UBA FCE
Universidad de Buenos Aires
Facultad de Ciencias Económicas
ENAP Escuela de Negocios y Administración Pública

Universidad de Buenos Aires

Facultad de Ciencias Económicas

Escuela de Negocios y Administración Pública

MAESTRÍA EN CIBERDEFENSA Y CIBERSEGURIDAD

TRABAJO FINAL DE MAESTRÍA

Aportes para la adecuación del marco jurídico de la ciberdefensa y la ciberseguridad en Argentina

AUTOR: NICOLÁS SANTIAGO TATO

DIRECTOR: DR. LUIS MARÍA GONZÁLEZ DAY

SEPTIEMBRE DE 2020

Esta página ha sido dejada en blanco intencionalmente.

i. Resumen

Este trabajo plantea aportes al desarrollo jurídico argentino en el ámbito de la ciberdefensa y la ciberseguridad. Parte de un análisis histórico del acompañamiento jurídico a la evolución tecnológica desde sus incipientes comienzos en el siglo XIX, y analiza la situación jurídica actual en la Comunidad Europea, en los Estados Unidos y en la Argentina. Completa el cuadro, una descripción de los problemas que los conceptos legales tradicionales encuentran en un área altamente intangible. Estos análisis están acompañados de la descripción de los principales eventos relacionados con la ciberdefensa y ciberseguridad y cómo estos eventos han sido en algunos casos disparadores de nuevas legislaciones. En base a estos análisis, este trabajo propone aportes para la legislación en cuatro aspectos esenciales relacionados con la ciberdefensa y la ciberseguridad: soberanía, atribución, ciberarmas e inteligencia artificial.

ii. Abstract

This work proposes contributions to the Argentine legal development in the field of cyber defense and cybersecurity. It starts from a historical analysis of the legal support to technological evolution since its incipient beginnings in the 19th century, and analyzes the current legal situation in the European Community, the United States and Argentina. Completes the picture a description of the problems that traditional legal concepts within the scope in a highly intangible area. These analyzes are accompanied by the description of the main events related to cyber defense and cybersecurity and how these events have in some cases been triggers for new legislation. Based on these analyzes, this work proposes contributions to legislation in four essential aspects related to cyberdefense and cybersecurity: sovereignty, attribution, cyber weapons and artificial intelligence.

Esta página ha sido dejada en blanco intencionalmente.

iii. Dedicatorias

A mi esposa, por su apoyo incondicional. A mis padres, a quienes debo mis virtudes.

iv. Agradecimientos

A mi Director de Tesis, Dr. Luis María González Day, por su invalorable guía y apoyo en la creación de este Trabajo Final de Maestría.

A los directivos de esta Maestría, el Dr. Roberto Uzal y el Ing. Carlos Amaya, sin cuyo esfuerzo de creación y perseverancia en el trabajo durante estos dos años este posgrado no habría sido posible.

A los profesores de la Maestría, especialmente al Ing. Aníbal Intini, la Mg. Adriana Baravalle, el Mg. Daniel Piorun, el Dr. Gabriel Urchipia y el Lic. Christian Borghello.

A mis compañeros de la cohorte 2018 de la Maestría en Ciberdefensa y Ciberseguridad, quienes con su apoyo y amistad hicieron más ameno el arduo camino transitado durante estos dos años.

Esta página ha sido dejada en blanco intencionalmente.

Índice

Introducción

La evolución tecnológica actual tiene como elemento distintivo su carácter exponencial. Esto se evidencia, por ejemplo, en la Ley de Moore, que indica que la cantidad de transistores en un microprocesador se duplica cada dos años. En la década de 1970 había 4.000 transistores por cada microprocesador, ese número se incrementó a 500.000 en la década de 1980, a 10.000.000 en la década de 1990, y a 500.000.000 en la década siguiente. Podemos verificar el mismo proceso en las capacidades de memoria volátil (tradicionalmente conocidas como memorias RAM, siglas en inglés para *Random Access Memory*).

A principios de la década de 1980 las computadoras hogareñas poseían en promedio 4 Kilobytes de memoria, lo que les permitía almacenar 4.192 caracteres. En la década de 1990 el estándar promedio era de 4.096 Kilobytes, denominado también 1 Megabyte, que permitía almacenar 4.194.304 caracteres. Actualmente el promedio de memoria es de 8 Gigabytes, equivalente a 8.000 Megabytes, lo que permite almacenar 8.388.608.000 caracteres.[1]

La modernidad se define en gran medida por las consecuencias de esta velocidad evolutiva, de la cual las personas no son plenamente conscientes por estar inmersas en este mundo cuya vorágine e inmediatez impide prestar atención al largo plazo. Es la compresión del tiempo la que nos acecha como especie.

La mayoría de las personas se sorprende cuando se les recuerda que el IPhone fue creado en el año 2007, y que el primer celular con sistema operativo Android vio la luz en el año 2008. O que antes de 1997 no existía la conexión de Banda Ancha en Argentina, y que en el año 2002 había apenas 200.000 clientes conectados a través de dicho servicio.

La tecnología ha penetrado de manera veloz y profunda en nuestra vida cotidiana y en todos los ámbitos del quehacer humano, desde el comercial y económico hasta el político y cultural. Hoy en día la mayor parte de las actividades humanas pasan por Internet o dependen de Internet para darle soporte a la actividad. Asistimos actualmente al

[1] Evolución de la memoria RAM, disponible en https://sites.google.com/site/lineadetiempomemoriaram/evolucion-de-la-memoria-ram, y en https://www.adslzone.net/2016/11/28/curioso-caso-del-precio-la-memoria-ram-evolucion-tiempo/, consultados el 17 de agosto de 2020.

uso en todo el mundo de dispositivos conectados a Internet para gestionar varios aspectos de la pandemia de COVID-19, como el análisis de la movilidad de las personas[2], el contacto entre personas basados en la cercanía de los dispositivos móviles[3], la gestión y control de permisos de circulación[4], y además se ha ampliado con éxito el teletrabajo y la educación a distancia con alcances impensados 5 meses atrás.

Una de las consecuencias de esta penetración es que Internet se ha convertido en un ámbito en el cual se desarrollan delitos y ataques que, otrora fueron físicos o materiales, y hoy son digitales, pero con el mismo o mayor efecto dañino en el plano económico, social y en algunos casos y como consecuencia directa, físico.

El ataque más conocido en el plano internacional fue el ataque de Denegación de Servicio Distribuido (DDoS, por sus siglas en inglés) que sufrió Estonia (Ottis, 2008) entre el 27 de abril y el 18 de mayo de 2007. Estonia había desarrollado desde 1996 una fuerte política de digitalización de su sociedad. Comenzó por el sector educativo con la interconexión de escuelas y logró desarrollar un ambicioso proyecto denominado X-Road[5] que interconecta bases de datos públicas y privadas, mediante el cual los ciudadanos pueden realizar la mayoría de los trámites ciudadanos de forma digital, desde votar hasta la gestión de recetas médicas. En este entorno altamente digitalizado se produjo el ataque, el cual tenía motivaciones políticas, llevado a cabo mientras en la ciudad había protestas y disturbios por parte de la comunidad rusa en Estonia.

El ataque cibernético incapacitó varias organizaciones y servicios, como el parlamento, bancos, ministerios y sitios de noticias. “Los ataques afectaron a casi toda Estonia paralizando sus actividades políticas y financieras e incrementándose con fuerza en ocasión de la conmemoración de la victoria rusa sobre el ejército alemán el día 9 de mayo” (Pessino, 2017). Pero este ataque, sin bien uno de los más citados, no fue el primero del que se tiene registro. En el año 1982 los Estados Unidos llevaron a cabo una forma de ataqué informático sobre la Unión Soviética. Nos dice Schreier al respecto:

[2] Informe de movilidad local sobre COVID-19, disponible en https://www.google.com/covid19/mobility/, consultado el 22 de agosto de 2020.
[3] Cómo Apple y Google están habilitando el seguimiento de contactos Covid-19 , disponible en https://www.wired.com/story/apple-google-bluetooth-contact-tracing-covid-19/ ,consultado el 22 de agosto de 2020.
[4] Sitio web de la República Argentina para gestionar el certificado de libre circulación , obtenido de https://www.argentina.gob.ar/circular, consultado el 22 de agosto de 2020.
[5] Sitio oficial X-Road, obtenido de https://e-estonia.com/solutions/interoperability-services/x-road/, consultado del 22 de agosto de 2020.

> En 1982, el presidente de Estados Unidos, Reagan, aprobó un plan de la CIA para transferir el software utilizado para hacer funcionar tuberías, turbinas y válvulas a la Unión Soviética. El software, posteriormente robado por los rusos en Canadá, tenía características integradas, una bomba lógica, diseñada para provocar un mal funcionamiento de la velocidad de la bomba y la configuración de la válvula. "El resultado fue la explosión no nuclear más monumental y el fuego jamás visto desde el espacio", señaló el ex Secretario de la Fuerza Aérea de los Estados Unidos y ex Director de la Oficina de Reconocimiento Nacional, Thomas C. Reed, en su libro 'At the Abyss: An Insider's History of the Cold War'. El ataque tuvo un enorme impacto económico y psicológico en la Unión Soviética y se le atribuye la ayuda para poner fin a la Guerra Fría. (Schreier, 2012, pág. 107)

En el año 2007, casi en simultáneo con el ataque a Estonia, la operación “ORCHAD” llevada a cabo por el gobierno de Israel a través de un ataque aéreo destruyó un reactor nuclear en Siria construido con tecnología norcoreana cuya finalidad era procesar plutonio. Si bien las técnicas electrónicas que anularon los radares sirios y permitieron el paso de los aviones israelíes no han sido confirmadas, se especulan dos posibilidades:

> La industria estadounidense y las fuentes militares especularon que los israelíes podrían haber utilizado tecnología similar al sistema de ataque de la red aérea Suter de Estados Unidos para permitir que los aviones pasen sin ser detectados por radar a Siria. Esto permitiría alimentar a los emisores de radar enemigos con objetivos falsos e incluso manipular directamente los sensores enemigos. En mayo de 2008, un informe en la revista IEEE Spectrum (revista editada por el Instituto de Ingenieros Eléctricos y Electrónicos - IEEE por sus siglas en inglés) citó fuentes europeas que alegaban que la red de defensa aérea siria había sido desactivada por un interruptor secreto integrado activado por los israelíes. (Schreier, 2012, pág. 111).

