es necesaria a elaboración de un código de conducta para las empresas internacionales, cuya aplicación debería dejarse en manos de las organizaciones internacionales, como la Organización Mundial del Comercio o la Unión Internacional de Telecomunicaciones[808], en sus foros de arbitraje interno.

Como lo hace notar el análisis presentado en el Capítulo II de la tesis, de acuerdo con los tratados de derechos humanos vigentes, los Estados tienen una obligación tanto negativa como positiva de luchar por la protección efectiva de los derechos humanos individuales para quienes se encuentran dentro de su jurisdicción. Al igual que con cualquier obligación internacional de conducta, la evaluación de las acciones y omisiones estatales se basará en un estándar de diligencia debida (due-diligence). La diligencia debida requiere que los Estados adopten "todas las medidas razonables"[809] para cumplir con sus obligaciones internacionales, mientras que no hacerlo puede resultar en su responsabilidad internacional.

De acuerdo con los extensos estudios de la Comisión de Derecho Internacional (CDI), resumidos en dos documentos clave: el Proyecto de artículos sobre la

[808] La Unión Internacional de Telecomunicaciones es un organismo especializado de las Naciones Unidas para las tecnologías de la información y la comunicación. Fundada en 1865 para facilitar la conectividad internacional de las redes de comunicaciones, atribuye en el plano mundial el espectro de frecuencias radioeléctricas y las órbitas de satélite, elabora las normas técnicas que garantizan la interconexión armoniosa de redes y tecnologías, y lucha para mejorar el acceso a las TIC para las comunidades insuficientemente atendidas del mundo entero. La Unión está comprometida para conectar a toda la población mundial – dondequiera que viva y cualesquiera que sean sus medios, apoyando el derecho de cada persona a comunicarse con los demás individuos. De conformidad con su mandato y los documentos finales de la Cumbre Mundial sobre la Sociedad de la Información (CMSI), la Unión sigue desempeñando un papel fundamental en la aplicación y el seguimiento de la CMSI.

[809] Pisillo-Mazzeschi, R. (1992) *The "Due Diligence" Rule and the Nature of the International Responsibility of States*, 35 German Yearbook of International Law 9 (1992), pp. 9 – 49

responsabilidad del Estado por hechos internacionalmente ilícitos[810] y el Proyecto de Principios sobre la asignación de la pérdida en caso de daño transfronterizo resultante de actividades peligrosas[811], respectivamente, un principio de diligencia debida acompaña a cualquier obligación de conducta y consta de nueve elementos.

La debida diligencia requiere que los Estados actúen de buena fe al cumplir con sus obligaciones internacionales, incluidas las obligaciones preventivas. En segundo lugar, está estrechamente relacionado con el principio de buena vecindad, que exige a los Estados que se abstengan de causar daños o perjuicios dentro del territorio o en interés de otros Estados, así como en territorios comunes. La evaluación de la diligencia debida debe realizarse con respecto al territorio estatal y son las acciones potencialmente dañinas iniciadas dentro del territorio estatal las que deben evitarse. En cuarto lugar, la obligación de diligencia debida es un derivado del principio de desarrollo sostenible, ya que la diligencia también debe acompañar a la evaluación del riesgo de introducir cualquier nuevo procedimiento o legislación.

El quinto elemento del principio de diligencia debida es la obligación del Estado de adoptar "todas las medidas necesarias" que se esperan de un "buen gobierno" para cumplir el objetivo de una obligación, mientras que el contenido particular de dicha obligación es siempre específico para cada caso. Esas medidas particulares dependerán en gran medida del estado de la técnica en un área determinada frente a las capacidades económicas y tecnológicas de un estado. En consecuencia, el séptimo elemento de la debida diligencia es la obligación de intercambiar información con las contrapartes sobre los riesgos evaluados y las medidas tomadas para prevenir el incumplimiento de las obligaciones internacionales.

De acuerdo con el trabajo de la CDI, los estados también están obligados a abstenerse de discriminar a las víctimas de una determinada infracción o sus autores. Finalmente, el estándar de diligencia debida es de naturaleza continua, lo que obliga a los Estados a mantener sus esfuerzos para identificar y prevenir el incumplimiento de sus obligaciones internacionales.

---

[810] Naciones Unidas (2002) *Resolución aprobada por la Asamblea General [sobre la base del informe de la Sexta Comisión (A/56/589 y Corr.1)]*, A/RES/56/83, Responsabilidad del Estado por hechos internacionalmente ilícitos, recuperado de: https://undocs.org/es/A/RES/56/83

[811] Naciones Unidas (2006) *Resolución aprobada por la Asamblea General el 4 de diciembre de 2006 [sobre la base del informe de la Sexta Comisión (A/61/454)],* A/RES/61/36, Asignación de la pérdida en caso de daño transfronterizo resultante de actividades peligrosas,
recuperado de: https://undocs.org/pdf?symbol=es/A/RES/61/36

En este contexto, puede evaluarse que los Estados tienen la obligación de actuar con la diligencia debida para prevenir violaciones de los derechos humanos individuales. Para cumplir con esa obligación, deben participar en la cooperación internacional y buscar activamente la adopción de "todas las medidas necesarias" para prevenir violaciones de los derechos humanos dentro de su jurisdicción, poder o control. Esto no significa que estén obligados a prevenir con éxito cualquier incumplimiento o tener conocimiento de cualquier intento de tal incumplimiento. Deben desplegar las acciones que se esperan de un buen gobierno en una situación determinada.

La protección de los derechos humanos en línea es, por lo tanto, un concepto de dos caras, que incluye, por un lado, la obligación de abstenerse de interferir con un derecho humano individual, pero al mismo tiempo, de tomar con la debida diligencia todas las medidas necesarias para prevenir cualquier violación de este tipo afectada por tercero dentro de la jurisdicción estatal.

Como ocurre con cualquier obligación internacional, la falta de diligencia debida por parte de las autoridades estatales en la adopción activa de medidas para prevenir violaciones de la vida privada, de la libertad de expresión o de cualquier otro derecho individual puede resultar en responsabilidad del Estado de acuerdo con las normas identificadas en el derecho internacional cuando no existen circunstancias legales excluyentes, como estado de necesidad o la fuerza mayor[812].

Como hemos visto en el capítulo IV de la presente tesis, el concepto de los derechos humanos ha ido madurando junto con la comunidad internacional. Después de sanar la mentalidad colectiva de muchos prejuicios, los grandes pensadores, filósofos y activistas del siglo XX consiguieron, a través de un intenso trabajo, el reconocimiento de una larga paleta de derechos humanos, entre cuales la dignidad humana, la privacidad, la libertad de pensamiento y opinión juegan un papel determinante para la nueva arquitectura social del siglo XXI.

La conceptualización, definición y regulación universal de los derechos humanos no ha sido un trabajo fácil y tampoco lo podemos declarar finalizado. La lucha contra los prejuicios continua y la garantías del respecto de estos derechos siguen siendo insuficientes para la cantidad de amenazas identificadas cada día. El proceso de desarrollo de los derechos humanos está muy lejos de su punto final. A medida que se desarrollan y evolucionan, los derechos humanos reflejan en su alcance valores nuevos,

[812] Dupuy, P.-M. (1989) *The International Law of State Responsibility: Revolution or Evolution?*, Michigan Journal of International Law Vol.11./Issue 1, pp. 105-128.

directamente conexas con las transformaciones sociales actuales, como los derechos ambientales o sexuales.

La revolución y la evolución de los derechos humanos fueron aceptadas por primera vez por la comunidad internacional de los Estados que eligieron firmar la Declaración Universal de Derechos Humanos de 1948. Con este documento se abrió la nueva época de los derechos fundamentales, que fueron poco a poco incluidos en los tratados internacionales, en las constituciones y en las leyes de cada estado miembro. El compromiso universal de proteger y garantizar los derechos fundamentales se convierte en una política articulada al nivel global.

La elaboración y adopción de los siguientes tratados internacionales, como el Pacto Internacional de Derechos Civiles y Políticos (1966) y el Pacto Internacional de Derechos Económicos, Sociales y Culturales (1966), abren la nueva reflexión sobre los derechos humanos, creando diferente clases y categorías, incluso generaciones de derechos. Los derechos económicos, sociales y culturales enumerados en estos pactos se consideran positivos, intensivos en recursos, progresistas, vagos, políticos (ideológicamente divisivos), socialistas y no justiciables, lo que los convierte en aspiraciones u objetivos, luego en requisitos legales reales.

Al mismo tiempo, los derechos civiles y políticos enumerados en el Pacto Internacional de Derechos Civiles y Políticos se consideran derechos de carácter negativo: esto significa que requieren que un estado permita ciertas libertades individuales en lugar de proporcionar recursos o servicios reales, sin costo, inmediatos, precisos, no ideológicos (no políticos), justiciables y por tanto considerados derechos reales "legales"[813]. Por tanto, la ideología de los derechos humanos condiciona el cumplimiento del segundo grupo de derechos, los llamados derechos a la subsistencia, como resultantes de los derechos identificados como pertenecientes a la primera generación.

Los desarrollos recientes en el derecho internacional invitaron a la idea de una tercera categoría de derechos humanos, que incluye, por ejemplo, derechos ambientales, como el derecho a un medio ambiente sano o adecuado o los derechos sexuales. Estos últimos incluyen los derechos de lesbianas, gays, bisexuales y transexuales (LGBT) identificados en los Principios de Yogyakarta de 2007, seguidos por la Declaración de la Asamblea General de la ONU de 2008 sobre orientación sexual e identidad de género.

[813] Scott, C. (1989) *Interdependence and Permeability of Human Rights Norms: Towards a Partial Fusion of the International Covenants on Human Rights*, Revista: Osgoode Hall Law Journal 27.3, pp. 769-878.

La Declaración recibió el apoyo de 67 estados miembros y la oposición de 57, lo que muestra claramente la disparidad en la comprensión del concepto moderno de derechos humanos. También dentro de esa categoría se pueden nombrar los derechos reproductivos, incluido el derecho al aborto frente al clásico derecho a la vida. De toda forma, el debate filosófico sobre el momento de la existencia efectiva del derecho a la vida sigue en primera fila, aumentando las páginas de doctrina, sin poder concluir si este coincide con el momento de nacer, o de obtener la capacidad de mantener físicamente la función vital o al momento de la concepción. La falta de un acuerdo común sobre el tema influye en políticas nacionales y alimenta un gran debate emocional sobre valores y moralidad.

El tercer grupo de derechos fundamentales puede derivarse de otros derechos humanos, por ejemplo: el derecho a la vida, el derecho a la salud o el derecho a la vida privada y familiar. Esta categoría incluye también el derecho a la comunicación, derivado del bien establecido derecho a la libertad de expresión. Lo que podría denominarse un nuevo cuarto grupo o generación de derechos humanos podría incluir aquellos derechos que son derivados de uno o más derechos de los grupos ya desarrollados. El derecho al acceso a Internet entra en esta categoría, a lo mejor junto al recientemente discutido derecho al olvido o al propuesto derecho a la personalidad virtual.

Consecuente del derecho a la libre expresión, o más directamente derivado del derecho a recibir y difundir información, como elemental para la libertad de expresión, se fundamenta en el convencimiento de que Internet se ha convertido en una de las herramientas más importantes para la interacción humana, y como tal, la principal fuente de información y conocimiento. Limitar o negar el acceso a la red equivale a limitar o negar el acceso a la información y limitar la capacidad de compartir las opiniones de uno libremente. El derecho al acceso a Internet puede percibirse como un elemento de la necesidad de proteger la integridad sustancial de los derechos humanos.

En el año 2009, el Consejo Constitucional francés se enfrentó a la cuestión del acceso a Internet como derecho humano en un asunto relativo a la protección del derecho de autor previsto por la legislación francesa. La Ley n ° 2009-669 del 12 de junio de 2009 sobre la difusión y la protección de la creación en Internet (también llamada «loi Hadopi») introdujo una nueva institución, la "Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet" (HADOPI) - un organismo administrativo autorizado para prohibir el acceso a Internet a usuarios individuales que infringieron las normas nacionales de derechos de autor a pesar de las advertencias previas (la llamada ley de los

tres strikes). Según la primera versión de este texto legal, que fue evaluada por el Consejo Constitucional, la decisión de no permitir el acceso a Internet la tomaría un órgano administrativo (HADOPI) sin supervisión judicial.

La consecuencia de la adopción de este texto legal consiste en una denuncia constitucional basada en el derecho a la libertad de expresión, y en particular en el derecho a la información. Los demandantes argumentaron que "al otorgar a una autoridad administrativa, aunque independiente, el poder de imponer sanciones como la denegación del acceso a Internet, el Parlamento violó en primer lugar el derecho fundamental a la libertad de expresión y comunicación y, en segundo lugar, introdujo sanciones evidentemente desproporcionadas"[814].

Según el Consejo, "la facultad de imponer sanciones […] confiere a [HADOPI], que no es un tribunal de justicia, la facultad de restringir o denegar el acceso a internet a los titulares del acceso y a las personas a las que éstos permitan acceder a la Internet" y, por tanto, podría llevar "a restringir el derecho de cualquier persona a ejercer su derecho a expresarse y comunicarse libremente, en particular desde su propia casa", es contraria a la garantía de libertad de expresión prevista por el artículo 11 de la Constitución francesa.