Entre los años 2009 y 2010 un virus del tipo gusano llamado Stuxnet[6] atacó la planta de refinación de uranio en Natanz, Irán. Dicha planta violaba los acuerdos de no proliferación de 1970.

> El daño sufrido por Irán [...] se consideró posteriormente como "sustancial" y se pensó que había retrasado el programa de desarrollo de armas nucleares durante algunos años. Stuxnet es un arma sofisticada. Ataca y desactiva las centrífugas nucleares que funcionan con un sistema denominado Supervisory Control And Data Acquisition (SCADA) del tipo Siemens, anulando el software propietario y sobrecargando las centrífugas. Este último lo hace tan hábilmente, que oculta el daño en progreso de los operadores y supervisores hasta que es demasiado tarde para revertirlo. Se estima que su desarrollo deba haber tomado meses o años, y llevado a cambo con programadores expertos y acceso información y equipos altamente restringidos y clasificados. Un esfuerzo que requirió una inversión en tiempo, recursos y experiencia que sólo de un estado o coalición podría haberlo realizado, y claramente más allá de lo que podría haber llevado a cabo un grupo terrorista o una organización criminal bien financiada (Schreier, 2012, págs. 114-115).

Otro ataque de relevancia con efectos en el plano físico fue el ataque a la red de suministro eléctrico de Ucrania en el año 2015. Dicho ataque es descripto en la Estrategia Nacional de Ciberseguridad del Reino Unido del año 2016:

> Un ciberataque a las empresas de distribución de energía eléctrica de Ucrania occidental, Prykarpattya Oblenergo y Kyiv Oblenergo el 23 de diciembre de 2015 causó un apagón importante, con interrupciones en 50 subestaciones en las redes de distribución. Según se informa en la región experimentaron un apagón de varias horas y muchos otros clientes y áreas sostuvieron perturbaciones menores en su suministro de electricidad, afectando a más de 220.000 consumidores. El ataque se ha atribuido por unos al uso del malware BlackEnergy3 [7], tras la identificación de

[6] Stuxnet es un gusano informático que originalmente tenía como objetivo las instalaciones nucleares de Irán y desde entonces ha mutado y se ha extendido a otras instalaciones industriales y de producción de energía..
[7] BlackEnergy es un troyano que se utiliza, en principio, para realizar ataques DDoS, ciberespionaje y ataques de destrucción de información. La versión 3 citada aquí contaba con complementos relacionados con

> muestras en la red. Al menos seis meses antes del ataque, los agresores habían enviado correos phishing a las oficinas de las empresas de suministro eléctrica en Ucrania, que contenían documentos Microsoft Office maliciosos. Sin embargo, no es muy factible que el malware haya sido culpable de abrir los interruptores que resultaron en el apagón. Es probable que el malware les haya permitido a los atacantes reunir credenciales que les hayan permitido ganar un control directo remoto de algunos aspectos de la red, que subsecuentemente les permitirían causar el apagón (HM Government, 2016, págs. 13-14).

Estos son sólo algunos de los ataques realizados en y a través de Internet. Quedan sin citar decenas de ciberoperaciones como las realizadas en la guerra de Rusia-Georgia en el año 2008 (Dov Bachmann & Gunneriusson, 2015) que incluyó ataques distribuidos de denegación de servicio, *SQL Inyection, cross-site scripting* y *web defacements;* el ataque distribuido de denegación de servicio a Kyrgyzstan en enero 2009; y en julio de ese mismo año el ataque distribuido de denegación de servicio a Corea del Sur y Estados Unidos.

En el plano local de cada país, cientos de casos por año afectan a los estados a partir de acciones de agentes no estatales. Por ejemplo, sólo entre los años 2017 y 2019 numerosos casos de infecciones de ransomware afectaron a las fuerzas de seguridad de los Estados Unidos. Esto perjudicó severamente el curso de investigaciones al afectar pruebas en formato digital (como audios y videos) de las cuales dependían varios casos judiciales, lo que tuvo como consecuencia en algunos de esos casos la liberación de los sospechosos. El sitio Segu-Info, especializado en seguridad informática, recoge en un artículo 7 hechos relevantes (Segu-Info, 2020) que se dieron en los Estados Unidos entre 2017 y 2019:

> Enero de 2017: la policía de Cockrell Hill, Texas, admitió haber perdido ocho años de evidencia tras una infección con el ransomware Osiris.
>
> Mayo de 2018: la policía de Riverside, Ohio, perdió diez meses de casos después de una infección por ransomware. Se re infectó un mes después, pero la segunda vez estaban preparados y no perdieron ningún archivo adicional.

---

sistemas de tipo SCADA relacionados con la industria de la energía. Más información sobre este tema, disponible en https://www.kaspersky.com/resource-center/threats/blackenergy, consultado el 2 de agosto de 2020

Junio de 2018: los funcionarios de Atlanta descubrieron que el departamento de policía de la ciudad perdió casi dos años de evidencia de video de la cámara del tablero de la policía después de un ataque de ransomware en marzo de 2018.

Abril de 2019: una infección de ransomware afectó al departamento de policía de Stuart, Florida, y eliminó archivos que eran parte de evidencia (fotos y videos) en varias investigaciones que se estaban realizando, lo que obligó a los fiscales a dejar caer 11 casos contra presuntos narcotraficantes.

Julio de 2019: la policía de Lawrenceville, Georgia, perdió archivos relacionados con el caso y grabaciones de la cámara corporal tras un incidente de ransomware. No está claro cuántos datos perdió el departamento de policía, ya que hay informes contradictorios que van desde semanas hasta años de evidencia de casos.

Julio de 2019: una infección de ransomware afectó las computadoras portátiles de los autos de la policía para la Patrulla del Estado de Georgia, la Policía del Capitolio de Georgia y la División de Cumplimiento de Autotransportes de Georgia. Las computadoras portátiles y las cámaras del tablero de la policía permanecieron inactivas y no pudieron grabar nuevas pruebas de video durante más de un mes.

Diciembre de 2019: la Oficina del Sheriff del Condado de St. Lucie en Florida perdió una semana de correos electrónicos y pruebas después de una infección de ransomware, incluso si la oficina se restableció de las copias de seguridad.

Hasta el momento estas ciberoperaciones se consideran incidentes aislados. Pero podría tomarse como hipótesis la posibilidad de que hayan sido realizados por individuos alentados por algún Estado, mediante asistencia económica y/o técnica, con el fin de afectar la estabilidad social de los Estados Unidos; lo que constituiría una de las formas de la guerra híbrida[8]. La naturaleza de Internet permite que las acciones de agentes Estatales puedan disfrazarse atomizándolas hasta el punto de aparecer como decenas de acciones de agentes individuales.

[8] Es un tipo de conflicto diferente tanto de la guerra convencional como de la guerra irregular; y que es la resultante del empleo simultáneo de ambas formas de lucha. (Sánchez García, 2012, pág. 11)

Sin perjuicio de ello queda claro que en cualquier caso Internet se ha convertido, sin duda, en un campo de batalla empleado cada vez más por agentes estatales y no estatales, donde sus acciones comparten sin distinción de jerarquías el mundo virtual y hasta llegan a confundirse. Internet configura un ámbito que potencia las virtudes humanas, y también los defectos. Por un lado potencia la solidaridad. Un ejemplo concreto es la distribución a todo el planeta de planos para hacer prótesis 3D a bajo costo. Por otro lado permite al mismo tiempo el tráfico de pornografía infantil sin límites geográficos. Permite educar a niños en lugares remotos y al mismo tiempo permite que un atacante deje sin energía a una ciudad sin salir de su casa.

Aspiro a que el desarrollo de este trabajo final de maestría ponga sobre la mesa la necesidad imperiosa de legislar sobre los aspectos legales de la ciberdefensa y la ciberseguridad de manera abarcativa y como un todo coherente; con el fin de contener, limitar y restringir los aspectos negativos de la evolución tecnológica y al mismo tiempo acompañar adecuadamente los valiosos aspectos positivos que esta cuarta revolución industrial nos ha venido otorgando en las últimas décadas.

Objetivos

Objetivo general:

- Realizar aportes que contribuyan a actualizar y adaptar el sistema legal argentino a la realidad del quinto dominio en materia de seguridad y defensa.

Objetivos específicos:

- Analizar la relación de adecuación del derecho en general a los cambios en las relaciones sociales que el avance tecnológico impone.
- Analizar la adaptación legal de los principales países al V domino en relación a la ciberdefensa y la ciberseguridad.

Metodología

Dada la naturaleza de la hipótesis, el enfoque del trabajo será cualitativo con una lógica de proceso inductiva (Hernández Sampieri, Fernández Collado, & Bpatista Lucio, 2014), desde una perspectiva teórica.

Mediante el análisis cualitativo se compararán las legislaciones de Argentina, Europa, y EEUU, contrastadas con documentos académicos, literatura especializada y los hechos más recientes que impactan en el ámbito del quinto dominio.

Este enfoque cualitativo aborda una concepción múltiple de la realidad, en la cual existen diferentes intencionalidades en las relaciones internas, y donde investigador y objeto se interrelacionan e influyen mutuamente. Este trabajo, en consecuencia, no pretende llegar a abstracciones universales sino que busca elucidar elementos o entidades faltantes en las dinámicas analizadas.

La fuente principal y directa de datos son las situaciones naturales, y el investigador es el principal instrumento de recolección de datos. Este incorpora conocimiento tácito (intuiciones, aprehensiones o sentimientos, como aspectos conocidos de algún modo).

Esta investigación es exploratoria y cualitativa. Ello responde a que, en base a la experiencia del autor y luego de la revisión de antecedentes sobre el problema abordado, se consideró necesario aportar elementos que se considera que son necesarios para los aspectos implicados. Paralelamente, las exploraciones brindan datos que permiten ser clasificados, ordenados e interpretados para descubrir ideas y relaciones nuevas; que además permiten establecer prioridades para estudios futuros.

En esta misma línea, el diseño exploratorio se caracteriza por su posibilidad de construir un camino abierto a diferentes alternativas que pueden ir definiéndose a lo largo del proceso. El presente trabajo se apoya en recursos como fuentes bibliográficas, documentales y datos secundarios.

El método escogido para el desarrollo de la tesis se basa en la recopilación e interpretación de leyes, doctrina, jurisprudencia sobre la materia. La investigación desarrollada no se rige por el principio de representatividad de la muestra, sino que el investigador busca adquirir la idea más completa posible del objeto (Vieytes, 2004).

El tratamiento de estos datos fue realizado mediante un análisis descriptivo-cualitativo. Respecto a la confiabilidad de la información se puede argumentar, siguiendo a Vieytes, que esta ha cumplido con los siguientes criterios: participación prolongada en el campo (el autor es abogado, y desde el año 2003 se ha desempeñado como Full Stack

Developer con conocimientos teóricos y prácticos de ciberseguridad, criptografía y Ethical Hacking en varias empresas, entre ellas Accenture, una de las consultoras informáticas más importantes a nivel global; y entre los años 2016 y 2020 fue Jefe de Informática de la Dirección Nacional de Inteligencia Estratégica Militar en el Ministerio de Defensa; es coautor del libro "Elementos Fundamentales del Derecho Informático" y profesor de Derecho Informático en la carrera de Abogacía en la Universidad del Salvador) y revisión por expertos (el trabajo fue revisado tanto por académicos externos como por el comité experto de evaluación de tesis de la Maestría, quienes aportaron sus opiniones, sugerencias y divergencias con el trabajo).

Hipótesis

Hipótesis principal

El quinto dominio requiere un esquema legal específico con el fin de reducir el riesgo de incertidumbre jurídica ante situaciones no contempladas completa o parcialmente, y/o facilitar acciones preventivas y reactivas eficaces.

Hipótesis secundaria

La legislación argentina actual no provee las herramientas adecuadas para reducir el riesgo ante situaciones no contempladas y facilitar acciones preventivas eficaces de los organismos estatales en el quinto dominio.

Esta página ha sido dejada en blanco intencionalmente.

Capítulo I - Marco teórico

1.1 Terminología

En este trabajo, para referirnos al Internet (también referenciado por otros autores con el término Ciberespacio, Red de redes, etc.) utilizaremos el término quinto dominio por ser el más adecuado a la naturaleza de Internet en relación a los conceptos de defensa y seguridad, por ser el nuevo ámbito de desarrollo. Este concepto es expresado por Richard Clarke y Robert Knake:

> El Pentágono ha identificado durante mucho tiempo cuatro dominios principales de conflicto: tierra, mar, aire y espacio. En los últimos años, el ciberespacio se conoce como el "quinto dominio". A diferencia de los otros, el ciberespacio es artificial. Por lo tanto, puede ser cambiado por el hombre. (Clarke & Knake, 2019, pág. 11)

En relación a las acciones y entidades que se manifiestan en el quinto dominio seguiremos lo establecido por la Real Academia Española, que establece que se debe agregar el prefijo ciber- al término original. Aunque también es de aceptación en algunos casos el agregado de la palabra "electrónico/a" luego del sustantivo. El Diccionario Prehispánico de Dudas publicado en al año 2005 establece que:

> **Ciber:**
> **1.** Elemento compositivo prefijo, creado por acortamiento del adjetivo cibernético, que forma parte de términos relacionados con el mundo de las computadoras u ordenadores y de la realidad virtual: ciberespacio, cibernauta, etc. Se recomienda su uso en la creación de nuevos términos pertenecientes al ámbito de las comunicaciones por Internet, lo que permite sustituir por voces propias numerosos anglicismos que circulan hoy en español. A continuación se ofrecen algunos ejemplos de la gran productividad de este prefijo en nuestros días: «Una de las características del ciberarte es precisamente esa: su intangibilidad» (Mundo [Esp.] 15.12.96); «El cibercafé es un disco-bar que ofrece conexiones públicas a Internet» (Mundo [Esp.] 1.6.97); «El programa más comentado en esto de las cibercharlas es Internet Phone» (Nacional [Ven.] 1.7.96); «Uno de los principales peligros serán los cibercriminales» (Mundo [Esp.] 2.2.97); «Pretendemos tener a nuestro

ciberlector informado en todo momento» (Mundo [Esp.] 10.10.96); «De la muerte de Asturias a la cibernovela» (Hora [Guat.] 3.5.97). Debe evitarse su escritura con la grafía anglicada.

2. En muchos casos, el sentido que aporta este elemento compositivo puede expresarse mediante el adjetivo electrónico pospuesto al sustantivo correspondiente (? electrónico): mensaje electrónico, buzón electrónico, comercio electrónico, etc. (Real Academia Española, 2005)

1.2 El quinto dominio

La importancia del quinto dominio radica en el profundo nivel de penetración económica, social y cultural. Se ha transformado en el ámbito en el cual transcurre gran parte de la vida de las personas, las empresas y los países. En ese sentido, el ex Ministro de Defensa de Argentina, José Horacio Jaunarena afirma que:

> En la actualidad, los adelantos tecnológicos y la creciente infraestructura digital han hecho que poblaciones enteras dependan de sistemas entrelazados y complejos. La demanda de Internet y de conectividad digital exige una integración cada vez mayor de las Tecnologías de la Información y la Comunicación (TIC) en productos que anteriormente funcionaban sin estas tecnologías, por ejemplo, automóviles, edificios e incluso sistemas de control para las redes de distribución eléctrica y de transporte. Prácticamente todos los servicios modernos dependen de la utilización de las TIC. (Jaunarena, Ciberseguridad y Ciberdefensa, 2015, pág. 2)

Estos conceptos se reflejan en la Estrategia Nacional de Ciberseguridad del año 2019, donde dice:

> [...] el ciberespacio se ha constituido en un elemento esencial en la vida de las personas y las organizaciones, las que despliegan allí gran parte de su actividad, no habiendo aspecto de la vida social que no esté alcanzado por este fenómeno.
>
> Que este nuevo paradigma, junto a sus enormes beneficios, implica también graves riesgos a la seguridad de las personas, las organizaciones y los gobiernos, estando el entorno digital amenazado por nuevas formas de delitos, la acción de grupos

> terroristas y la confrontación entre los Estados. (Resolución Nº 829/2019 - Estrategia Nacional de Ciberseguridad, 2019)

En el mismo sentido, la Ciberestrategia Nacional de los Estados Unidos del año 2018 establece que: "El ciberespacio es un componente integral de todas las facetas de la vida estadounidense, incluida nuestra economía y defensa". Luego establece como una de las metas estratégicas: "Promover la prosperidad estadounidense fomentando una economía digital segura y próspera y fomentando una fuerte innovación nacional". (The White House, 2018, pág. 3) y la Publicación el Estado Mayor Conjunto de los EE.UU. con respecto a las ciberoperaciones establece que:

> La relación entre el espacio y el ciberespacio es única, ya que prácticamente todas las operaciones espaciales dependen del ciberespacio, y una parte crítica del ancho de banda del ciberespacio sólo se puede proporcionar a través de operaciones espaciales, que proporcionan una opción clave de conectividad global para las ciberoperaciones. (Joint Chiefs of Staff (CJCS), 2018)

Paralelamente la primer Estrategia Nacional de Ciberseguridad de España, aprobada en 2013, dice:

> El desarrollo de las Tecnologías de Información y Comunicación (TIC) ha generado un nuevo espacio de relación en el que la rapidez y facilidad de los intercambios de información y comunicaciones han eliminado las barreras de distancia y tiempo. El ciberespacio, nombre por el que se designa al dominio global y dinámico compuesto por las infraestructuras de tecnología de la información –incluida Internet–, las redes y los sistemas de información y de telecomunicaciones, han venido a difuminar fronteras, haciendo partícipes a sus usuarios de una globalización sin precedentes que propicia nuevas oportunidades, a la vez que comporta nuevos retos, riesgos y amenazas. (España, Estrategia Nacional de Ciberseguridad, 2013, pág. 9)

En al año 2019 el segundo documento sobre Estrategia Nacional de Ciberseguridad de España ampliará este concepto, al incluir: "La ausencia de soberanía, su débil jurisdicción, la facilidad de acceso y la dificultad de atribución de las acciones que en [el

ciberespacio] se desarrollan definen un escenario que [...] presenta serios desafíos a la seguridad" (España, Estrategia Nacional de Ciberseguridad, 2019, págs. 17-18).