En conclusión, las disposiciones de la ley HADOPI han sido declaradas inconstitucionales y la decisión del Consejo se interpretó como una confirmación del derecho al acceso a Internet. Finalmente, el parlamento francés revocó toda la ley en 2013 por ser excesivamente restrictiva de los derechos individuales, pero el debate sobre la existencia de un derecho humano al acceso a Internet y la protección de los derechos humanos en el ciberespacio continúa.

En resumen, se puede reconocer en el siglo XXI que el derecho a acceder el Internet es un derecho humano fundamental nuevo y específico, derivado del derecho a la vida privada, de la libertad de expresión, incluido el derecho a recibir información. Limitar o privar del acceso a Internet influye directamente en el alcance de la libertad de expresión exigible. Como nota al margen, se podría considerar esta conclusión como una fuerte adición a la importancia de las iniciativas[815] de la ONU destinadas a desarrollar políticas internacionales de protección de los derechos humanos en el entorno virtual.

---

[814] Conseil Constitutionnel Français (2009) *Décision n° 2009 – 580 DC. Loi favorisant la diffusion et la protection de la création sur Internet*, recuperado de: https://www.conseil-constitutionnel.fr/sites/default/files/as/root/bank_mm/decisions/2009580dc/doc.pdf.

[815] James, J. (2008) *Digital Divide Complacency: Misconceptions and Dangers*, The Information Society Journal Volume 24, 2008 - Issue 1, pp. 54-61.

Como hemos mostrado más arriba, el poder de abusar de los derechos humanos individuales en línea, especialmente en el caso del derecho a la vida privada, ya no está exclusivamente en manos de los gobiernos. Solo con la ayuda de los proveedores de servicios informáticos como Google, Microsoft, Facebook o Yahoo, que ofrecen sus servicios a millones de usuarios de diversas jurisdicciones y de diferentes nacionalidades, un estado es capaz de ejercer sus leyes nacionales.

Al mismo tiempo, el carácter transfronterizo de la red hace que sea técnicamente mucho más fácil invadir los derechos individuales, ya sea mediante la recopilación automática de datos digitalizados, la interceptación de comunicaciones en línea o la inhabilitación del acceso a contenido particular. Esos detalles requieren readaptar el marco de derechos humanos, que es una obligación específica a los Estados parte, para corresponder a la multitud de intereses que se manifiestan en el ciberespacio. Por más desafiante que pueda parecer, la comunidad internacional ha intentado involucrar a las empresas privadas en la protección de los derechos humanos durante más de medio siglo; el punto de partida fue el surgimiento del derecho ambiental internacional, lo que exigió una mayor cooperación pública-privada para proteger los derechos ambientales de las personas.

A partir de la experiencia del derecho ambiental internacional, se debe identificar un conjunto de normas, como una guía universal dedicada a las empresas en línea, es decir a los proveedores de servicios de Internet, que les permitan identificar sus obligaciones en materia de derechos humanos. Para que eso sea posible, el catálogo de derechos humanos, tal como se reconocía antes del rápido desarrollo de las comunicaciones en línea, es decir hasta principios de la década de 1990 (en 1991, la Fundación Nacional de Ciencia de los Estados Unidos habilitó el uso comercial de la red inicialmente académica, provocando la "burbuja punto.com") deben volver a analizarse con el contexto de la aplicación de los derechos humanos en el ciberespacio transfronterizo.

La sociedad civil, las organizaciones internacionales y los Estados han realizado numerosos intentos en ese sentido. Todos brindan interpretaciones prácticas del amplio catálogo de derechos humanos a la luz de los escritos académicos y la jurisprudencia existentes en el contexto de la práctica y los principios de gobernanza de Internet. Nuevas categorías de derechos humanos han sido identificadas en el nuevo contexto tecnológico, incluso derechos que se manifiestan exclusivamente en el entorno online.

Desde la colaboración pública-privada han resultado varias iniciativas que tienen como objetivo mejorar la experiencia del usuario en el entorno online para poder gozar de todos sus derechos y libertades. Entre las iniciativas de la sociedad civil, la más elaborada es un intento de un grupo de trabajo financiado inicialmente para el Foro de Gobernanza de Internet, que actualmente opera como una "red abierta" compuesta por "personas y organizaciones (…) comprometidas con hacer que Internet funcione a favor de los derechos humanos"[816].

Sus diez principios y derechos de Internet[817], denominados la Carta IRPC, son la propuesta más concisa para reintroducir los derechos humanos en el entorno en línea. La carta está fuertemente arraigada en el derecho internacional de los derechos humanos y se basa en un análisis exhaustivo de los documentos existentes y el soft law. Los principios básicos, que reflejan las condiciones para la mínima protección de los derechos humanos en línea, incluyen:

1. igualdad de oportunidades y universalidad de derechos: el entorno on line debe garantizar el libre ejercicio de los derechos humanos, el respeto de la dignidad y el acceso de los usuarios a todas las oportunidades de desarrollo personal.
2. justicia social y respeto mutuo: el Internet, como espacio libre e infinito, permite a los usuarios de manifestarse de forma libre, pero el respeto de los derechos humanos y de la dignidad de los demás usuarios debe representar la norma social que regula las relaciones virtuales.
3. acceso libre a los recursos electrónicos: el espacio cibernético es el mejor medio para la promoción y cumplimento de los derechos humanos. Para permitir la libre manifestación de estos derechos se debe garantizar el libre acceso para todos los individuos a los recursos en línea. Dicho acceso debe ir acompañado del derecho a utilizar la red de una forma "segura y abierta";
4. libre capacidad de expresión y asociación: los internautas son personas interesadas a buscar, recibir y difundir información. La censura o la interferencia con esta actividad de los usuarios puede constituir un abuso. El acceso no discriminatorio a la red debe permitir a cualquier ciudadano informarse y participar en el proceso de e-gobernanza de la

[816] La Coalición "Principios y Derechos de Internet" es una de las coaliciones dinámicas creadas bajo los auspicios del Foro de Gobernanza de Internet. Es una red abierta de participación múltiple de individuos y organizaciones dedicada a fomentar los estándares de derechos humanos en las políticas y procesos de gobernanza de internet. La visión de la coalición de Principios y Derechos de Internet se concentra sobre los esfuerzos de impulsar estándares de derechos humanos en la gobernanza de internet. Mas información sobre la coalición en: https://internetrightsandprinciples.org/.
[817] Disponible en: https://derechoseninternet.com/docs/IRPC_Carta_Derechos_Humanos_Internet.pdf

sociedad. Al mismo tiempo, todo el mundo tiene derecho a asociarse libremente a través de Internet, con fines sociales, políticos, culturales o de otro tipo.

5. protección de la intimidad y de los datos personales: el Internet no es una selva y el usuario no puede ser sometido a navegar en un estadio de permanente estrés causado por la falta de protección de su vida privada. El usuario debe tener la posibilidad y las herramientas necesarias para proteger sus datos personales, de navegar en modo anónimo o ocultar su verdadera identidad. Su derecho de existir digitalmente de le permite elegir su personalidad virtual, su perfil, ocultar su identidad real detrás de contraseñas y claves de acceso. Todo usuario tiene derecho a la protección de datos, incluyendo el control sobre la recolección, retención, transformación, eliminación y divulgación de sus datos personales.

6. seguridad, libertad y vida virtual: El derecho a la vida, la libertad y la seguridad deben ser respetados, protegidos y cumplidos en Internet, de mismo modo que ocurre en el entorno físico. Ningún otro derecho digital no puede afectar estos derechos fundamentales, siendo prohibido cualquier acto de incitación al odio racial o religioso o de alentando al genocidio.

7. diversidad cultural y lingüística: los usuarios que interaccionan en el mundo virtual pertenecen a culturas y pueblos diferentes, aspecto que hace interesante toda esta interaccion libre e ilimitada. Preservar la diversidad significa aumentar el intercambio de información y datos lo que fomenta las "innovaciones técnicas y políticas".

8. igualdad en la red: es un derecho humano especifico [ara el entorno virtual que supone el acceso universal y abierto a los contenidos de Internet, sin priorizaciones discriminatorias, filtrados o control de tráfico por razones comerciales o políticas.

9. sistema de normas y procedimientos: la interoperabilidad completa, la inclusión y la igualdad de oportunidades para todos se basa en los estándares abiertos que son a la base de la arquitectura de Internet. Otro derecho específico del ciberespacio es el derecho a la reglamentación técnica no discriminatoria de los recursos en línea, resultado de la estructura de Internet en capas, mencionada anteriormente. Esta propuesta debe verse como una referencia a la necesidad de garantizar los derechos humanos en línea no solo por medios políticos o legales, sino también por medios técnicos, fundamentales para el funcionamiento de Internet. La interferencia con este último está destinada a dar forma al primero: en el entorno en línea, cualquier modificación de este tipo debe garantizar un acceso igualitario y no discriminatorio a todos los recursos de Internet, a fin de evitar la discriminación basada en la situación económica o tecnológica.

10. el estado de derecho virtual: los derechos Humanos y la justicia social deben ser la base jurídica y normativa sobre la que operar en Internet. Con un Internet basado en los principios de la participación inclusiva y la rendición de cuentas estos principios se vuelven realidad. La carta se refiere a los derechos humanos como la base de toda la gobernanza de Internet, dado que es la comunidad global la que debe ser gobernada, el compromiso existente de derechos humanos, que refleja las diferentes facetas de la dignidad humana, debe estar en sus bases. Dicho compromiso debe identificarse y aplicarse mediante una cooperación de múltiples partes interesadas.

Otra propuesta de la sociedad civil, ofrecida por la Asociación de Comunicaciones Progresistas[818], una asociación sin fines de lucro de más de cinco docenas de redes miembro de todo el mundo, con el compromiso de asegurar que Internet sirva a los intereses de la sociedad civil global. Tiene el mismo objetivo y un contenido muy similar al del IRPC, aunque organizado de manera diferente. La propuesta[819] se centra en seis temas que reflejan:

1) la necesidad de un acceso universal a Internet "para todos";

2) la libertad de expresión y asociación debe otorgarse tanto en línea como fuera de línea;

3) acceso al conocimiento, que refleja la necesidad de preservar la neutralidad de la red, así como el uso justo y la libertad de información, incluido el derecho a compartirlo y acceder a él;

4) en consecuencia, una referencia directa a la necesidad de seguir desarrollando software libre y de código abierto como garantía de "aprendizaje y creación compartidos";

5) la necesidad de privacidad en línea y el derecho a protegerla a través de medios electrónicos, como software de cifrado;

6) la necesidad de utilizar los derechos humanos como base para todas las actividades relacionadas con la gobernanza de Internet, en particular la neutralidad de su establecimiento de normas y la supervisión de múltiples partes interesadas de todas las actividades de gobernanza. Finalmente, la carta pide una mayor difusión de información sobre el alcance de los derechos en línea, derivada de la legislación de derechos humanos

[818] La Asociación para las comunicaciones progresistas (APC) es una red global de redes dedicada a apoyar a organizaciones, movimientos sociales e individuos en el uso de la información y las tecnologías de la comunicación, para ayudar a construir comunidades e iniciativas que tengan el propósito de realizar aportes significativos al desarrollo humano, la justicia social, las democracias participativas y las sociedades sostenibles. Mas información disponible en: https://www.apc.org/es/sobre-apc.

[819] Disponible en: https://www.apc.org/sites/default/files/APC_charter_ES_0_0_0_0.pdf.

y enfatiza la necesidad de introducir medidas efectivas de aplicación frente a las violaciones de derechos humanos en línea.

En los últimos años hay muchas propuestas sobre la reglamentación de los derechos humanos en el entorno online. La vida digital se está expandiendo y la práctica demuestra que es necesario adaptar el marco legislativo a las nuevas realidades. Pero la velocidad del desarrollo electrónico es difícil de seguir por los juristas y los legisladores.

Todas las propuestas comparten una característica común: introducen un nuevo modelo de redacción de actos jurídicos, basado en la participación de la comunidad en línea, abierto a la participación de la sociedad civil, que refleja las necesidades y esperanzas de los miembros de la comunidad. Las propuestas de cartas y códigos de derechos digitales reflejan el catálogo bien establecido de derechos humanos, pero lo modifican mediante la introducción de novedades, elementos cibernéticos específicos, como la necesidad de hacer de la gobernanza de Internet un proceso de múltiples partes interesadas y garantizar su neutralidad a través de procedimientos democráticos y estándares técnicos.

Sin embargo, la reevaluación de los derechos humanos para el entorno en línea no ha sido realizada únicamente por la sociedad civil y las ONG. En este proceso también participan tribunales y órganos internacionales.