Esto acarrea, en el marco de la defensa nacional, que los conflictos a través del quinto dominio adquieran una relevancia sin precedentes e involucren actores de envergadura como Estados Unidos, Rusia e Irán, como afirman Clarke y Knake: “Mientras escribimos esto en 2019, vemos un patrón de actividad maliciosa en el ciberespacio que sugiere que ya estamos involucrados en un conflicto cibernético de bajo grado y lento con Rusia, China e Irán”. (Clarke & Knake, 2019, pág. 10).

En forma simultánea, la naturaleza del quito dominio lo convierte en un campo de batalla de grandes dimensiones donde puede lograrse anonimato con relativa facilidad, pueden realizarse ataques de bajo costo con altos efectos, donde las amenazas tienen alcance global, y donde conviven ataques de todo tipo de actores, ya sea un ciberdelincuente, un ciberterrorista o un ciberejército[9].

Entre las innumerables consecuencias disruptivas del quinto dominio, tenemos que los conceptos de soberanía, ciudadanía y territorio han sido afectados espacialmente debido a que en el quinto dominio no existe la dimensión del espacio, en la cual dichos conceptos se fundan. No puede hablarse de eventos locales o globales, ni de fronteras, y el concepto distancia no es de aplicación. Como dice Freitas Gómez:

> Sin duda, la revaluación de conceptos como los de soberanía, ciudadanía y territorio no puede dejar a un lado las Nuevas Tecnologías de Información. Los problemas y retos que comienzan a enfrentar los Estados en torno a la legislación sobre el ciberespacio será, una constante en el mediano y largo plazo. Lo que se vive ahora es tan sólo la punta de un iceberg que ha puesto en evidencia la encrucijada en la que Internet ha puesto al Estado, motivado a que, si bien esta tecnología ofrece la posibilidad de una optimización de la democracia e, incluso, de una mejor inserción en el mercado de la globalización, también representa la oportunidad para que los asuntos locales de las naciones se conviertan en globales (Freita Gómez, 2019, pág. 5).

[9] Para ampliar estos conceptos puede verse (Freita Gómez, 2019, pág. 7 y 8).

Si bien en el aspecto puramente físico el quinto dominio existe gracias al crecimiento exponencial (referido oportunamente) de las redes informáticas, que a su vez están constituidas por cables y equipos electrónicos, los cuales están lugares específicos en ciudades y países, en edificios especialmente diseñados para la guarda y el procesamiento de datos, constituyendo redes de información que se interconectan a través de cables de fibra óptica que atraviesan el océano; el quinto dominio es una entidad abstracta que va más allá de su soporte físico. El valor del quinto dominio radica en la información que almacena y transporta, y los servicios que se brindan en él y a través de él. El soporte físico del quinto dominio podrá cambiar[10], pero el mismo, en tanto que entidad, seguirá existiendo. Y esto es así debido a que en las últimas décadas ha aumentado la valoración que se le da a los datos, es decir, a la información. En las palabras de Anzit Guerrero:

> Los avances científicos y tecnológicos han venido modificando con aceleración constante la forma de vida de las sociedades, determinando que a mediados del siglo XX la denominada "sociedad industrial" fuera reemplazada por la actualmente llamada "sociedad de la información".
>
> La "sociedad de la información" se caracteriza, fundamentalmente, en que la creación, distribución y manipulación de la información forman parte importante de las actividades culturales y económicas, convirtiéndose sin lugar a dudas en bienes intangibles altamente valorados. (Anzit Guerrero, Profumo, & Tato, 2010, pág. 3)

Este marco de realidad ha sido magistralmente resumido por el Dr. Horacio Jaunarena, abogado y tres veces Ministro de Defensa de la República Argentina, basándose en los siguientes conceptos: 1) el avance tecnológico que define la modernidad, 2) el quinto dominio (al que llama ciberespacio), y 3) el marco legal:

> La modernidad introdujo un nuevo espacio y forma de conflicto que, si bien no está plenamente asumido, siempre está activo y nadie puede escapar de él.
>
> El ciberespacio constituye una nueva dimensión creada por el hombre en la que es difícil atribuir una agresión y que genera una nueva preocupación para los estados.

[10] De hecho, está cambiando. El uso de Internet desde dispositivos inalámbricos ha aumentado en forma sostenida en los últimos años. La AIMC (Asociación para la Investigación de Medios de Comunicación) ha realizado un estudio que determinó que el teléfono celular es el dispositivo más utilizado para acceder a Internet. (El móvil, líder en el consumo de internet, 2017).

Se trata de un ámbito común y global, semejante al mar internacional pero virtual, donde existe una seria dificultad para definir fronteras y soberanía, lo que impacta en el orden mundial.

Su violación afecta la seguridad individual y colectiva al dañar el funcionamiento del estado, por ello este debe protegerse, informar y educar a la población para prevenir sus efectos.

La ciberguerra no solo se trata de una guerra sin ruido ni armas, sino también de un delito rentable y, por ello, la ciberdefensa constituye un reto que impone equilibrar el anhelo de la apertura y la libertad, con los reparos frente a las amenazas crecientemente sofisticadas.

Cualquier proyecto debería considerar el desarrollo de un marco legal y protocolos, el diseño y aplicación de una estrategia organizacional y, especialmente, la generación de una cultura nacional ciudadana, similar a lo que fue la "Nación en armas" en el siglo XIX. (Jaunarena, Ciberseguridad y Ciberdefensa, 2015)

1.3 El marco legal argentino

Las leyes nos permiten establecer cuál es la idea rectora sobre un tema en una sociedad determinada. Es en ese sentido en el que se analizarán las leyes que reflejan el concepto de seguridad y defensa en la República Argentina, con el fin de determinar el marco teórico actual desde el punto de vista del derecho positivo. Esta idea rectora define el punto de partida desde el cual se realizarán los aportes.

La leyes marco fundamentales son la Ley de Seguridad Interior (Ley Nº 24509 de Seguridad Interior, 1991) y la Ley de Defensa Nacional (Ley N° 23554 de Defensa Nacional, 1988).

Estas leyes determinan los ámbitos pertinentes de la seguridad y la defensa a partir de dos elementos fundamentales. El primer elemento lo constituye la frontera del país, al indicar taxativamente que las fuerzas armadas no deben cumplir tareas con el fin de garantizar la seguridad interior (Ley Nº 24509 de Seguridad Interior, 1991). El segundo elemento es el origen del ataque, estableciéndose que las fuerzas armadas deberán actual sólo ante agresiones de origen externo (Ley N° 23554 de Defensa Nacional, 1988).

La ley de Defensa Nacional establece el concepto de Defensa Nacional en su artículo 2º, que dice: "La defensa nacional es la integración y acción coordinada de todas

las fuerzas de la Nación para la solución de aquellos conflictos que requieran el empleo de las fuerzas armadas, en forma disuasiva o efectiva, para enfrentar las agresiones de origen externo. Tiene por finalidad garantizar de modo permanente la soberanía e independencia de la Nación Argentina, su integridad territorial y capacidad de autodeterminación; proteger la vida y la libertad de sus habitantes"

Por su parte, la ley de Seguridad Interior define en su art 2º: "se define como seguridad interior a la situación de hecho basada en el derecho en la cual se encuentran resguardadas la libertad, la vida y el patrimonio de los habitantes, sus derechos y garantías y la plena vigencia de las instituciones del sistema representativo, republicano y federal que establece la Constitución Nacional" mediante el empleo de los elementos humanos y materiales de las fuerzas policiales y de seguridad para dicho objetivo.

En el año 2006 se reglamentó la Ley 23554 mediante el Decreto 727/2006, el cual especificó las diferencias entre seguridad interior y defensa nacional (la primera, a cargo de las fuerzas de seguridad y la segunda a cargo de las fuerzas armadas) y estableció que las fuerzas armadas sólo intervendrán ante agresiones de origen externo perpetradas por fuerzas armadas de otros estados. Dicho decreto define la agresión de origen externo como “el uso de la fuerza armada por un Estado contra la soberanía, la integridad territorial o la independencia política de nuestro país, o en cualquier otra forma que sea incompatible con la Carta de las Naciones Unidas” (Decreto Nº 727/2006 - Defensa Nacional, 2006).

En el año 2018 el Decreto 727/06 fue modificado por el Decreto 683/18. Este último eliminó el requisito de que la agresión de origen externo fuera perpetrada por fuerzas armadas de otros estados, lo que permitió la intervención de las fuerzas armadas ante agresiones externas de cualquier origen. Paralelamente facultó a las Fuerzas Armadas a prestar apoyo logístico a las Fuerzas de Seguridad (Decreto Nº 683/18 - Defensa Nacional, 2018).

Además de estas dos normas fundamentales para esta temática, el marco legal argentino consta de un sinnúmero de normativas de diverso grado jerárquico en cuanto a la organización de la seguridad y la defensa. En ese sentido, comienza diciendo Cornaglia:

> La Ley N° 24.948 (B.O. 8/04/1998) establece las bases políticas, orgánicas y funcionales fundamentales para la reestructuración de las Fuerzas Armadas, estableciendo en su artículo segundo que la política de defensa se sustenta en lograr

> consolidar e incrementar las capacidades espirituales y materiales que tornen eficaz una estrategia disuasiva, coadyuvando al mantenimiento de la paz y la seguridad internacionales. La Directiva de Política de Defensa Nacional, materializada en el Decreto N° 1714/ 2009 (B.O. 12/11/2009) y en su actualización conforme el Decreto N° 2645/2014 (B.O. 19/01/2015), inicia el planeamiento para la defensa nacional. De estos documentos derivan los principales lineamientos de la política de defensa y de la política militar de la República Argentina.
>
> [...]
>
> En 2014, la actualización de la Directiva de Política de Defensa Nacional contempló de manera expresa la importancia del ciberespacio para el desarrollo de las operaciones militares y planteó la necesidad de adaptar los sistemas de defensa a estos nuevos componentes. La Directiva destaca que solo una parte de la amplia gama de operaciones cibernéticas, afectan el ámbito de la Defensa Nacional.
>
> Además, estableció que resulta sencillo desde el punto de vista fáctico determinar a priori y ab initio si la afectación se trata de una agresión militar estatal externa. (Cornaglia & Vercelli, 2017)

En el año 2018 la Directiva de Política de Defensa Nacional (DPDN) establecida por el Decreto 7030 de dicho año ahondó más en los conceptos del quinto dominio, al considerar al ciberespacio como un bien común al igual que el alta mar y el espacio exterior. Estableció que el desarrollo tecnológico "incrementó los riesgos asociados a la militarización del ciberespacio. La disuasión se ha extendido al ámbito cibernético, al tiempo que han surgido nuevos desafíos producto de las tensiones entre una mayor conectividad, la privacidad y los derechos de la ciudadanía" (Decreto Nº 703/2018 - DPDN, 2018). Y también estableció que "El abordaje de esta problemática desde la perspectiva de la Defensa Nacional requiere adoptar medidas y acciones tendientes a resguardar la seguridad cibernética" (Decreto Nº 703/2018 - DPDN, 2018).

Cabe destacar que en el apartado c del Anexo I del citado decreto se aborda el tema de la utilización del ciberespacio con fines militares. Afirma que el ciberespacio es un ambiente operacional militar donde los estados despliegan operaciones de agresión e influencia sobre naciones adversarias. Finalmente establece que "La política de ciberdefensa debe orientarse a la reducción gradual de las vulnerabilidades que emergen de la informatización de los activos estratégicos de interés para la Defensa Nacional" (Decreto Nº 703/2018 - DPDN, 2018).

Con relación a la ciberseguridad, la Resolución SGM N° 829/2019 de la Secretaría de Gobierno de Modernización aprobó la Estrategia Nacional de Ciberseguridad y creó la Unidad Ejecutiva del Comité de Ciberseguridad en la órbita de dicha Secretaría. Dicha Estrategia permite entrever conceptos jurídicos relevantes a los efectos de este trabajo al establecer que:

> La irrupción de las nuevas Tecnologías de la Información y las Comunicaciones ha significado un punto de inflexión en la historia. Todos los aspectos de la vida humana están atravesados por este fenómeno. Hoy las personas se comunican, se expresan, se educan, crean, comercian, investigan y desarrollan gran parte de su vida social y laboral en el Ciberespacio.
>
> [...] el uso de las Tecnologías de la Información y las Comunicaciones para el relacionamiento entre las personas, la interacción del Estado con el ciudadano o el surgimiento de la economía digital, entre otras actividades, ha contribuido al crecimiento exponencial del uso del Ciberespacio, aumentando consecuentemente los riesgos a los que se encuentran expuestas las personas y las organizaciones. Es necesario reconocer esta realidad y asumir su complejidad, como primer paso indispensable para enfrentar las dificultades y problemas y hallar las soluciones adecuadas.
>
> La realidad nos muestra que en el Ciberespacio existen, entre otras, dificultades originadas en aspectos relacionados con la atribución de responsabilidad, las vulnerabilidades de las infraestructuras críticas, las grandes asimetrías que se manifiestan entre los países a partir de la globalización y las cuestiones vinculadas con el ejercicio de la soberanía. Este último concepto en particular, entendido como el ejercicio supremo del poder del Estado, está necesariamente vinculado a lo territorial. Sin embargo, Internet representa un dominio global e intangible y un flujo infinito de datos sobre el cual no se ejerce dominio ni soberanía, poniendo a prueba el concepto antes mencionado e instaurando un nuevo paradigma que es necesario entender. (Resolución Nº 829/2019 - Estrategia Nacional de Ciberseguridad, 2019)

Bajo estos conceptos y como consecuencia de los mismos se establece como uno de los objetivos el "Adecuar y generar las normas jurídicas, marcos regulatorios, estándares y protocolos, para hacer frente a los desafíos que plantean los riesgos del ciberespacio,

asegurando el respeto de los derechos fundamentales" (Resolución Nº 829/2019 - Estrategia Nacional de Ciberseguridad, 2019).

1.4 El marco legal internacional

En el mismo sentido que en el caso del marco legal argentino, el análisis del marco legal internacional nos provee las ideas rectoras y definiciones respecto a la ciberdefensa y la ciberseguridad. En el caso internacional me limitaré a enumerar los casos de la Unión Europea, Estados Unidos, y el Manual de Tallin por considerarlos los más relevantes en Occidente en relación a la temática tratada en este trabajo.

1.4.1 Unión Europea

La Directiva 2016/1148 reconoce la importancia de los sistemas informáticos para las actividades sociales y económicas, y reconoce el aumento de la magnitud, frecuencia y consecuencia de los incidentes de seguridad informática[11]. Bajo ese criterio, establece requisitos mínimos comunes de seguridad, y obliga a los estados de la UE a adoptar una estrategia nacional de seguridad de las redes y sistemas de información.

Establece las definiciones, al igual que muchas normas relacionadas con los sistemas informáticos, sobre el alcance de conceptos informáticos tales como punto de intercambio de internet, operador de servicios esenciales, servidor de nombres de dominio, servicio de computación en la nube, entre otros, con el fin de establecer claramente una base común de significados.

La directiva determina los alcances y objetivos de la estrategia nacional de seguridad, pero deja en manos de cada estado miembro el determinar el modo en que esos alcances y objetivos serán solventados. Esto se refleja en su artículo 14, donde dice "Los Estados miembros velarán por que los operadores de servicios esenciales tomen las medidas técnicas y de organización adecuadas y proporcionadas para gestionar los riesgos que se planteen" (Directiva (UE) 2016/1148, 2016). Incorpora además el concepto de debida diligencia, que jurídicamente se ha impuesto en cuanto a la responsabilidad de los prestadores de servicios en el quinto dominio, el cual exige a los involucrados la aplicación

[11] La magnitud del daño se evalúa, conforme a esta directiva, en base al número de usuarios afectados por la perturbación del servicio esencial; la duración del incidente; y la extensión geográfica con respecto a la zona afectada por el incidente (art. 14.4).

de aquellas medidas razonables de gestión y seguridad conforme a la actividad o giro del negocio.

Obliga a que cada estado miembro establezca uno o más CSIRT (*Computer Security Incident Response Team*)[12], y determina la obligatoriedad de la cooperación entre los CSIRT de cada estado miembro.

Con respecto a la jurisdicción, determina que se aplicará la jurisdicción donde el proveedor de servicios digitales tenga su domicilio societario.

En su Anexo II, enumera los servicios que son considerados esenciales. Dentro del sector energía, enumera la electricidad (producción, transporte y distribución), el crudo (producción, transporte, almacenamiento y refinamiento), y el gas natural y licuado (producción, almacenamiento, transporte y distribución). En el sector transporte, enumera el transporte aéreo (aerolíneas, aeropuertos, gestión del tráfico aéreo), el ferrocarril (empresas e infraestructura), transporte marítimo y fluvial (empresas, puertos, gestión de tráfico), y transporte por carreteras (autoridades y operadores de transporte inteligente). En el sector de banca incluye las entidades de crédito en general. En el sector de Infraestructura de los mercados financieros incluye las Bolsas y gestión de instrumentos de mercados financieros. En el sector sanitario incluye los hospitales y clínicas. En el sector de infraestructura digital incluye los proveedores de servicio de DNS (*Domain Name Servers*, Servidores de Nombres de Dominio), los registros de nombre de dominio de primer nivel, y los proveedores de interconexión, también denominados puntos neutros, que interconectan a los proveedores de servicios de internet (ISP por sus siglas en inglés). Resulta notoria la no inclusión de los ISP dentro de los servicios considerados esenciales.

La Decisión 7219/19 (Decisión del Consejo de la Unión Europea 7299/19 relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros, 2019), tiene como fin el impedir y contrarrestar los ciberataques contra estados miembros de la Unión, mediante la incorporación de una legislación de tipo disuasivo. Sólo se aplican a ataques que se originen fuera de la Unión, o utilicen infraestructura fuera de la Unión; hayan sido cometidos por personas o entidades que tengan actividad fuera de

[12] Un CSIRT es un Equipo de Respuesta a Incidentes de Seguridad Informática. Está conformado por un grupo de profesionales de TI (Tecnología de la Información) que brinda servicios y soporte en torno a la prevención, gestión y coordinación de posibles emergencias relacionadas con la seguridad informática.

la Unión; o hayan sido realizados con el apoyo o bajo el control de una persona física o jurídica que tengan actividad fuera de la Unión[13]. Y sólo se aplica a actores no estatales. Para el caso de actores estatales se establece que las medidas a adoptar constituyen una decisión soberana que queda en manos del Estado atacado.

Se considera un ciberataque a toda acción que accede a sistemas de información, interfiera en el sistema de información, interfiera con los datos, o intercepte los datos.

Para estar sujeto a sanciones, un ciberataque debe cumplir dos criterios: que el ataque tenga un efecto significativo y que el ataque constituya una amenaza externa para la Unión o sus Estados miembros.