En lo que concierne a las comunicaciones en línea, los desafíos clave, que enfrentan la comunidad internacional en general y los tribunales internacionales en particular, consisten en la confrontación de valores iguales presentados por la privacidad individual y la seguridad colectiva, por un lado, y la libertad de expresión frente a la obscenidad nacional de las leyes de difamación por el otro. Mientras el primer desafío permanezca sin resolver, el último parece ser desmantelado lentamente por los tribunales internacionales y las reglamentaciones nacionales, introduciendo regulaciones cada vez más detalladas sobre el filtrado de Internet y los procedimientos de notificación y eliminación.

Con respecto a la privacidad, las Observaciones generales del Comité de Derechos Humanos de la ONU de 1988 sobre la privacidad (uno de los primeros documentos de la ONU sobre el tema relacionado con las redes de telecomunicaciones) sigue siendo directamente aplicable a los desafíos en línea, en particular a la luz de la reciente controversia sobre la vigilancia de la NSA. El caso de la libertad de expresión en línea parece algo más desafiante que todavía no tiene un documento-guía para orientar las partes implicadas.

La vida privada del ser humano ocupa un lugar bien establecido en el catálogo de derechos humanos, con el artículo 12 de la Declaración Universal de los Derechos Humanos o el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos que conceden a todas las personas la libertad de "injerencias arbitrarias" en su "privacidad, familia, hogar o correspondencia", así como de cualquier "atentados contra su honor y reputación"[820], colocando la privacidad entre el catálogo de derechos personales conocido por todos los ordenamientos jurídicos nacionales.

La ONU dedicó mucha atención a la protección de la vida privada de los individuos al discutir los temas de la prevención del terrorismo. M. Scheinin[821] relator especial sobre derechos humanos y terrorismo, manifiesta acertadamente que, fue la guerra contra el terrorismo la que condujo a una rápida erosión del derecho a la privacidad. La razón de esto fue principalmente la deficiencia inherente del artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, que otorga al individuo el derecho a la vida privada: la falta de una cláusula limitativa que requiera que los estados cumplan con tres criterios básicos: la necesidad, proporcionalidad y legalidad de la interferencia, pero argumenta que su contexto mismo introdujo tales obligaciones que recaen sobre los Estados.

El contenido de dicha obligación y los límites de la privacidad individual permitidos por el derecho internacional de los derechos humanos son el núcleo del desafío que plantean las comunicaciones en línea, ya que, como ya se mencionó anteriormente, la comunidad en línea global necesita un estándar de privacidad global para una protección verdaderamente eficaz.

De acuerdo con la Declaración Universal de los Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos por igual, la libertad frente a las intrusiones en la privacidad debería ser protegida a través de leyes que otorguen protección "contra tales injerencias o ataques". Sin embargo, cuando se trata de establecer los límites de la privacidad, existe una diferencia significativa entre los dos documentos de derechos

[820] Observación general No. 16 del Comité de Derechos Humanos de la ONU: Artículo 17 (Derecho a la privacidad), El derecho al respeto de la privacidad, la familia, el hogar y la correspondencia, y la protección del honor y la reputación, 8 de abril de 1988, disponible en: https://conf-dts1.unog.ch/1%20SPA/Tradutek/Derechos_hum_Base/CCPR/00_2_obs_grales_Cte%20DerHum%20%5BCCPR%5D.html#GEN16.

[821] Asamblea General de las Naciones Unidas, Consejo de Derechos Humanos (2009) Informe del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Martin Scheinin, 28 de diciembre de 2009, U.N. Doc. A / HRC /13/37, pág. 1;

humanos fundamentales analizados. Si bien la Declaración contiene una cláusula limitativa general en su artículo 29 párrafo 2:

> *"En el ejercicio de sus derechos y en el disfrute de sus libertades, toda persona estará solamente sujeta a las limitaciones establecidas por la ley con el único fin de asegurar el reconocimiento y el respeto de los derechos y libertades de los demás, y de satisfacer las justas exigencias de la moral, del orden público y del bienestar general en una sociedad democrática".*

que somete el ejercicio de todos los derechos y libertades mencionados a las limitaciones determinadas exclusivamente por la ley, en el Pacto Internacional de Derechos Civiles y Políticos no se puede encontrar una referencia general ni una relacionada directamente con la privacidad, aunque se pueden encontrar cláusulas limitativas individuales para otros derechos, como el artículo 19 párrafo 3, permitiendo la limitación legítima de la libertad de expresión:

> "*El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para: a) Asegurar el respeto a los derechos o a la reputación de los demás; b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas*".

Si bien la prueba de las tres condiciones para restringir los derechos puede ser objeto de críticas por ser ampliamente vaga, por lo menos establece algunos estándares básicos que los Estados deben respetar cuando interfieren con las libertades fundamentales y brinda garantías para los derechos de las personas dentro de sus jurisdicciones. Sin embargo, esto no significa que el derecho a la vida privada sea absoluto. Como es visible también en otros tratados de derechos humanos, solo por mencionar el artículo 8 del Convenio Europeo de Derechos Humanos, el derecho a la vida privada, como cualquier otro derecho humano, puede estar sujeto a limitaciones previstas por la ley y necesarias en una sociedad democrática para la protección de derechos y libertades de los demás.

La necesidad de esbozar una cláusula limitativa para la privacidad se materializo con la serie de documentos del Comité de los Derechos Humanos (CDH) de las Naciones Unidas, iniciados en 1988, y la Observación General No. 16 mencionada anteriormente. En este documento elemental, el CDH declaró claramente que, de acuerdo con los estándares de derechos humanos vigentes: "*Debe prohibirse la vigilancia, por medios*

electrónicos o de otra índole, la intervención de las comunicaciones telefónicas, telegráficas o de otro tipo, así como la intervención y grabación de conversaciones". Si bien este no es ni mucho menos el único documento que expresa la necesidad de proporcionar bases legales legítimas para cualquier vigilancia, debe tenerse en cuenta que ya en 1988, antes de que Internet ganara su valor comercial, el CDH proporcionó orientación directamente aplicable a las comunicaciones en línea. En su comentario, el CDH confirmó la aplicabilidad de la prueba de los tres pasos a la privacidad. Cualquier invasión a la privacidad debe ser legal y no arbitraria, mientras que no puede tener lugar ninguna interferencia "excepto en los casos previstos por la ley", mientras que la legislación pertinente debe especificar en detalle las circunstancias precisas en las que se pueden permitir tales interferencias, y "una decisión para hacer uso de dicha interferencia autorizada debe hacerse […] caso por caso"[822].

Para evitar la injerencia arbitraria, el CDH hizo hincapié en que "incluso la injerencia prevista por la ley debe estar en consonancia con las disposiciones, las finalidades y los objetivos del Pacto y ser razonable en las circunstancias particulares"[823]. El régimen de derechos humanos existente obliga a los estados no solo a abstenerse de violar los derechos humanos individuales, incluido el derecho a la vida privada, sino también a actuar para brindar su protección efectiva. El CDH enfatiza esta obligación de diligencia debida al afirmar que: "*los Estados deben adoptar medidas eficaces para velar por que la información relativa a la vida privada de una persona no caiga en manos de personas no autorizadas por ley para recibirla, elaborarla y emplearla y porque nunca se la utilice para fines incompatibles con el Pacto"*[824].

La Observación general de 1988 fue seguida por otros documentos de la ONU que tratan de forma directa o indirecta sobre los límites de la privacidad individual percibida como un derecho humano. Como hemos analizado, el derecho a la vida privada está particularmente amenazado por las operaciones de seguridad del Estado, y en estas circunstancias la polémica sobre la cuestión de sus límites en las acciones estatales contra el terrorismo sigue fomentando la literatura jurídica y filosófica en este ámbito. Es el

[822] Consejo de Derechos Humanos (2009) *Informe del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Martin Scheinin, 28* de diciembre de 2009, U.N. Doc. A / HRC /13/37, pág. 2.
[823] Ibidem.
[824] Observación general No. 16 del Comité de Derechos Humanos de la ONU: Artículo 17 (Derecho a la privacidad).

Informe de 2009 del Relator Especial del CDH[825] sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo el que proporciona un análisis detallado del frágil equilibrio entre la seguridad del Estado y la privacidad individual.

El Relator Especial sostiene que el artículo 17 permite "restricciones necesarias, legítimas y proporcionadas al derecho a la vida privada", al tiempo que contiene "elementos de una prueba de limitaciones permisibles". Con base en esta evaluación, considera que el derecho internacional exige que los estados "justifiquen por qué un objetivo particular es una justificación legítima para las restricciones al artículo 17" y enfatiza el papel que las nuevas tecnologías han tenido un papel importante en la erosión de la privacidad. Haciendo eco del trabajo del CDH y resumiendo la jurisprudencia del Protocolo Facultativo, Scheinin identifica siete criterios que cualquier restricción de privacidad debe cumplir. Entre ellos se incluyen: su disposición por ley, la no injerencia en la esencia del derecho, la necesidad en una sociedad democrática, la ausencia de discrecionalidad ilimitada, la necesidad de cualquier restricción para alcanzar, más que el objetivo, uno de los fines legítimos, la proporcionalidad de la medidas restrictivas y coherencia con otros derechos otorgados por el Pacto[826].

Hablando de mejores prácticas, Scheinin propone cinco principios aplicables a cualquier restricción de la vida privada introducida de acuerdo con el régimen del Pacto. El opta por un principio de intrusión mínima, alentando a los estados a asegurarse de que han "agotado las técnicas menos intrusivas antes de recurrir a otras"[827]. Siguiendo el ejemplo británico, recomienda un principio de minimización de datos que ayuda a los Estados a resistir a la tendencia de recopilar para siempre más datos personales, incluso cuando no sea necesario, pero es técnicamente fácil y posible.

Otra recomendación se expresa en el principio de "especificación del fin para limitar utilizaciones secundarias", que obliga a los Estados a introducir salvaguardias legales para el uso de datos por razones distintas de las identificadas como fundamento para su recopilación inicial. Otra garantía para la privacidad es el principio de "supervisión y autorización regulada del acceso legal". Esta noción fomenta la

[825] Consejo de Derechos Humanos (2009) *Informe del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Martin Scheinin*, 28 de diciembre de 2009, U.N. Doc. A / HRC /13/37. Recuperado de: https://undocs.org/es/A/HRC/13/37
[826] Idem.
[827] Idem.

introducción de salvaguardas efectivas para la supervisión de las entidades de recolección y procesamiento de datos, también con posibilidad de revisión independiente.

El cuarto principio para la protección de la privacidad es el de "transparencia e integridad" que requiere apertura y comunicación entre los estados sobre sus prácticas de vigilancia. Este principio refleja la normativa de protección de datos personales que otorga a las personas el derecho a acceder a la información sobre ellos recopilada por organismos públicos y privados. Finalmente, reflejando el acelerado progreso tecnológico, el Relator Especial recomienda la "modernización efectiva" como el quinto principio de protección de la vida privada en la sociedad moderna. A juicio del Relator especial, la facilidad con la que se pueden recopilar los datos no se refleja en el nivel de las medidas legislativas y tecnológicas para protegerlos del uso o acceso no autorizado. Las evaluaciones de impacto en la privacidad, introducidas por algunos estados y por algunas empresas, se recomiendan como una herramienta para combatir esta falta de proporcionalidad[828].

La Resolución A/HRC/20/L.13 adoptada por la Asamblea General de la ONU en el año 2012[829], que consta de 5 párrafos, expresa la aplicabilidad esencial de la jurisprudencia de derechos humanos a las comunicaciones en línea. Adoptada por 71 partes, incluso los estados conocidos por sus políticas de filtrado y vigilancia como Estados Unidos, Turquía, India, Egipto y Túnez, el documento afirma directamente que los mismos derechos que las personas tienen fuera de línea también deben protegerse en línea con especial énfasis a la libertad de expresión en línea, de acuerdo con las normas vigentes del artículo 19 de la Declaración Universal de Derechos Humanos. Reflejando la Agenda de Túnez de 2005, hace una referencia a la "naturaleza global y abierta de Internet como fuerza impulsora" para el progreso, estimulando a los estados a "promover y facilitar" el acceso a Internet.

Analizando todo lo expuesto, parece que la ONU está en camino de asumir el desafío de resolver el problema de los derechos humanos en línea. Sin embargo, debe enfatizarse que, si bien la aplicabilidad de los derechos humanos globales, pero interpretados localmente, puede considerarse un desafío difícil para la sociedad mundial de la información. Es la voluntad diplomática la que puede determinar el éxito en su protección efectiva. Con respecto a las directrices detalladas de la ONU sobre privacidad mencionadas anteriormente y la reciente controversia de la NSA, que desplegó una

[828] Idem.
[829] Disponible en: https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_20_L13.pdf

vigilancia masiva sin un objetivo legítimo y una validación de caso afirmado, no es el desafío legal sino la motivación política lo que es decisivo para la protección efectiva de los derechos humanos en línea.

Si bien la aplicación de los derechos humanos en línea puede parecer un desafío, el derecho internacional existente proporciona soluciones detalladas para su aplicación en el ciberespacio. La jurisprudencia de los derechos humanos y la literatura jurídica académica permiten identificar los límites de las intrusiones permitidas sobre los derechos individuales, mientras que el derecho internacional sobre la responsabilidad estatal contiene la obligación de los estados de prevenir activamente las violaciones de los derechos humanos dentro de sus jurisdicciones.

Por lo tanto, parece que la Resolución del CDH de 2012 sobre la aplicabilidad de los derechos humanos en línea es el primer paso hacia la aplicación al entorno en línea del marco regulatorio vigente sobre de derechos humanos, siguiendo las recomendaciones y análisis proporcionados por los relatores especiales de la ONU, así como por el mundo académico y la sociedad civil, reiterados anteriormente.

Por esta razón, el elemento crucial para una protección efectiva de los derechos humanos no es el desafío legal, sino la falta de voluntad política. Esa voluntad política puede ser provocada por la sociedad civil, consciente de sus derechos y de las obligaciones de los Estados. Como demostraron los ejemplos de la Primavera Árabe o las manifestaciones del ACTA, el ciberespacio es una herramienta eficaz para aumentar la participación de la sociedad y aumentar la conciencia individual. A medida que los usuarios de Internet se vuelven más conscientes de sus derechos, los estados seguramente serán más conscientes de sus obligaciones en materia de derechos humanos, incluido su deber de responsabilizar a las empresas privadas por su participación en violaciones de derechos humanos, por ejemplo, exportando tecnologías de vigilancia.

La revolución de Internet ha provocado un cambio significativo en el panorama del derecho público e internacional: el papel cada vez mayor del derecho indicativo (soft law), visto como directrices no ejecutables que configuran las políticas futuras. Debido a su carácter multifacético y complejidad, es difícil ubicar el Internet bajo un único régimen legal internacional; por lo tanto, la mayoría de los documentos internacionales contemporáneos relacionados con la gobernanza de Internet se consideran de naturaleza indicativa. Si bien, esta distinción es desafiante debido a la naturaleza ambigua de la

división entre el derecho imperativo y el derecho indicativo. McDougal[830] y Lichtenstein[831] cuestionan la distinción misma entre ley y política, mientras que Fastenrath[832] considera que el derecho indicativo es crucial en términos de ejercer cualquier impacto político.

En el contexto de las obligaciones internacionales de los estados, la distinción generalmente reconocida entre la ley dura y la ley blanda radica en la posibilidad de poder responsabilizar a los estados por no cumplir con tales obligaciones. Aun cuando, un Estado que infringe una obligación especificada en un tratado o en la práctica del derecho consuetudinario puede ser considerado internacionalmente responsable de hacerlo, no se le pueden imponer consecuencias legales por no cumplir con un requisito de derecho indicativo, consagrado, por ejemplo, en una declaración o una recomendación de una organización internacional o un grupo de expertos.

Dichos documentos pueden considerarse fuentes adicionales para identificar una norma consuetudinaria existente, pero deben ir acompañados de prácticas estatales uniformes y decisiones judiciales que confirmen el carácter vinculante de las normas allí consagradas. Sin embargo, esta distinción teórica aparentemente simple entre el derecho imperativo y el derecho indicativo, que identifica las obligaciones individuales como originadas en un tratado o derecho consuetudinario universal o regional, resulta ser más difícil en la práctica en todas las áreas de las relaciones internacionales, y en particular cuando se trata de identificar las partes responsables de violaciones de derechos humanos.

Por lo tanto, son principalmente los documentos de derecho indicativo, como la Resolución del año 2012 sobre la promoción, protección y disfrute de los derechos humanos en Internet, acompañada de otros documentos discutidos anteriormente, los que están destinados a dar forma a la formulación de políticas futuras, tanto a nivel nacional como internacional.

Sobre todo, estamos viviendo tiempos interesantes para la evolución de los derechos humanos y la sociedad. La pandemia COVID 19 nos ha demostrado que la limitación de los derechos fundamentales puede surgir tan fácil y las personas la aceptan sin pedir mucha justificación, solo para defenderse ante de un enemigo invisible,

[830] McDougal, M. S. (1954) *International Law, Power and Policy: A Contemporary Conception*, Recueil des cours, Vol 82.
[831] Crawford Lichtenstein, C. (2001) *Hard Law v. Soft Law: Unnecessary Dichotomy?*. The International Lawyer Vol. 35, No. 4 (WINTER 2001), pp. 1433-1441
[832] Fastenrath, U. (1993) *Relative Normativity in International Law*, European Journal of International Law, Volume 4, Issue 3, 1993, pp. 305–340

insuficientemente conocido o demostrado. En el transcurso del año 2020, nuestros derechos y libertades para viajar, explorar, buscar la felicidad, trabajar se han visto limitados, anulados sin posibilidad de protestar ante todas estas restricciones.

Las generaciones que han nacido con estos derechos y no fueron implicadas en la lucha para su reconocimiento deben comprender y apreciar la importancia del ejercicio efectivo de sus libertades. Renunciar a los instrumentos legales de reconocimiento y protección de los derechos y aceptar restricciones e intrusiones en los contenidos de los derechos fundamentales, sin interrogar las autoridades sobre la necesidad y legalidad de las medidas restrictivas, no es un comportamiento que puede fomentar el desarrollo democrático de la comunidad internacional.

CONCLUSIONS

The cyberspace is a new virgin territory that states are interested in, exploring the possibility to transfer their sovereignty using the relentless technological advance. The rapidity of the changing process of information technologies causes constant challenges that must be solved by the international community in order to find the best way to regulate this space.

The legal problems that arise in the virtual context are far from being resolved. However, the international legal system provides a point of reference and establishes a normative framework that in some way provides a solution - often transitory - to the problems that must be resolved without delay. On many occasions this fact reflects the interest of the States to promote a specific regulation.

There are some fundamental questions to which international law must provide an answer: like the issue of sovereignty and jurisdiction are essential when determining the competences of the State in the regulation of cyberspace and the activities related to it. In this context, first of all, it will be necessary to determine the legal regime of cyberspace – for example if it is a space susceptible of appropriation or if a particular legal regime is established - to be able to determine the state competences both over the space itself considered and with respect to the activities carried out in it. In this way, it will be feasible to determine the responsibility of the State with respect to the prosecution of criminal activities that take place in cyberspace.

Likewise, another matter of fundamental importance is linked to the State's international responsibility regime. In this area, determining what acts can be attributed to the State is essential since issues such as the consequences of international responsibility or the exercise of the right of self-defense depend on this attribution. Given the characteristics of cyber operations, it is very important to determine the value that will be given to those cyber operations carried out by non-state actors, since the possibility of the occurrence of such events is increasing.

In relation to the use of force within the framework of the *ius ad bellum*, there is no doubt that the current legal regime, elaborated from common law and conventional rules (like

articles 2 (4) and 51 of the Charter of the United Nations) and customary law, is capable of providing a satisfactory, albeit transitory, response to the problems that arise around cyber operations. However, it is also undoubted that it will be necessary to adapt them to the new realities that arise and for this an open debate among all States will be necessary.

Cybercrime, considered one of the most profitable criminal behavior, comprises a varied panoply of criminal activities, some of which are nothing but traditional criminal behaviors that take advantage of this new medium that is cyberspace to develop, while others constitute new forms of crime associated with the birth of this new space for social interaction. In this field we find the first international rule, accepted by a great number of states, that establishes a legal framework dedicated to cybercrime prevention. We are talking here about the Convention on Cybercrime (Budapest, 2001), drawn up within the framework of the Council of Europe. The Convention does not contain a definition of what is to be understood by "cybercrime", but instead opts to refer, within the part corresponding to substantive criminal law, to the different criminal behaviors that the States parties must incorporate into their internal legal framework. In this sense, crimes against the confidentiality, integrity and availability of data and computer systems are distinguished (illegal access, illegal interception, attacks on data integrity, attacks on the integrity of systems and abuse of devices), computer crimes (computer forgery and computer fraud), crimes related to content (child pornography) and, finally, crimes related to infringements of intellectual property and related rights.

Kenneth Geers[833] describes the evolution of cybersecurity as an international experiment which has rapidly evolved from a purely technical discipline to a strategic concept. Globalization and the Internet, he notes, have provided individuals, organizations, and states with incredible power based on the constant development of network technology. For everyone - students, military, spies, propagandists, hackers or terrorists - the collection of information or funds, communications and public relations have been digitized in a truly revolutionary way. The former United States Under-Secretary of Defense Marco Roscini[834] reminds us that this digitization is a double-edged sword,

[833] Geers, K. (2011). Strategic Cyber Security. Publicación del NATO Cooperative Cyber Defence Centre of Excellence (CCD COE).
[834] Roscini, M. (2014) Cyber Operations and the Use of Force in International Law Oxford University Press.

because in this our 21st century, “bits and bytes can become so threatening like bullets and bombs”.

Roscini himself announces that cybersecurity is set to become increasingly important in the years to come. The threat no longer comes, only, from the classic adolescent hacker, but also from highly ideological individuals (hacktivists), from States, criminals and terrorist organizations. Cyber technologies and skills are relatively cheap and easy to obtain, allowing weak states and even non-state actors to cause considerable damage to other states, even if these last ones have a considerably greater military power.

Cybersecurity has consequently changed, as we have already noted, from originally being a purely technical discipline to constituting an important part of national security strategies. Not surprisingly, there has been talk of the possibility of cyberspace becoming a global battlefield and, in fact, in not a few countries it is considered the fifth area of war (the other four are terrestrial, maritime, air and space). Since the 1990s all actors have being tryng to reaching an international agreement to limit the risk of an armed cyber conflict.

However, it does not seem that an agreement of such characteristics can be reached today, among other reasons because any effort to eliminate or reduce malicious software is not feasible, since, on the one hand, its intangibility makes it not It is possible to subject it to control and verification mechanisms and, on the other hand, its code is hardly recognizable as malicious without a deep analysis that, in addition, allows to find out the intended use of it.

Furthermore, States are reluctant to dispose of the possibilities offered by the non-lethal use of cyber weapons for the purpose of disruption or interference. Proposals such as the one made in September 2011 by China, the Russian Federation, Tajikistan and Uzbekistan, so that through a resolution of the United Nations General Assembly an “International Code of Conduct for Information Security” will be adopted, that included non-proliferation measures, have not yet found fertile ground in which to bear fruit.

Among other reasons, not the least is determined by terminological differences: while the member states of the Shanghai Cooperation Organization use the expression “information security”, in western states they speak of “cybersecurity”, which, beyond the pure nominal difference, it reflects a different approach in relation to the always complicated balance between security and civil liberties. While some States focus mainly on respect

for the principles of sovereignty and territorial integrity, national security and political stability, others emphasize the importance of safeguarding human rights and the free flow of information, as well as promoting police cooperation and information exchange.

In cyberspace, States are subject to the prohibition of the threat or use of force and the obligation to respect the sovereignty and territorial independence of other States, in the same way that they are in the physical world, in that world "of flesh and steel" of which Barlow[835] spoke. These confidence-building measures and the exchange of information between States will be, on a day-to-day basis, essential ways to increase predictability and reduce the risks that a misperception could lead to an escalation of tension in cyberspace.

However, the different approaches that exist in the international community regarding how to guarantee security in cyberspace have not prevented certain diplomatic initiatives from being undertaken to adopt "confidence-building measures" in this field. This type of measure, as an instrument of international relations, was developed among the military alliances during the cold war in order to avoid nuclear attacks by accident, and since then, its use has spread to other areas, both military and non-military. The most relevant initiatives in this field are those that are taking place within the framework of the United Nations, on whose agenda the issue of cybersecurity has been present since in 1998, when the Russian Federation introduced a draft resolution on the subject in the First Committee of the UN General Assembly (Disarmament and International Security), which was approved with the title of "Developments in the field of information and telecommunications in the context of international security".

Regarding the evolution of human rights in this new world, the current legal literature already proclaimed the appearance of a new range of rights related to the information society that would configure a fourth generation of human rights. Here are two kinds of rights: several rights that have already achieved recognition in many countries, such as

[835] John Perry Barlow (1947-2018), a poet and Internet philosopher, was a cofounder of the Electronic Frontier Foundation and a member of the Board of Directors from 1990 until his death. Barlow's passion for life, liberty, and human connection brought him in contact with a staggering range of people and made him an inspiration all around the world. In his work as an Internet activist, he made us all think about what computer networks might be and to approach the digital future with hope. He always saw the Internet as a fundamental place of freedom, where voices long silenced can find an audience and people can connect with others regardless of physical distance: *"Governments of the Industrial World, you weary giants **of flesh and steel**, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather".*

freedom of expression, the right to protection of sensitive data, privacy, secrecy of communications, among others; and other rights of new data that are just being born, such as the digital rights of the cybercitizen of the digital world.

Several authors and organizations have even advanced several projects and declarations on digital rights. One of the first was that of Robert B. Gelman, who in 1997 published a proposal for a "Declaration of Human Rights in Cyberspace"[836] based on the Universal Declaration of Human Rights of 1948. The Declaration of Independence of Cyberspace published by John Perry Barlow in 1996, presents the Internet as an open path for the improvement of the human condition and society:

"*We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth. We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity. Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here*"[837].