La magnitud de un efecto significativo se evalúa a partir de los siguientes indicadores: el alcance, la escala, el impacto o la gravedad de la interrupción causada; el número de personas físicas o jurídicas, entidades u organismos afectados; el número de Estados miembros interesados; el monto de la pérdida económica causada; el beneficio económico obtenido por el autor, para sí mismo o para otros; la cantidad o naturaleza de los datos robados o la escala de las infracciones de datos; y la naturaleza de los datos sensibles desde el punto de vista comercial a los que se accede.

Las medidas disuasivas que establece incluyen en primera instancia la obligación de negar el ingreso o tránsito a las personas físicas responsables de los ciberataques o tentativas de ciberataques, de quienes provean ayuda técnica, material o económica[14]. Se exceptúan a los nacionales de cada país, y los casos de obligaciones internacionales[15]. Como segunda medida, la Decisión ordena la inmovilización de fondos cuya propiedad, tenencia, titularidad o control correspondan a las personas físicas o jurídicas quienes hayan intentado o realizados los ciberataques, hayan prestado colaboración material, económica o técnica; y las personas física o jurídicas asociadas a las antedichas.

1.4.2 Estados Unidos

Entre el año 2002 y 2014 rigió la *Federal Information Security Modernization Act* (FISMA) (Federal Information Security Management Act, 2002) la cual exigía el

[13] Art. 1.2
[14] Art. 4.1
[15] Art. 4.2 y 4.3

desarrollo y la implementación de políticas, principios, estándares y directrices obligatorios sobre seguridad de la información en el ámbito público, es decir, que no se aplicaba a compañías privadas, como las proveedoras de infraestructura de Internet.

En el año 2009 se crea el *U. S. Cyber Command* [16]. Su director es el director de la *National Security Agency* (NSA)[17] y sus oficinas están en la sede de la NSA.

Creado originalmente como un organismo defensivo, ahora realiza también acciones ofensivas. Su misión es descripta de la siguiente manera:

> **USCYBERCOM** [18] planifica, coordina, integra, sincroniza y realiza actividades para: dirigir las operaciones y la defensa de redes de información específicas del Departamento de Defensa y; prepararse y, cuando se le indique, realizar operaciones militares de ciberespacio de espectro completo para permitir acciones en todos los dominios, garantizar la libertad de acción de los Estados Unidos / Aliados en el ciberespacio y negar lo mismo a nuestros adversarios (United States Cyber Command, 2009).

En el año 2018 se dicta la ley de creación de la Agencia de Ciberseguridad y Seguridad de la Infraestructura de la Información (115 Congress of the United States of America, 2018), que depende del *Department of Homeland Security*.

Sus funciones principales son las de desarrollar la capacidad para defenderse de los ataques cibernéticos; y proporcionar al gobierno federal herramientas de seguridad cibernética, servicios de respuesta a incidentes y capacidades de evaluación. Esta agencia trabaja con asociaciones en los sectores público y privado, y brinda asistencia técnica y evaluaciones a entes federales y privados de infraestructura.

[16] Sitio oficial del Comando Cibernético de los Estados Unidos, disponible en https://www.cybercom.mil/, consultado el 15 de agosto de 2020.
[17] Sitio oficial de la Agencia Nacional de Seguridad de los Estados Unidos, disponible en https://www.nsa.gov/, consultado el 15 de agosto de 2020.
[18] Es el nombre corto utilizado para denominar al U.S. Cybercommand (Comando Cibernético de los Estados Unidos)

1.4.3 Manual de Tallin 2.0

El Manual de Tallin 2.0 (Schmitt & Vihul, 2017) conforma un modelo que circunscribe elementos jurídicos y figuras normativas para ciberoperaciones en tiempos de guerra y en tiempos de paz, y es considerado mundialmente como uno de los documentos jurídicos más importantes relativo al quinto dominio. Afirma William Banks:

> El Manual de Tallin 2.0 marca un punto importante pero temprano en una conversación entre los Estados sobre los principios más importantes del derecho internacional en cibernética. La conversación es muy importante porque gran parte de nuestras relaciones internacionales ahora están ligadas al dominio cibernético, y las reglas actuales del camino están plagadas de áreas grises y entendimientos incompletos. (Banks, 2017, pág. 1513)

En su comienzo cita, en relación al ataque sufrido por Estonia en 2007, la reconocida frase de Von Clausewitz: "La guerra es la continuación de la política por otros medios". Dicha guerra, afirma el Manual, fue una simple operación de ataque de denegación de servicio distribuido y aceleró la creación del Centro de Excelencia de Ciberdefensa Cooperativo de la Organización del Tratado del Atlántico Norte (NATO CCD COE, por sus siglas en inglés) con sede en Tallin, capital de Estonia. Una de las primeras actividades de dicho organismo fue un estudio sobre ciberguerra realizado por un grupo internacional de expertos del cual resultó el Manual de Tallin publicado en el año 2013. Dicho manual ha constituido una guía útil para varios países para aplicar el Derecho Internacional a ciberconflictos. La evolución del trabajo de la NATO CCD COE llevó a la creación de la segunda edición del Manual de Tallin (*Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*) la cual, además de la ciberguerra, abarca las situaciones del ámbito cibernético en tiempos de paz; e incluye conceptos como el derecho espacial, la jurisdicción en el ciberespacio, y los derechos humanos.

> [El] segundo Manual de Tallin [...] servirá como una hoja de ruta para gobiernos que busquen una mayor claridad con respecto a sus derechos y obligaciones en el ciberespacio. El libro también será útil para la comunidad internacional mientras lucha con la complejidad de identificar las normas cibernéticas existentes y promulgar otras nuevas. (Schmitt & Vihul, 2017, pág. xxiv)

El segundo Manual de Tallin define los conceptos de soberanía, debida diligencia, jurisdicción territorial y extraterritorial, responsabilidad internacional, contramedidas ante ataques y reparaciones. Trata también sobre ciberespionaje y actores no estatales. En su segunda parte trata sobre derechos humanos en el ciberespacio, aspectos diplomáticos y consulares aplicados al ciberespacio y su infraestructura, ciberoperaciones relacionadas con el derecho del mar (que incluye lo respectivo a los cables submarinos), el derecho del aire y del espacio exterior. En su tercera parte trata sobre el uso de la fuerza, la amenaza del uso de la fuerza, y la defensa propia donde incluye los elementos de necesidad y proporcionalidad. En su cuarta parte comienza a tratar las leyes del conflicto armado, establece las responsabilidades de los actores, el modo en que debe conducirse las hostilidades y los aspectos referentes a sus actores; definición de ciberataque, estado de la población civil, objetivos civiles, medios y métodos de ataques, el concepto de proporcionalidad, el uso apropiado de las armas, su uso desleal e inapropiado, la protección de personal religioso y médico, personal detenido, niños, y periodistas; la protección de bienes culturales, la protección de bienes ambientales y la asistencia humanitaria. Establece también las reglas referentes a la ocupación, y las ciberoperaciones en territorios neutrales.

Esta página ha sido dejada en blanco intencionalmente.

Capítulo II - Evolución de la interacción entre la tecnología y el derecho

Nadie se baña dos veces en el mismo río.
Heráclito

Estudia el pasado si quieres pronosticar el futuro.
Confucio

Introducción

Abordaré el análisis del efecto en el aspecto jurídico de la sociedad que ha tenido el avance tecnológico durante el pasado reciente, a partir del estudio de hechos de especial relevancia como la invención de la fotografía instantánea o el teléfono, los cuales han introducido desafíos de fuste a los conceptos jurídicos de la época. Analizaré el nivel de resistencia al cambio o adaptación que ha existido ante estos cambios tecnológicos con el fin de evaluar, a partir de las experiencias del pasado, si en el presente estamos ante una situación de similares características, lo que facilitaría el análisis y a la cual podríamos aplicar recetas similares.

2.1 El avance tecnológico y el derecho a la privacidad

La frase de Heráclito, el oscuro de Éfeso, plasmaba ya hace más de 2.500 años la realidad cambiante de la existencia. Una característica de la historia humana ha sido que la velocidad de dichos cambios ha sufrido una aceleración constante. Desde la invención de la imprenta de tipos móviles en el siglo XV hasta la invención del motor a vapor pasaron tres siglos. La revolución industrial que trajo esta última invención provocó un cambio social inesperado a partir de fines del siglo XVIII, una notable migración del campo a la ciudad y un enorme aumento del trabajo en fábricas. La legislación debió adaptarse a estas nuevas circunstancias, y será recién a comienzos del siglo XX cuando en diversos países comenzarán a sancionarse leyes laborales regulen adecuadamente la actividad en fábricas. "Desde la Revolución Industrial, al ser el trabajo una actividad permanente del diario vivir de la sociedad, se hizo necesario contar con una normativa eficiente sobre los derechos,

deberes, prohibiciones y beneficios que deben sujetarse tanto los empleados como los empleadores." (Antezana de Guzman, 2012, pág. 67).

La evolución tecnológica nos trajo la fotografía instantánea, inventada por Kodak en las postrimerías del siglo XIX, que junto con la impresión y distribución masiva de periódicos provocó un profundo debate en la sociedad del siglo XIX respecto a la reducción del ámbito de privacidad que dicha tecnología provocaba. El debate pendulaba entre quienes afirmaban que la privacidad era un lujo del pasado que debíamos resignarnos a perder y quienes afirmaban que la privacidad debía ser protegida mediante la ley.