In cyberspace things are somewhat different than in reality: they have no matter, photos can be retouched, ideas circulate with greater freedom. Something similar happens with rights, which are "digitized". This "digitization of rights" is nothing more than making the rights of always pass through the sieve of the characteristics of the digital world.

Private International Law has begun to design new principles to determine what is the applicable law in the digital world, which judges are competent to know the events that occurred there, which procedure is the most appropriate, etc. In general, these principles try to tie the digital event to the real world, seeing where the effects fall: if an injury appears on the Internet, it will be necessary to determine which real world person introduced it, where it is located, the residence of the victim, before which public the offense occurred, etc. The application of spatial criteria (lex loci) is a bit forced in the digital world; It is more convenient to apply personal criteria to the digital legal relationship.

[836] The text of the Declation is available at: http://www.be-in.com/10/rightsdec.html.
[837] John Perry Barlow (1996) A Declaration of the Independence of Cyberspace, available at: https://www.eff.org/ro/cyberspace-independence

Today more than ever it is necessary to escalate the concept of law as a legal rule, to the concept of law as "justice." State law is designed to solve national or sectoral problems, not to address global problems. On the other hand, the notion of "a priori" justice can. Thus, for example, the general principle of "good faith" should be given much more emphasis on the Internet than to the meticulous compliance with the law of the multiple countries where the information may eventually reach.

In this "legal revolution" the protection of human rights must be the main objective. We may renounce to the old law concepts, but we must never give up defending our human liberties and rights also in the cyberspace. Real life and virtual life have the same central point: the individual, as a complex construction, who can not develop and live without the respect for his rights and his human dignity.

BIBLIOGRAFIA

Adler, E (2004) *Communitarian International Relations: The Epistemic Foundations of International Relations*. Editorial Routledge.

Albaladejo, M. (1985) Derecho civil, Tomo. I, vol. 2, Editorial Bosch Barcelona, p. 231.

Albersheim, R. (1999) *The Legal Implications of Corporate Reverse Hacking*, Preventive Law Reporter, vol. 18.

Alexy, R. (2002) *Teoría de los derechos fundamentales*, Editorial CEPEC Madrid.

Alfaro Aguila-Real, J. (1993) *Autonomía privada y derechos fundamentales*. Anuario de derecho civil, Vol. 46, Nº 1, págs. 57-122.

Alland, D. (1994) *Justice privée et ordre juridique international* en Étude théorique des contre-mesures en droit international public, Editorial Pedone, Paris.

Alonso García, R. y Sarmiento, D. (2003) *Los efectos colaterales de la Convención sobre el futuro de Europa en la arquitectura judicial de la Unión: ¿Hacia una jurisdicción auténticamente constitucional europea?*, en Revista de Estudios Políticos, pp. 111-138.

Alonso, J. (2011) *Identidad y reputación digital* en P. Cerezo (Ed.), Cuadernos de comunicación Evoca, 5. Identidad digital y reputación online (págs. 5-10). Madrid, España

Amezúa Amezúa, L. C. (2004) *Los derechos fundamentales en la unión europea*, Revista de derecho (Valdivia), no. 16, pp. 105-130.

Anita L. Allen (1988) *Uneasy Access: Privacy for Women in a Free Society*, Editorial Rowman & Littlefield.

Ansuátegui, F. J. (1997) *Derechos fundamentales, poder político, y poderes sociales*, en (varios autores) Direitos humanos: a promesa do século XXI, Porto, Editorial ELSA.

Anzures Gurría, J. J. (2010) *La eficacia horizontal de los derechos fundamentales*. Cuestiones constitucionales, (no. 22), pp. 3-51;

Aragón Reyes, M. (1997) *La interpretación por el Tribunal Constitucional de la legalidad constitucional y su fuerza vinculante*, en Revista Estudios Jurídicos, Año 2007, Número 2007;

Arbós, T. y otros. (1998) *Los fundamentos de los derechos humanos desde la filosofía y el derecho.* Editorial EDAI, Barcelona.

Arguilla, J. y Ronfeldt, D., (1999) *The Advent of Netwar: Analytic Background*, Studies in Conflict & Terrorism 22.3, pp.193–206;

Aristóteles (1988) *Política*, Editorial Gredos Madrid.

Arthur Raphael Miller (1971) *The Assault on Privacy: Computers, Data Banks, and Dossiers*; University of Michigan Press; First Edition.

Azpitarte Sánchez, M. (2015) *Los derechos fundamentales de la Unión en busca de un nuevo equilibrio,* Revista Española de Derecho Constitucional n.º 104/2015, pp. 243-268;

Azurmendi Adarraga, A. (1998) *El derecho a la propia imagen: su identidad y aproximación al derecho a la información*, 2da. ed., Fundación Manuel Buendía, Universidad Iberoamericana, México, pp. 21 y ss.

Balboni, P. (2010) *Data Protection and Data Security Issues Related to Cloud Computing in the EU*; ISSE 2010 Securing Electronic Business Processes - Highlights of the Information Security Solutions Europe Conference 2010; Tilburg Law School Research Paper No. 022/2010.

Bannelier, K. y Christakis, T. (2017) *Cyberattaques - Prévention-Réactions : Rôles des Etats et des acteurs privés*, Les Cahiers de la Revue Défense Nationale, Paris.

Barnett, S. (1999) The Right to One's Own Image': Publicity and Privacy Rights in the United States and Spain. American Journal of Comparative Law 47, pp. 555–582

Bastida, F.J.; Villaverde, I.; Requejo, P.; Presno, M. A.; Benito Aláez y Sarasola I. F. (2004) *Teoría General de los Derechos Fundamentales en la Constitución española de 1978*, Editorial Tecnos Madrid.

Becet, J. M. y Colar, D. (1982), *Les droits de l'hommes, dimensions nationales et internationales*, Paris, Economica.

Beleiu, Ghe. (1994) *Derecho civil rumano*. Editorial: Sansa SRL, Bucarest.

Bendiek, A. (2016). *Due Diligence in Cyberspace: Guidelines for International and European Cyber Policy and Cybersecurity Policy*, Berlin: Stiftung Wissenschaft und Politik German Institute for International and Security Affair.

Benvenisti, E. (2006) *Substituting International Law*, en The Move from Institutions?, American Society of International Law Proceedings, Vol. 100/2006, p. 289-290.

Bertrand, A. (1999) *Droit à la vie privée et Droit à l'image*, Editorial Litec: Paris.

Bidart Campos, G. (1994) *La interpretación de los derechos humanos*. Editorial Ediar, Buenos Aires.

Bioy, Xavier (2011) *Droit constitutionnel, bioéthique et vie privée*. Recueil des cours de l'Académie Internationale de Droit Constitutionnel, 17. pp. 103-178.

Bîrsan, C. (2010) *Conventia europeana a drepturilor omului. Comentariu pe articole (El Convenio Europeo de Derechos Humanos. Comentarios sobre los artículos)*, Edición 2, C.H. Beck, Bucarest.

Blanke H. J. y Mangiameli, S. (2011) *The European Union after Lisbon: Constitutional Basis, Economic Order and External Action*, Editorial Springer Science & Business Media Berlin.

Blanke, H. J (2006) *Protection of Fundamental Rights afforded by the European Court of Justice in Luxembourg* en: Blanke H. J. y Mangiameli S. (eds) Governing Europe under a Constitution. Editorial Springer, Berlin, Heidelberg.

Böckenförde E. W. (1991) *State, Society, and Liberty: Studies in Political Theory and Constitutional Law*, Editorial Berg, New York.

Böckenförde, E. W. (1993) *Escritos sobre derechos fundamentales*, trad. de Juan Luis Requejo Pagés e Ignacio Villaverde Menéndez, 1.a ed., Editorial Nomos Verlagsgesellschaft, Baden-Baden.

Bogdan, D. y Selegean, M. (2005) *Drepturi şi libertăţi în jurisprudenţa Curţii Europene a Drepturilor Omului (Derechos y libertades en la jurisprudencia del Tribunal Europeo de Derechos Humanos)*, Editorial All Beck Publishing House, Bucarest.

Boizard, M. (2016) *Le temps, le droit à l'oubli et le droit à l'effacement*. Revista Les Cahiers de la Justice 2016/4 (N° 4), pp. 619 – 628.

Bon, P. (1992) *La protección constitucional de los derechos fundamentales. Aspectos de Derecho Comparado Europeo*, en Revista del Centro de Estudios Constitucionales, N.º 11, Madrid.

Bonilla Sánchez, J. J. (2010) *Personas y derechos de la personalidad*, Editorial Reus, Madrid.

Botero Marino, C. y otros (2017) *El derecho a la libertad de expresión. Curso avanzado para jueces y operadores jurídicos en las Américas*. Guía curricular y materiales de estudio, Editorial Centro de Estudios de Derecho, Justicia y Sociedad

Boukongou, J. D. (2007) *Dignité humaine en Afrique centrale 1990-2007*, APDHAC, Yaoundé, 9 juin 2007.

Bowden, J. (2014). *Reasons to explore big data with social media analytics*. Recuperado de: https://www.socialmediatoday.com/content/reasons-explore-big-data-social-media-analytics-videos .

Boyd, J. P. (1950) *The Papers of Thomas Jefferson*. Vol. 1. Princeton, NJ: Princeton University Press, pp. 243–247.

Braud, Ph. (2015) *La notion de liberté publique en Droit français*, Editorial LGDJ, París;

Brunnee, J. and. Toope, S. J. (2010) *Legitimacy and Legality in International Law: An Interactional Account*. Editorial Cambridge University Press.

Buchan, R. (2018) *Cyber espionage and international law*, Editorial Hart Publishing, pp. 168-189;

Bumiller, E y Shanker, T. (2012) *Panetta Warns of Dire Threat of Cyberattack on U.S.*, N.Y. Times Journal, 12 October 2012.

Burgorgue-Larsen, L. (2012) *La convention européenne des droits de l'homme*, Editorial LGDJ Paris.

Burgueño P. F. (2012) *Aspectos jurídicos de la identidad digital y la reputación online*, adComunica. Revista de Estrategias, Tendencias e Innovación en Comunicación, 2012, nº3, p. 127.

Bustamente Donas, J. (2001) *Hacia la cuarta generación de Derechos Humanos: repensando la condición humana en la sociedad tecnológica*, CTS+I: Revista Iberoamericana de Ciencia, Tecnología, Sociedad e Innovación, Nº.1/2001.

Caro Bejarano, M. J. (2012) *Ciberdefensa. Equipos de respuesta inmediata de la OTAN. Ministerio de Defensa*, Instituto Español de Estudios Estratégicos.

Carrillo Salcedo, J. A. (1991) *Protección de derechos humanos en el Consejo de Europa: hacia la superación de la dualidad entre derechos civiles y políticos y derechos económicos y sociales*, Revista de Instituciones Europeas, Vol. 18, Nº 2, págs. 431-454;

Carrillo, M. (1993). *La cláusula de conciencia y el secreto profesional de los periodistas*. Cuadernos Civitas, Editorial Civitas Madrid.

Cassin, R. (1951) *La déclaration universelle et la mise en œuvre des droits de l'homme*, Paris, Librairie du Recueil Sirey.

Charles-Louis de Secondat Baron de La Brède et de Montesquieu (1964) *El Espiritu de las Leyes*, Vol. I, Editorial Científica, Bucarest, 1964.

Charpentier, J. (1997) *Le fondement du pouvoir des organisations internationales*, en Mélanges offerts à G. Burdeau: Le Pouvoir, Paris, éd. LGDJ, 1997, pp. 999-1011.

Chinchilla Sandí, C. (2005) *Personalidad virtual: necesidad de una reforma constitucional*. Revista de Derecho Informático, no. 82/2005.

Choi, J., Kaplan, J., Krishnamurthy, C. y Lung, H. (2017) *Hit or myth? Understanding the true costs and impact of cybersecurity programs*. Editorial McKinsey Digital.

Christakis T. (2007) *Nécessité n'a pas de Loi' ? Rapport introductif sur la nécessité en droit international* en T. Christakis y K. Bannelier (eds), La nécessité en droit international, Colloque de la Société française pour le droit international, Editorial Pedone, Paris, p. 9- 62.

Christakis, T. (2007) *Les circonstances excluant l'illicéité : une illusion optique ? en Droit du pouvoir, pouvoir du droit*, en Mélanges offerts à Jean Salmon, Bruxelles, Editorial Bruylant, p. 201-248.

Christakis, T. y Bannelier, K. (2009) *La légitime défense a-t-elle sa place dans un code relatif à la responsabilité des Etats?*, en Constantinides (A.), Zaïkos (N.), (ed.), The Diversity of International Law, Essays in Honour of Professor Kalliopi Koufa, Institute of International Public Law and International Relations of Thessaloniki, Martinus Nijhoff, The Hague, pp. 519-533.

Chueca Sancho, A. G. (1989) *Los derechos fundamentales en la Comunidad Europea*, Editorial Bosch, Barcelona.

Clarke, R. A. y Knake, R. (2010) *Cyber War: The Next Threat to National Security and What to Do about It*. Editorial Harper Collins.

Clem, R. (2018) *Clearing the Fog of War: public versus official sources and geopolitical storylines in the Russia-Ukraine conflict*, Eurasian Geography and Economics Journal, no. 58, pp. 1-21.

Colin, A.; Capitant, H. y Morandière, J. (1940) *Curso de Derecho Civil*, traducción por V. G. Falls, I. Miloaie, volumen I, 7ª edición, Bucarest, Central Printing.

Cooley, TH. M. (1880) *A Treatise on the Law of Torts or the Wrongs Which Arise Independently of Contract*, Editorial Callaghan Chicago.

Corten, O. (2010) *The Law Against War: The Prohibition on the use of Force in Contemporary International Law*, Editorial Hart Publishing.

Craig, P. y de Búrca, G. (2011) *EU Law: Text, Cases, and Materials*, Editorial OUP Oxford; 5 edicion;

Crawford Lichtenstein, C. (2001) *Hard Law v. Soft Law: Unnecessary Dichotomy?*. The International Lawyer Vol. 35, No. 4 (Winter 2001), pp. 1433-1441.

Daniel J. Solove (2002) *Conceptualizing Privacy*, California Law Review, Vol. 90, p. 1096.

Danileț, C. (2013) *Insulta y calumnia siguen siendo infracciones*. Revista Juridice.ro, Recuperado de https://www.juridice.ro/257671/insulta-si-calomnia-sunt-din-nou-infractiuni.html.

David Lyons, D. (2001) *Surveillance Society: Monitoring Everyday Life*, Editorial Buckingham, UK: Open University Press.

Deaconu, S. (2011) *Drepturile şi libertăţile fundamentale în sistemul constituţional românesc (Derechos y libertades fundamentales en el sistema constitucional rumano)*, artículo publicado en "Revista rumana de derecho privado", núm. 4/2011.

Deeks, A. (2014) *An International Legal Framework for Surveillance*. Public Law and Legal Theory Research Paper Series 2014-53, vol. 52:2, pp. 292-368.

Deibert R. (2012) *The Growing Dark Side of Cyberspace (. . . and What To Do About It)*. Penn State Journal of Law & International Affairs, vol. I, Issue 2.

Deibert, R. y Rohozinski, R. (2012) *Contesting Cyberspace and the Coming Crisis of Authority*, recuperado de: https://citizenlab.ca/cybernorms2012/DeibertRohozinski2011.pdf.

Deibert, R; Palfrey, J.; Rohozinski, R. y Zittrain, J. (2010) *Access Controlled. The Shaping of Power, Rights, and Rule in Cyberspace*. Editorial The MIT Press.

Delaume, G. R. (1971) *Excuse for non-performance and force majeure in economic development agreements*. Columbia Journal of Transnational Law, Nueva York, vol. 10, N.° 2.

Den Dekker, G. (2001) *The Law of Arms Control: International Supervision and Enforcement*, Editorial Martinus Nijhoff Publishers.

Deudney, D. H. (2007) *Bounding Power: Republican Security Theory from the Polis to the Global Village*, Editorial Princeton University Press.

Díaz Revorio, F. J. (2006) *El derecho fundamental al secreto de las comunicaciones*, Derecho PUCP: Revista de la Facultad de Derecho, no. 59, pp. 159-175.

Díez-Picazo, L. M. (2003) *Sistema de Derechos fundamentales*, Editorial Civitas Madrid;

Dinstein, Y. (2011) *War, Agression and Self Defence*, Fifth, Editorial: Cambridge University Press.

Domínguez Bascoy, J. (2014) *La ciberseguridad: aspectos jurídicos internacionales*. Cursos de derecho internacional y relaciones internacionales de Vitoria-Gasteiz = Vitoria-Gasteizko nazioarteko zuzenbide eta nazioarteko herremanen ikastaroak, N.º. 1, 2015, pp. 161-224.

Draganu, T. (1992) *Introducere în teoria şi practica statului de drept (Introducción en la teoría y la práctica del estado de derecho)*, Editorial Dacia Publishing House, Cluj-Napoca.

Draghici, S. (2009) *Derechos fundamentales entre la definición y los efectos legales*, en "The New Journal of Human Rights", no. 1/2009.

Dreyer, E. (2006) *Du caractère fondamental de certains droits*, en "Revue de la Recherche Juridique, Droit Prospectif", nr. 113/2006.

Duculescu, V. (1994) *Protecţia juridică a drepturilor omului (Protección jurídica de los derechos humanos)*, Lumina Lex Publishing House, Bucarest.

Duguit, L. (2003) *L´Etat, le droit objectif et la loi positive*. Réimpression de l'édition de 1901 (Études de droit public I), Editorial Dalloz Paris.

Dumitru, H. D. (2012) *La libertad de expresión y la vida privada. Conexiones constitucionales y civiles*. Revista Pandectele Romane, nr. 5/2012.

Dupuy, P.-M. (1989) *The International Law of State Responsibility: Revolution or Evolution?,* Michigan Journal of International Law Vol.11./Issue 1, pp. 105-128.

Dupuy, P-M y Kerbrat, Y. (2014) *Droit international public*, Editorial Dalloz, Paris,12eme édition.

Eckhold-Schmdt, F. (1974) *Legitimation durch Begründung.* Editorial Dissertation Berlín.

Egan, B. J. (2017) *International Law and Stability in Cyberspace*, 35 Berkeley J. Int'l Law. 169/2017.

Espinosa de los Monteros, R. Z. (2014) *El impacto de la prueba de ADN en los derechos fundamentales* (1), Diario La Ley, ISSN 1989-6913, Nº 8283.

Etzioni, A. (2007) *Security First: For a Muscular, Moral Foreign Policy.* Editorial New Haven: Yale University Press.

Eudes, M. (2006) *De la Commission au Conseil des droits de l'homme : vraie réforme ou faux-semblant ?* en Annuaire français de droit international, volume 52, 2006. pp. 599-616.

Evans, E. (2004) *Derechos Constitucionales*. Tomo I. Editorial Jurídica. Santiago.

Farwell, J.P. y Rohozinski, R. (2011) *Stuxnet and the Future of Cyber War*, Survival, Global Politics and Strategy Review, vol. 53, issue 1, pp. 23-40.

Fastenrath, U. (1993) *Relative Normativity in International Law,* European Journal of International Law, Volume 4, Issue 3, 1993, pp. 305–340.

Favoreu, L. (1990) *L'élargissement de la saisine du Conseil constitutionnel aux jurisdictions administratives et judiciaires*, RFDC N°4/1990, pp. 581 y siguientes.

Favoreu, L. y otros (2008) *Droit constitutionnel*, 11e édition, Editorial Dalloz, Paris.

Fernández, E. (1991) *Teoría de la justicia y derechos humanos*, Editorial Debate, Madrid.

Ferrajoli, L. (2010) Derechos y garantías. La ley del más débil, Editorial Ariel Barcelona.

Fidler, M. (2015) *Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis*, I/S: A Journal of Law and Policy for the Information Society, Vol. 11, No. 2/2015, pp. 405-482.

Finnemore, M. y Sikkink, K. (1998) *International Norm Dynamics and Political Change*. The Review of International Organization 52.4, pp. 894-905.

Fonseca, C. E., Perdomo, I. L., Arozarena Gratacos, L. M., Ulises Ortiz, J. (2014) *El Manual de Tallin y la Aplicabilidad del Derecho Internacional a la Ciberguerra*, Revista de la ESG no.588-143.

Frank La Rue (2011) *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión*, Asamblea General de las naciones Unidas, 16 de Mayo 2011 New York.

Franzen, C. (2013) *US national security advisor warns China: 'We will take action... against cyber threats*. Recuperado de: https://www.theverge.com/2013/3/11/4091112/white-house-advisor-tom-donilon-warns-china-cyber-attacks.

Freih, L. (2005) *Les droits de l'homme seront mieux défendus sans leur Commission* en Le Temps, 7 avril 2005 (http://hrw.org/)

Freixes Sanjuán, T. (2005) *Derechos fundamentales en la Unión Europea. Evolución y prospectiva: la construcción de un espacio jurídico europeo de los derechos fundamentales*, Revista de derecho constitucional europeo Nº. 4/2005, pp. 43-86,

Froomkin, A. M. (2000) *The Death of Privacy?* Standford Law Review 52/5, recuperado de: https://cyber.harvard.edu/privacy/Fromkin_DeathOfPrivacy.pdf

Frosio, G. (2017) *Right to Be Forgotten: Much Ado About Nothing* , Colorado Technology Law Journal 307/2017.

Galtung, J. (1969) *Violence, Peace, and Peace*; Journal of Peace Research, Vol. 6, No. 3, pp. 167-191.

García Amado, J. A. (2000) *Los derechos fundamentales y las enseñanzas de la historia: Breve comentario al volumen 1 de la historia de los derechos fundamentales, titulado Tránsito a la modernidad. Siglos XVI y XVII*, en Derechos Y Libertades: Revista Del Instituto Bartolomé De Las Casas, Año 5, N. 8 (en.-jun. 2000).

García Moriyon, F. (1983) *Enseñar los derechos humanos*. Editorial: Zero Madrid.;

Garcia T. (2017) *Les entreprises militaires et de sécurité privées appréhendées par le droit*. Editorial: Mare & Martin.

Garrós Font , I. (2019) *Avances y retos de la Agencia Europea para la Ciberseguridad*. El nuevo marco de la certificación. E.M. no. 62 mayo-agosto 2019.

Gavison, R. E. (1980) *Privacy and the Limits of Law*, The Yale Law Journal, Vol. 89, No. 3, pp. 421-471.

Gearty, C. A. (ed.) (1997) *European civil liberties and the European Convention on Human Rights,* Editorial Nijhoff, La Haya-Boston-Londres;

Geers, K. (2011). *Strategic Cyber Security*. Publicación del NATO Cooperative Cyber Defence Centre of Excellence (CCD COE).

Gerety, T. (1977) *Redefining Privacy, Harvard Civil Rights-Civil Liberties Law Review*, Vol. 12, Pages:233-296.

Gervais, M. (2012) *Cyber Attacks and the Laws of War*, Berkeley Journal of International Law, 30/2/2012.

Girard, P. F. (1924) *Manuel élementaire de Droit Romain*, Librairie Arthur Rousseau, Paris.

Glenny, M. (2011) *DarkMarket: Cyberthieves, Cybercops and You*. Editorial Knopf; Canadian First edition.

Gómez Bengoechea, B. (2007) *Derecho a la identidad y filiación: Búsqueda de orígenes en adopción internacional y en otros supuestos de filiación transfronteriza*, Editorial Dykinson, Madrid.

Gómez Montoro, Á. (2001) *Titularidad de derechos fundamentales* en Manuel Aragon Reyes (coord.), Temas de Derecho Constitucional, t. III (Tribunal Constitucional y derechos fundamentales, Editorial Cívitas, Madrid, pp. 116 ss.

Gómez, A. (2012) *El ciberespacio como escenario de conflicto*. *Identificación de las amenazas en el ciberespacio. Nuevo escenario de confrontación*, Madrid, Ed. Ministerio de Defensa.

Hauser, R. (1970) *United Nations Law on Racial Discrimination*, American Journal of International Law, n° 64/1970.

Heathcote, S. (2005) *State of Necessity and International Law*, Thesis No. 772, University of Geneva.

Hilling, C. (1991) *Le système interaméricain de protection des droits de l'Homme: le modèle européen adapté aux réalités latino-américaines*, Revue Québécoise de droit international, vol. 7-2/1991, pp. 210-217.

Hitoshi, N. (2013) *The Place of Human Security in Collective Security*, Journal of Conflict and Security Law 18, no.1.

Holland, M. (1995) *El fin del estado nacional: las relaciones institucionales de la Unión Europea*, Revista de Ciencias Políticas Polis No. 3/1995, p. 22-46.

Hollis, D. B. (2014) *Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?,* en Cyberwar: Law & Ethics for Virtual Conflicts, Temple University Beasly School of Law Legal Studies Research Paper nº 2014-16.

Hume, D. (1995) *Sobre el suicidio y otros ensayos*. Alianza Editorial. Madrid.

Hurtaud, S. (2014) *Cyber security. Time for a new paradigm*. Information & Technology Risk. Editorial Deloitte.

Igareda Gónzalez, N. (2014) *El derecho a conocer los orígenes biológicos versus el anonimato en la donación de gametos*, Revista Derechos y Libertades, núm. 31/2014, pp. 227 a 249.

Innerarity, D. (2013) *Un mundo de todos y de nadie. Piratas, riesgos y redes en el nuevo desorden global*. Editorial Espasa Libros Barcelona.

Inness, J. C. (1992) *Privacy, Intimacy, and Isolation*; Oxford University Press.

James, J. (2006) *Digital Divide Complacency: Misconceptions and Dangers*, The Information Society International Journal, Vol. 24, pp. 54-61.

Jarufe Contreras, D (2013) *Tratamiento legal de las filiaciones no biológicas en el ordenamiento jurídico español: adopción "versus" técnicas de reproducción asistida*, Editorial Dykinson, Madrid.