En esta última postura se destacó el artículo "*The right to privacy*" publicado en el Harvard Law Review el 15 de Diciembre de 1890, donde sus autores Samuel D. Warren y Louis D. Brandeis definieron a la privacidad como "*the right to be left alone*" (Warren & Brandeis, 1890), es decir, el derecho a no ser molestado. Esta definición de privacidad, si bien es ampliamente aceptada hoy en día, fue revolucionaria para la época. Ya entrado el siglo XX la invención del teléfono trajo aparejado un nuevo conflicto jurídico, en este caso, respecto a la privacidad de las conversaciones telefónicas. En 1927, en el caso "Olmstead vs. United States", la Corte Suprema de los Estados Unidos determinó que una conversación telefónica no era un ámbito privado, y que por lo tanto no consistía invasión a la privacidad la escucha de la misma mediante la interceptación. Esta decisión fue adoptada con el voto en disidencia del en ese entonces juez Louis D. Brandeis. Será recién en 1967, en el caso "Katz vs. United States" cuando la Corte Suprema de los Estados Unidos adopte el concepto de privacidad plasmado en el artículo "*The right to privacy*", y considere la conversación telefónica como un ámbito privado.

En Argentina una situación similar sucedió en dos casos particulares. El primero, respecto a los derechos de autor y el software. La Cámara Nacional de Casación Penal falló en 1995 que el software no podía considerarse dentro de las obras artísticas, científicas y literarias tuteladas por la Ley 11.723 de propiedad intelectual. Dicho fallo fue confirmado por la Corte Suprema en la causa "Autodesk, Inc. s/recurso de casación" (Autodesk, Inc. s/recurso de casación, 1997). En consecuencia, la copia sin autorización de software no constituía delito. Este criterio recién fue modificado en 1998 con la sanción de la Ley 25036, donde explícitamente se incorporan los programas de computación, fuente y

objeto[19], como obras protegidas por los derechos de autor. El segundo caso consistió en la difusión pública de un correo electrónico por parte del periodista Jorge Lanata. En este caso, la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Ciudad Autónoma de Buenos Aires, en el caso "Lanata, Jorge s/ desestimación" determinó que:

> [...] el tan difundido "e-mail" de nuestros días es un medio idóneo, certero y veloz para enviar y recibir todo tipo de mensajes, misivas, fotografías, archivos completos, etc.; es decir, amplía la gama de posibilidades que brindaba el correo tradicional al usuario que tenga acceso al nuevo sistema. Es más, el correo electrónico posee características de protección de la privacidad más acentuadas que la inveterada vía postal a la que estábamos acostumbrados. (Lanata, Jorge s/ Desestimación, 1998)

En este caso el criterio judicial, a diferencia del fallo Autodesk, fue ampliar el objeto protegido por el tipo penal (el correo epistolar) a los nuevos objetos creados por la tecnología (el correo electrónico). Esto se hizo no sin poner en peligro uno de los conceptos más elementales del derecho penal, *nullum crimen, nulla poena sine praevia lege* [20]. Será recién en el año 2008, con la sanción de la Ley 26388 de Delitos Informáticos, cuando quede plasmado sin lugar a dudas en nuestro ordenamiento jurídico el concepto de protección del correo electrónico[21].

Estos ejemplos nos marcan que la evolución tecnológica se acelera y el marco jurídico que debe dar soporte a la misma evoluciona de manera más pausada. Esto tiene como consecuencia directa la demora de años o décadas en contemplar adecuadamente la realidad que la tecnología modifica o crea. En palabras de Jesús Reguera Sánchez, respecto a adecuación de los marcos legales a la realidad del quinto dominio:

---

[19] Se denomina "código fuente" al código escrito por un programador en cualquier lenguaje. Se denomina "código objeto" al código resultante de compilar (una forma de traducción) el código fuente. El "código objeto" es el que puede interpretar la computadora, y lo que la gente denomina comúnmente "programas".

[20] Este aforismo latino establece que los delitos sólo pueden considerarse tales si existe una ley previa que lo defina específicamente. Si así no fuera, podrían sancionarse leyes que penasen conductas anteriores a la sanción de la ley, o podrían considerarse delitos conductas que no surgen claramente en la ley como punibles. En ambos casos se caería en un estado de inseguridad jurídica contrario al derecho, poniéndose en peligro la libertad de los ciudadanos.

[21] La Ley 26388 empela el concepto "comunicación electrónica", con lo que amplía la protección a todo tipo de mensaje enviado por medios electrónicos.

> El gran problema que se les presenta a los que defienden una regulación es la lentitud intrínseca de las regulaciones nacionales e internacionales ante los rápidos avances tecnológicos, debido a la falta de preparación ante estos nuevos retos. Ésta es una de las razones por la que la red es tachada de pesadilla jurídica. (Reguera Sánchez, 2015, pág. 6)

En la actualidad encontramos una reedición del debate respecto al ámbito de la privacidad de las personas. Lo que hace más de un siglo significó un acalorado debate respecto al cercenamiento del ámbito de privacidad por la invención de la fotografía instantánea hoy se reedita a partir de la invención del reconocimiento facial practicado por cámaras en la vía pública.

> China fue de los primeros países en utilizar el reconocimiento facial como aliado y salvaguarda de la seguridad en las calles. Allí, más de 300 millones de cámaras de seguridad, gracias a esta tecnología, detectan una cara entre una multitud en cuestión de segundos. Aunque Estados Unidos cuenta con este sistema de detección en muchos de sus aeropuertos, en ciudades como San Francisco ha prohibido técnicas de reconocimiento facial para identificar a criminales[...] Alemania lo prohíbe para su policía y Francia en las instituciones educativas, mientras otras ciudades, como Londres, llevan el camino contrario. En concreto, la Policía Metropolitana londinense anunció a principios de año que la tecnología de reconocimiento facial en las calles ha superado la etapa de prueba previa y está lista para integrarse permanentemente en la vigilancia diaria de la ciudad. (Díaz, 2020)

En la Ciudad de Buenos Aires se aplica la misma tecnología de reconocimiento facial, pero no en forma generalizada sino limitada a una base de datos de rostros de personas con pedido de captura. Entre abril y diciembre de 2019 "el sistema identificó y detuvo 343 prófugos, incluyendo personas implicadas en casos de homicidio, delitos sexuales, narcotráfico y estafas" (Silvestrini, 2019). Un sistema similar ha sido adoptado por la provincia de Córdoba.

El debate en este sentido está lejos de terminar y la legislación aún no ha dado una respuesta definida; aunque probablemente se repita la historia tal como presagia la frase de Confucio citada al comienzo de este capítulo: la sociedad se adaptará a este nuevo límite

impuesto por el avance tecnológico, como lo hizo anteriormente a partir de la invención de la fotografía instantánea.

2.2 Big Data y los datos personales

Otro conflicto tecnológico-legal ha surgido a partir de la tecnología conocida como *Big Data*. Esta tecnología permite el tratamiento de grandes volúmenes de datos para obtener nueva información a partir de un análisis estadístico. Sin bien la obtención y tratamiento de datos personales está legislada en Argentina desde el año 2000 (Ley Nº 25326 de Protección de Datos Personales, 2000), los nuevos datos que se obtienen a partir de una enorme cantidad de datos simples no están abarcados específicamente por dicha ley. El New York Times Magazine (Duhigg, 2012) refleja un caso real ocurrido en Target, una tienda de ramos generales de los Estados Unidos con más de un siglo de existencia.

Durante años Target recolectó información respecto a lo que compraba cada cliente. Esa información estaba relacionada con un ID[22] de cliente que además contenía información demográfica como su edad, si estaba casado y tenía hijos, en qué parte de la ciudad vivía, cuánto tiempo le llevaba manejar hasta la tienda, su salario estimado, si se había mudado recientemente, qué tarjetas de crédito llevaba en su billetera y qué sitios web visitaba. Target además pudo comprar datos sobre su origen étnico, historial laboral, las revistas que leía, si alguna vez se había declarado en bancarrota o si se había divorciado, el año en que había comprado (o perdido) su casa, a qué universidad había asistido, sobre qué tipo de temas hablaba en Internet, sus inclinaciones políticas, hábitos de lectura, donaciones caritativas y la cantidad de autos que poseía, entre otros datos.

En el año 2011 se planteó la necesidad de reconocer lo antes posible cuando una mujer estaba embarazada y cursando el segundo trimestre, con el fin de enviarle ofertas de productos y cupones de descuentos relacionados antes que otras tiendas similares; y ganar así más cuota de mercado.

Target tenía un registro de *baby shower* (brindado por las mujeres voluntariamente) sobre el cual analizaron los cambios en los hábitos de compra a medida que una mujer se acercaba a su fecha de parto. Luego de varios análisis comenzaron a emerger patrones. Lociones, por ejemplo. Mucha gente compra loción, pero notaron que las mujeres

[22] Código identificador

registradas estaban comprando cantidades más grandes de loción sin perfume alrededor del comienzo de su segundo trimestre. Otro analista notó que en algún momento de las primeras 20 semanas las mujeres embarazadas compraban suplementos como el calcio, el magnesio y el zinc. También notaron que muchas compradoras compraban jabón y bolas de algodón, pero cuando alguien comenzaba a comprar más cantidades de jabón sin olor y bolsas grandes de bolas de algodón, además de los desinfectantes para las manos y toallas, esto indicaba que podrían estar acercándose a su fecha de parto.

Luego del análisis se pudieron identificar unos 25 productos que, cuando se analizaron juntos, le permitieron asignar a cada compradora una puntuación de "predicción de embarazo". Más importante aún, el sistema también podría estimar su fecha de parto con bastante aproximación, lo que permitía a Target enviar cupones de descuento específicos para cada etapa del embarazo.