Jellinek, G. (2005) *L'Etat moderne et son droit: Tome 2*, Théorie juridique de l'Etat, Editorial Pantheon-Assas París.

Jensen, E. T. (2010) *Cyber Warfare and Precautions against the Effects of Attacks*, Texas Law Review 88.7, pp. 1533–1569.

Joyner, C. C. y Lotrionte, C. (2001) *Information Warfare as International Coercion: Elements of a Legal Framework*, EJIL, vol 12, no. 5, pp. 825-865.

Jugastru, C. (2007) *Reflexiones sobre la noción y la evolución de los derechos de la personalidad*, Instituto de Historia "George Bariţiu" de Cluj-Napoca, Serie Humanistica, tomo V, p 326.

Julio Estrada, A. (2000) *La eficacia de los derechos fundamentales entre particulares*, Universidad Externado de Colombia.

Kamwanga, K. D. (2005) *Les mécanismes internationaux de protection et l'effectivité des droits de l'homme*, Mémoire de DEA, Université D'ABOMEY-CALAVI (Bénin).

Kant, I. (1873) *Principios Metafísicos del Derecho*, Editorial Kessinger Publishing.

Kanuck, S. (2010) *Sovereign Discourse on Cyber Conflict Under International Law*. Texas Law Review, vol. 88, pp. 1571 y ss.

Katyal, N. (2005) *Community Self-Help, Journal of Law*, Economics and Policy, Vol. 1, p. 60.

King, G. (2014) *EU 'Right to be Forgotten' Ruling Will Corrupt History*. Recuperado de: https://cpj.org/2014/06/eu-right-to-be-forgotten-ruling-will-corrupt-histo/.

Kris, D. (2013) *Thoughts on a Blue-Sky Overhaul of Surveillance Laws: Approach*. Lawfare. Recuperado de: https://www.lawfareblog.com/thoughts-blue-sky-overhaul-surveillance-laws-approach

Kulesza J. (2012) *International Internet law,* Revista: Global Change, Peace & Security 24(3), pp. 351 – 364.

Kulesza, J. (2014) *Protecting Human Rights Online - An Obligation of Due Diligence*, Jean Monnet Working Paper 24/14.

Kurbalija, J y Gelbstein, E. (2005) *Gobernanza de Internet: Asuntos, Actores y Brechas*. Editorial DiploFoundation y la Sociedad para el Conocimiento Mundial.

Lebreton, G. (2008) *Libertés publiques et droits de l'homme*, Editorial Sirey.

Lefebvre, N. (2015), *Les services de renseignement européens face au terrorisme : coopération ou cloisonnement*, Presses Académiques Francophones, Saarbrücken.

Legrand, P. (2001) *Derecho Comparado*, Editorial Lumina Lex Bucharest, p. 80.

Levin, L. (2009) *Human Rights*. *Questions and Answers*. Editorial: UNESCO Publishing.

Llanos Mansilla, H. (1976) *El derecho humanitario y su aplicación en caso de conflictos armados de carácter interno*. Revista Chilena de Derecho vol. III. pp. 37-48.

Llorens, M. P. (2017). *Los desafíos del uso de la fuerza en el ciberespacio*. Anuario mexicano de derecho internacional, 17, 785-816.

Locke, J. (2012) *Segundo Tratado sobre el Gobierno Civil. Un ensayo acerca del verdadero origen, alcance y fin del Gobierno Civil*, Editorial Alianza Madrid.

Loisel, A. (2013) *Institutes coustumières, ou Manuel de plusieurs et diverses reigles: sentences & proverbes tant anciens que modernes du droict coustumier & plus ordinaire de la France*, Editorial Hachette Livre BNF.

López Acuña, C. R. (2016) *La evolución de la libertad de expresión y el derecho a la información en la España constitucional.* Relevancia de la jurisprudencia en la profesión periodística, Tesis doctoral, Universidad Complutense de Madrid, Facultad de Ciencias de la Información, recuperado de: http://eprints.ucm.es/42082/1/T38627.pdf.

Lotrionte, C. (2012) *Cyber Operations: Conflict Under International Law.* Georgetown Journal of International Affairs, pp. 15-24.

Lotrionte, C. (2012) *State Sovereignty and Self-defense in Cyberspace: A Normative Framework for Balancing Legal Rights*, Emory International Law Review 26/2012, pp. 825–919;

Maqueo Ramírez, M. S., Moreno González, J. y Recio Gayo, M. (2017) *Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario*. Revista de derecho (Valdivia), 30(1), 77-96.

Margulies, P. (2014) *The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism*, Fordham Law Review vol.82, issue 5.

Maritain, J. (1991) *Acerca de la filosofía de los derechos del hombre*, Editorial Debate, Madrid.

Martínez Martínez, R. (2016) *Directiva de ciberseguridad: un nuevo escenario jurídico y material*. Revista SIC: ciberseguridad, seguridad de la información y privacidad, Vol. 25, Nr. 121, p. 98-100.

Matefi, R. (2019) *El derecho al honor en el contexto legislativo nacional e internacional y en la jurisprudencia correspondiente (Dreptul persoanei la reputaţie, în contextul reglementărilor legale naţionale şi internaţionale şi a jurisprudenţei în materie)*, Revista Universul Juridic no.3, pp. 57-63.

Maurer, T. (2011) *Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security?*, Discussion Paper 2011-11, Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School.

Maurize, M. -O. (1992) *Au delà de l'Etat. Le droit international et la défense des droits de l'homme*, Paris, Amnesty International.

McDougal, M. S. (1954) *International Law, Power and Policy: A Contemporary Conception*, Recueil des cours, Vol 82.

Melin-Soucramanien, F. (2009) *Les constitutions de la France de la Revolution a la IVe Republique*, Editorial Dalloz, Paris.

Melkevik, B. (1997) *ISSE OMANGA BOKATOLA, L'Organisation des Nations Unies et la protection des minorités*. Les Cahiers de droit, 38 (1), 238–239., Editorial Bruylant, Bruxelles.

Messerschmidt, J. (2013), *Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm*, Columbia Journal of Transnational Law, 52(1).

Mihai G. (2005) *Fundamentele Dreptului (Fundamentos del Derecho)*, Editorial All Beck, Bucharest.

Milanovic, M. (2015) *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age.* Harvard International Law Journal 56 (1).

Miquel, P. A. (2008) *Respect et inviolabilité du corps humain*, Revista Noesis. Recuperado de : http://journals.openedition.org/noesis/1383

Monnet, J. (1978) *Memoirs*. Editorial Doubleday & Company, INC. Garden City, New York.

Montero, A. (2018) *Hack-back: ¿legítima ciberdefensa en empresas?*. Real Instituto Elcano.

Moore, A. D. (2010) *Privacy Rights: Moral and Legal Foundations*, Editorial University Park, PA: Penn State University Press.

Moore, A. D. (2011) *Privacy, security, and government surveillance: Wikileaks and the new accountability*. Public Affairs Quarterly Volume 25. no 2/2011. pp.162-188.

Moore, J. B. (1898) *History and digest of the international arbitrations to which the United States has been a party*, Washington: Gov't Print Off.

Morello, A. M. (1994) *El proceso justo. Del garantismo formal a la tutela judicial efectiva de los derechos*, Editorial Platense/Abeledo-Perrot, La Plata.

Mueller, M. L. (2010) *Networks and States: The Global Politics of Internet Governance*. Editorial Cambridge MIT Press.

Muraru I. (1995) *Reflectarea drepturilor omului în noua Constituţie a României (Reflexión de los derechos humanos en la nueva Constitución de Rumania)*, en I. Muraru, M. Constantinescu, Studii constitutionale (Estudios constitucionales), Editorial Actami, Bucarest.

Muraru, I. y Tanasescu, E.S. (2001) *Drept Constitutional si institutii politice (Derecho Constitucional e Instituciones Políticas)*, Volumen I, Edición 14, Editorial C.H. Beck, Bucarest.

Naranjo de la Cruz, R. (2000) *Los límites de los derechos fundamentales en las relaciones particulares: la buena fe*, Centro de Estudios Políticos y Constitucionales.

National Research Council (2010) *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, National Academies Press, Washington, DC.

Nipperdey, H. C. (1962) *Freie Entfaltung der Persönlichkeit* en Bettermann, H. C. et al., Die Grundrechte. Handbuch der Theorie und Praxis der Grundrechte, Berlín, Duncker & Humblot, t. IV.

O'Reilly, D. (2007). *Five ways to protect your privacy online*, disponible en: https://www.cnet.com/news/five-ways-to-protect-your-privacy-online/.

Ossenbühl, F. (2000) *Staatshaftungsrecht (Ley de responsabilidad del estado)*, Editorial C.H.Beck; Auflage.

Oumba, P. (2008) *La prise en compte de la règle de droit humanitaire dans la jurisprudence de la Cour internationale de justice*. Revue Aspects, 2008, pp.69-83.

Oumba, P. (2009) *La Cour internationale de justice et la problématique des droits de l'homme*. Humanité et liberté en Afrique centrale, 2009, Tome 1, pp.147-162.

Palfrey, J. y Gasser, U. (2008) *Born Digital: Understanding the First Generation of Digital Natives*. Editorial New York: Basic Books.

Pardo Iranzo, V. y Pascual Serrats, R. (2011) *Acceso a la Justicia de los más desfavorecidos y Unión Europea*, Revista Boliviana de Derecho, núm. 12/2011, pp. 172-202, Fundación Iuris Tantum, Santa Cruz, Bolivia.

Partsch, K. J. (1978) *Les principes de base des droits de l'homme : l'autodétermination, l'égalité et la non-discrimination* en "Les dimensions internationales des droits de l'homme", Paris, UNESCO.

Peces-Barba Martínez, G. (1976) *Derechos fundamentales*. Madrid: Guadiana de publicaciones, D.L.

Peces-Barba Martínez, G. (1993) *Derecho y derechos fundamentales*. Madrid: Centro de Estudios Constitucionales.

Peces-Barba Martínez, G. (1993) *El derecho y el amor: sus modelos de relación* en Derecho y derechos fundamentales, Centro de Estudios Constitucionales, Madrid.

Peces-Barba Martínez, G. (1995) *Curso de derechos fundamentales: teoría general*. Madrid: Universidad Carlos III de Madrid: Boletín Oficial del Estado.

Peces-Barba Martínez, G. (1999) *Derechos sociales y positivismo jurídico: (escritos de filosofía jurídica y política)*. Madrid: Dykinson: Instituto de Derechos Humanos Bartolomé de las Casas, Universidad Carlos III.

Peces-Barba Martínez, G. (2002) *La dignidad de la persona desde la filosofía del derecho*. Madrid: Dykinson.

Pepitone, J. (2013) *Cybersecurity lobbying doubled in 2012*. CNN Money (New York). The Cybercrime Economy.

Pérez Luño, A. E (1991) *Las generaciones de derechos fundamentales*, Revista del Centro de Estudios Constitucionales, Nº. 10, 1991, pp. 203-217;

Pérez Luño, A. E. (1991) *Estado constitucional y derechos de la tercera generación*, Anuario de Filosofía del Derecho, Tomos XIII-XIV, pp. 513.

Pérez Luño, A. E. (2011) *Internet y los derechos humanos*, Anuario de Derechos Humanos. Nueva Época. Vol. 12. 2011 (287-330).

Pérez-Luño, A. E. (2007) *Los derechos fundamentales*, Editorial Tecnos Madrid.

Perlroth, N. (2013) *Researchers Find 25 Countries Using Surveillance Software*, The New York Time Journal.

Pernice, I. (2009) *The Treaty of Lisbon: Multilevel Constitutionalism in Action* en The Columbia, Journal of European Law, Vol. 15, no. 3/2009.

Pezzimenti, R. (2001) *The Political Thought of Lord Acton: The English Catholics in the Nineteenth Century*, Editorial Millennium Romae 2000 AD.MM.

Piñar Mañas, J. L. (2010) *¿Existe privacidad?* en Protección de Datos Personales, Compendio de lecturas y legislación, Editorial Tiro Corto, México.

Pisillo-Mazzeschi, R. (1992) *The "Due Diligence" Rule and the Nature of the International Responsibility of States*, 35 German Yearbook of International Law 9 (1992), pp. 9 – 49

Popa, N. (1994) *Teoria generală a dreptului. (La Teoría General del Derecho)*; Editorial Actami Publishing, Bucarest.

Post, R. C. (2001) Three Concepts of Privacy, The Georgetown Law Journal, vol 89/2087, pag 2087 y ss.

Potter, E. H. (2002) *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century*. Editorial: McGill-Queen's University Press.

Poulain, J. ; Sandkuhler, H. J. y Triki, F. (2009) *La dignité humaine: Perspectives transculturelles (Philosophie und Transkulturalität / Philosophie et transculturalité)* (French Edition), Editorial Peter Lang GmbH, Internationaler Verlag der Wissenschaften.

Powell, R. (2012) *The Concept of Security*, University of Oxford Socio-Legal Review, no.1.

Prieto Sanchís, L. (1990) *Estudios sobre derechos fundamentales*, Editorial Debate, Madrid.

Prosser, W.S (1960) *Privacy*. California Law Review, vol.48, no.3.

Provost, R. (1992) *State Responsibility in International Law*, Londres: Editorial Routledge.

Renucci, J.-F. (2009) *Tratado de derecho europeo de derechos humanos*, Hamangiu Publishing House, Bucarest.

Riofrío Martínez-Villalba, J. C. (2014) *La cuarta ola de derechos humanos: los derechos digitales*, Revista Latinoamericana de Derechos Humanos Volumen 25 (1), I Semestre 2014.

Rivera, J. C. (2004) *Instituciones de derecho civil*, Editorial Abeledo Perrot Buenos Aires.

Roberto Ago (1978) *El hecho internacionalmente ilícito del Estado como fuente de responsabilidad internacional*, A/CN.4/307 Y ADD. 1 y 2. Séptimo informe sobre la responsabilidad de los Estados, Anuario de la Comisión de Derecho Internacional, vol. II.

Robinson, N. (2014) *EU cyber-defence: a work in progress*. European Union. Institute for Security Studies.

Roche, J. (1981) *Libertes publiques*, Editorial Dalloz, 6a ed. Paris.

Rodríguez Palop, M. E. (2010) *La nueva generación de derechos humanos. Origen y justificación*, Editorial Dykinson, Madrid;

Rodríguez Uribes, J. M. (1999) *Opinión pública. Concepto y modelos históricos*. Editorial Marcial Pons, Madrid.

Rodriguez Uribes, J. M. (2015) *Gregorio Peces-Barba – Justicia Y Derecho*. Editorial Aranzadi.

Romboli, R. (2018) *La influencia del C.E.D.H. y de la jurisprudencia del T.E.D.H. en el ordenamiento constitucional italiano*. Revista Teoría y Realidad Constitucional, núm. 42/2018, pp. 187-220.

Roscini, M. (2014) *Cyber Operations as a Use of Force* en Nicholas Tsagourias and Russell Buchan (eds.), Research Handbook on International Law and Cyberspace, Edward Elgar Publishing, 2015, 233-254, U. of Westminster School of Law Research Paper No. 16-05.

Rothkopf, D. (2015) *Is Unrestricted Internet Access a Modern Human Right?*, recuperado de: https://foreignpolicy.com/2015/02/02/unrestricted-internet-access-human-rights-technology-constitution/

Rousseau, J. J. (1996) *El contrato social*, libro II, cap. I, Edit. Alba, Madrid.

Rousseau, J. J. (2005) *Discurso sobre economía política*, Editorial Tecnos Madrid.

Ruiz-Jarabo, D. y Correa Guimerá, B. (1999) *La protección de los derechos humanos por el Tribunal de Justicia de las Comunidades Europeas* en A. MARZAL (ed.) Derechos humanos del migrante, de la mujer en el Islam, de injerencia internacional y complejidad del sujeto, Editorial Bosch, Barcelona, pp. 137 - 138.

Rusen, E. (2014) *Protection européenne et internationale des droits de l'homme*, Tercera Edicion, Editorial Larcier.

Salazar, S. (2013) *Fundamentación y estructura de los derechos sociales*, en Revista de Derecho (Valdivia), Vol. 26, Nº 1, pp. 69-93.

Salinas Alcega, S. (2001) *Desarrollos recientes en la protección de los derechos humanos en Europa. Nuevos elementos en una vieja controversia: la adhesión de las Comunidades*

europeas a la Convención europea de salvaguarda de los derechos humanos y las libertades fundamentales, en Noticias de la Unión Europea, núm. 199/2/2001;

Salmon, J. (1984) *Faut-il codifier l'état de nécessité en droit international?, Essays in international law in honour of Judge Manfred Lachs*, Études de droit international en l'honneur du juge Manfred Lachs, Martinus Nijhoff, The Hague (Boston), pp. 251-254.

Salmon, J. (2001) *Dictionnaire de droit international public*. Editorial Bruyant Bruxelles.

Sánchez de Rojas, E. (2010) *La ciberseguridad: retos, riesgos y amenazas*. Revista Ejército, 837: 136-143.

Sandru, D.M. (2019) *Răspunderea administratorului unei pagini găzduite de o rețea socială. Calitatea de operator în sensul reglementărilor privind protecția datelor (La responsabilidad del administrador de una página alojada en una red social. La calidad del operador en el sentido de las normas de protección de datos)*, Revista Dreptul 07: 160-174. 2019.

Sandru, D.M. y Alexe, I. (2018) *Legislatia Uniunii Europene privind protectia datelor personale. (Legislación de la Unión Europea sobre la protección de datos personales)*, Editorial Universitaria Bucarest.

Sandru, D.M.; Banu, C.M. y Calin, D. (2016) *Directiva - act de dreptul Uniunii Europene – si dreptul român*, Editura Universitara, Bucarest.

Sarfaty, G. A. (2013) *Human Rights Meets Securities Regulation*, 54:1 Va J Int'l L 97.

Schmitt, M. N. (2012) *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*. Harvard International Law Journal, vol. 54

Schmitt, M. N. (2013) *Tallinn Manual on the International Law applicable to cyber welfare*. Cambridge University Press.

Schmitt, M.N. y Watts S. (2016) *Beyond State-Centrism: International Law and Non-state Actors in Cyberspace*. Journal of Conflict & Security Law, Vol. 21, No. 3.

Schneider, H. P. (1979) *Peculiaridad y función de los Derechos fundamentales de un Estado constitucional democrático* en Revista de Estudios Políticos, Nº 7 (Nueva época), Madrid.

Schneider, H. P. (1985) *Derechos fundamentales en el Estado constitucional democrático*, Revista de Estudios Políticos, núm. 7.

Schoditsch, T.(2019) *Grundrechte und Privatrecht*, Editorial Verlag Österreich.

Schoeman, F. (1984) *Privacy: Philosophical Dimensions of the Literature, An Anthology*, Editorial Cambridge University Press.

Scott, C. (1989) *Interdependence and Permeability of Human Rights Norms: Towards a Partial Fusion of the International Covenants on Human Rights*, Revista: Osgoode Hall Law Journal 27.3, pp. 769-878.

Segal, A. (2016) *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*, Editorial Public Affairs; 1st Edition.

Selejan-Guţan, B. (2004) *Drept Constitutional si Institutii Politice (Derecho constitucional e instituciones políticas)*, volumen I, Universidad de Sibiu "Lucian Blaga", página 161.

Selejan-Guţan, B. (2005) *Excepţia de neconstituţionalitate (Excepción de la inconstitucionalidad)*, Editorial All Beck, Bucarest.

Shackelford, S. J. (2009) *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*. Berkley Journal of International Law, Vol. 25, No. 3/2009.

Shackelford, S. J. (2017) *Cybersecurity as Social Responsibility: Business, Music, and the Symphony of Cyber Peace*, Indiana Law Journal, Kelley School of Business Research Paper No. 17-69.

Shackelford, S. J. (2017) *Should Cybersecurity Be a Human Right? Exploring the "Shared Responsibility" of Cyber Peace*. Stanford Journal of International Law No. 2019, Kelley School of Business Research Paper No. 17-55.

Shackelford, S.J.; Fort, T.L. y Charoen, D. (2016) *Sustainable Cybersecurity. Applying Lessons From the Green Movement to Managing Cyber Attacks*, University of Illinois Law Review.

Sicilianos, L. A. (1990) *Les réactions décentralisées à l'illicite : Des contremesures à la légitime défense*, Revue internationale de droit comparé no. 4, Paris, p. 950 y ss.

Sivakumaran, S. (2007) *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)*, en The International and Comparative Law Quarterly, Vol. 56, No. 3, pp. 695-708.

Smith, B. (2017) *The Need for Urgent Collective Action to Keep People Safe Online: Lessons from last Week's Cyberattack*, Microsoft Corporation.

Solozábal Echeverría, J.J. (1991*) Algunas cuestiones básicas de la teoría de los derechos fundamentales* en: Revista de Estudios Políticos, Centro de Estudios Constitucionales, Madrid, Nº 71 enero-marzo de1991.

Standage, T. (1998) *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-line Producers*, Editorial New York: Berkeley Books.

Stone, N. (1985) *La Europa transformada, 1878-1919*. Siglo Veintiuno Editores, México.

Stytz, M. R. y Bank, S. B. (2014) *Cyber Warfare Simulation to Prepare to Control Cyber Space*. National Cybersecurity Institute Journal, vol 1, nº2.

Sudre, F., Milano, L., Surrel, H. (2019) *Droit européen et international des droits de l'homme*, Editorial Presses Universitaire de France Paris.

Sverrisson, H. B. (2008) *Countermeasures, the International Legal System, and Environmental Violations*, Editorial Cambria Press.

Tannenwald, N. (2007) *The Nuclear Taboo: The United States and the Nonuse of Nuclear Weapons since 1945*. Cambridge University Press.

Taylor, J. S. (2005) *In Praise of Big Brother*. Public Affairs Quarterly. vol. 19, no. 3/2005, pp. 227–246.

Thompson, K. (2014) *Lockheed Martin Moves to Dominate Cyber Defense of Electric Grid & Energy Complex*, Revista Forbes, 14 March 2014.

Thomson, J. J. (1975) *The Right to Privacy*, Philosophy & Public Affairs, Vol. 4, No. 4 (Summer, 1975), pp. 295-314

Torrecuadrada, S. (2013) *Internet y el uso de la fuerza, en Ciberseguridad global. Oportunidades y compromisos en el uso del ciberespacio*, Ed. Universidad de Granada.

Trevijano Sánchez, P.G. (2018) *El derecho al respeto de la vida privada: los retos digitales, una perspectiva de derecho comparado*, EPRS-Servicio de Estudios del Parlamento Europeo, Unidad

Turkington, R. C. y Allen, A. L. (2002) *Privacy Law: Cases and Materials* (American Casebook Series) 2nd Edition, Editorial West Group.

Ubillos, J. M. (1997) *La eficacia de los derechos fundamentales frente a particulares. Análisis de la jurisprudencia del Tribunal Constitucional*, Centro de Estudios Políticos y Constitucionales, Madrid.

Vallespín Pérez, D. (2002) *El modelo constitucional de juicio justo en el ámbito del proceso civil*, Editorial Atelier Barcelona.

Van Kempen, P. H. (2013) *Four Concepts of Security – A Human Rights Perspective*, Human Rights Law Review 13, no.1.

Vasak, K. (1984) *Las dimensiones internacionales de los derechos humanos*, Vol. III, Editorial Serbal/Unesco Barcelona.

Venegas Grau, M. (2004) *Derechos fundamentales y derecho privado. Los derechos fundamentales en las relaciones entre particulares y el principio de autonomía privada*, Editorial Marcial Pons Madrid.

Villaverde Menéndez, I.; Requejo Rodríguez, P; Aláez Corral, B.; Fernández Sarasola, I; Bastida Freijedo, F.J.; Presno Linera, M.A. (2004) *Teoría general de los derechos fundamentales en la Constitución española de 1978*, Editorial Tecnos, Madrid.

Viney, G. (2002) *Traité de droit civile. Les obligations. La responsabilité : effets*. Editorial Dalloz Paris.

Von Jhering, R. (2011) *El espíritu del Derecho romano en sus diferentes etapas de desarrollo*, Editorial Comares.

Wachmann, P. (1999) Libertés *publiques*, Editorial Dalloz, París.

Warren, S. D. y Brandeis, L. D. (1890) *The Right to Privacy,* Harvard Law Review, vol.5, no. 4.

Wegener, H. (2011) *Cyber Peace. A concept of Cyber Peace en The Quest for Cyber Peace* (cood. Hamadoun I. Touré), disponible en: https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf.

Weiler, J. H. H., (1985) *Il sistema comunitario europeo. Struttura giuridica e processo politico*, Editorial Il Mulino, Bolonia.

Welkowitz, D. S. (2013) *Privatizing Human Rights? Creating Intellectual Property Rights From Human Rights Principles*, Akron Law Journals, Akron Law Review: Vol. 46 : Iss. 3, Article 3.

Whitman, J. Q. (2004) *The Two Western Cultures of Privacy: Dignity versus Liberty* en Faculty Scholarship Series (Yale Law School Legal Scholarship Repository), Paper 649.

Wilhelm Gerber, C. F. (1852) *Über öffentliche Rechte*, Tubingen, Laupp;

William M. Beaney (1966) *The Right to Privacy and American Law*, Revista Law and Contemporary Problems, pp. 253-271.

Wohlstetter, A. (1959) *The Delicate Balance of Terror*, Revista Foreign Affairs 37.1, pp. 211–234;

Wood, M. M.; Pronto, A. y Wood M. (2010) *The International Law Commission 1999-2009: Volume IV: Treaties, Final Draft Articles, and Other Materials*, vol. IV, Editorial OUP Oxford.

Wunder Hachem, D. (2014). *Derechos fundamentales económicos y sociales y la responsabilidad del estado por omisión.* Estudios constitucionales, 12(1), pp. 285-328.

Zetter, K. (2010) *Google Hack Attack Was Ultra Sophisticated*, New Details Show.