Luego de un año de aplicar modelo predictor, un hombre indignado se acercó a la tienda porque su hija adolescente había recibido cupones para ropa de bebé y cunas, lo cual consideraba que incentivaba el embarazo adolescente. El gerente confirmó que la publicidad había sido enviada y le pidió disculpas al hombre ya que suponía que había sido algún tipo de error. Pero unos días después el padre de la adolescente llamó avergonzado. "Tuve una charla con mi hija", dijo. "Resulta que ha habido algunas actividades en mi casa de las que no he sido completamente consciente. La fecha de parto es en agosto. Le debo a Ud. una disculpa".

Target afirma que cumple con todas las regulaciones legales, lo que incluye la relativa a la protección de la información relativa a la salud de las personas, sin embargo, la pregunta esencial que genera este caso no tiene respuesta por el momento: ¿Cuál es el alcance de la regulación respecto a los nuevos datos que surgen del análisis mediante *Big Data*? ¿Qué nivel de seguridad pueden tener las personas cuando los datos "personales", como las compras en un almacén, revelan datos "sensibles"[23]?

[23] En el ámbito legal se distinguen los datos personales de los sensibles. Los primeros se refieren a cualquier dato sobre una persona. Los segundos se definen como aquellos datos que pertenecen a la esfera íntima de una persona. La Ley 25326 establece estos últimos taxativamente: origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual

Este tema, tal como está planteado, aún no ha sido abordado por nuestra legislación y es probable que genere próximamente un debate sobre la protección de los datos sensibles obtenidos a través de técnicas de *Big Data*.

2.3 El cambio como constante

La evolución tecnológica también se ve reflejada también en el ámbito de gerenciamiento de las empresas, donde se ha acuñado el concepto V.I.C.A., el cual responde a las palabras Volátil, Incierto, Complejo y Ambiguo. Este acrónimo caracteriza un entorno en el cual la alta velocidad de los cambios, la enorme cantidad de variables y la alta complejidad de los componentes y actores hacen que sea muy difícil diagramar o enmarcar en forma acabada una situación específica. Respecto al ambiente VICA, dice Alberto Teralto:

> En este tipo de ambientes, la relación causa-efecto no es fácil de determinar, no sólo porque es difícil de descubrir, sino porque no resulta ser siempre la misma. Los agentes sociales aprenden, modifican sus comportamientos, presentan gamas de comportamientos posibles y a veces, ocurren situaciones que no se han presentado en el pasado. (Terlato, 2018, pág. 9)

El cambio constante y la multiplicidad y complejidad de variables es una de las características que definen principalmente a la modernidad. Sus consecuencias en el plano jurídico no son menores. Los cambios tecnológicos en relativamente poco tiempo modifican el modo en que nos relacionamos social, cultural y económicamente; y el derecho (como hemos visto) ha debido sortear no pocas dificultades para actualizarse el ritmo de dichos cambios, tanto sea por lo complejo del cambio como por la resistencia al cambio de los actores involucrados. Esta problemática la analizaremos en relación a la ciberseguridad y la ciberdefensa.

La tecnología es un elemento esencial en la aceleración evolutiva. Hace relativamente poco años se expandió por el todo el planeta la utilización de pequeños dispositivos conectados a Internet, y además se le proveyó conexión a Internet a objetos que antes no la tenían, como heladeras, televisores y aires acondicionados. Este fenómeno se denomina "Internet de las cosas" (IoT, por sus siglas en inglés, *Internet of Things*). Esto

expandió el campo del quinto dominio en forma exponencial y abrió un campo de batalla y ciberdelitos sin precedentes, en el cual resulta muy difícil defenderse adecuadamente. Según palabras de Hodgson:

> [...] la creciente vulnerabilidad de muchas naciones a los ataques cibernéticos, particularmente en sociedades tecnológicamente más avanzadas, significa que la superficie de ataque potencial es tan grande que es improbable una preparación adecuada. La aparición del "Internet de las cosas" y los sistemas de tecnología operativa cada vez más conectados en red presagian una vulnerabilidad aún mayor en el futuro. (Hodgson, Ma, & Marcinek, 2019)

En el mismo sentido, la Estrategia Nacional de Ciberseguridad del Reino Unido dice que:

> Cuando la última estrategia de ciberseguridad nacional se publicó en 2011, la mayoría de las personas concebían la ciberseguridad a través del prisma de la protección de sus dispositivos como computadoras PC o laptops. Desde entonces el Internet se ha integrado cada vez más a nuestra vida diaria en formas que ignoramos. El Internet de las cosas crea nuevas oportunidades de explotación y hace que aumente el impacto potencial de los ataques que tienen el potencial de causar daños físicos, lesiones a personas y, en el peor de los caos, la muerte. La rápida implementación de conectividad en los procesos de control industrial en sistemas críticos, en una gran gama de sectores como el energético, el minero, el agrícola y el de la aviación, ha creado un Internet de las cosas industrial. Esto simultáneamente empezó a abrir las posibilidades de que dispositivos y procedimientos, que en el pasado nunca eran vulnerables a dichas interferencias, fueran atacados por los piratas informáticos y falsificados, con consecuencias potencialmente desastrosas. (HM Government, 2016, pág. 14)

Un ejemplo reciente fue la revelación de la ubicación de bases militares de los Estados Unidos a partir del uso de dispositivos *wearables* para deportistas, llamados *Activity Tracker*, los cuales mostraban en Internet (al alcance de cualquier persona) los recorridos realizados durante el ejercicio físico diario de su personal (HSU, 2018). Otros

dispositivos como los robots aspiradora que realizan un mapa electrónico de una habitación, oficina o inmueble con el fin de realizar la limpieza, podrían ofrecer un punto de vulnerabilidad a tener en cuenta. Ya en el ámbito de los datos personales, las recientes aplicaciones para dispositivos móviles (también conocidas como Apps) que permiten conocer la ubicación de personas infectadas por el coronavirus con el objetivo de evitar dichas zonas ya han tenido millones de descargas en Corea del Sur. "La app Corona 100m, por ejemplo, advierte a su usuario cuando se encuentra a menos de 100 metros de un lugar donde ha habido un paciente confirmado de coronavirus" (Pérez Colomé, 2020).

Corona 100m no es la única App. También se han creado las aplicaciones CoronaNow y CoronaAlert con similar funcionalidad. Esta información es brindada también por el gobierno en Hong Kong, aunque sin mostrar la dirección precisa con el fin de resguardar la privacidad. La información de este tipo es crítica para cualquier Estado, y las fallas de seguridad sobre estas Apps podrían ser aprovechadas por agentes enemigos.

2.4 Conclusiones parciales

Ha quedado en evidencia a partir de los casos analizados, tanto los históricos como los actuales, que la evolución tecnológica ha forzado la mano del legislador a adaptar los marcos jurídicos y las definiciones legales a las nuevas situaciones introducidas por la evolución tecnológica. Dicha adaptación ha tomado décadas en los casos más lejanos en el tiempo, y años en los casos más cercanos.

Cada cambio tecnológico planteó un desafío no menor a los conceptos jurídicos vigentes hasta ese entonces, como el ejemplo visto de la invención de la fotografía en su afectación al ámbito de privacidad vigente hasta ese momento, o como en el caso de la invención y generalización del uso del teléfono, en cuanto a la privacidad o no de una conversación telefónica. Cada evolución jurídica que resolvía o contemplaba adecuadamente las nuevas situaciones generadas por el avance tecnológico no era aplicable a nuevos avances, como pudimos ver el caso, más próximo en el tiempo, del correo electrónico durante la década del '90, en el cual si bien podríamos hacer una analogía entre la privacidad de una conversación telefónica y de un correo electrónico, jurídicamente el correo electrónico era un elemento nuevo y no contemplado por el derecho penal.

Y mientras esa adaptación legal a las nuevas situaciones creadas por la tecnología no se produce las personas quedan varadas en limbos legales, que no dejan de conformar una situación injusta para quienes han visto vulnerados su derechos. En esos limbos se ven obligados a deambular por la burocracia tribunalicia sin obtener respuestas u obteniendo respuestas diametralmente opuestas según el tribunal que tratare el caso.

Considerando el tiempo que tomó el aceptar modificaciones que hoy nos resultan naturales, como en los citados ejemplos de la comunicación telefónica y el correo electrónico, podemos concluir que existió una considerable resistencia al cambio a nivel jurídico por parte de quienes debían aplicarlos. Le llevó décadas a un sistema legal como el de los Estados Unidos aceptar que el concepto de privacidad incluía no sólo la propiedad y los papeles personales, sino también incluía conversaciones telefónicas, algo que hoy está fuera de discusión. En igual medida para el correo electrónico, hoy protegido por ley, pero cuya protección fue puesta en duda en su origen por los tribunales argentinos.

Vimos también que la evolución tecnológica se ha acelerado, lo que implica más cambios en períodos más cortos de tiempo y con cada vez más impacto. En los últimos años han surgido con cada vez más frecuencia nuevas tecnologías que impactan en la vida comercial y personal de los individuos, ya sean para brindar un nuevo servicio o para atender una necesidad imperiosa, como el citado caso de las aplicaciones que ayudan a gestionar el combate contra el coronavirus. Estos cambios en la actualidad y los que se produzcan en el futuro, si no son abordados desde el sistema jurídico, llevarán nuevamente a las personas a diversas situaciones de indefensión jurídica ante tecnologías que produzcan bienes y servicios nuevos, o invadan ámbitos privados, o lisa y llanamente produzcan daños que no puedan ser definidos o determinados por quien está a cargo de la aplicación de la ley.

Capítulo III - Aspectos legales del quinto dominio: ciberseguridad y ciberdefensa.

No hay pensamiento sin una sacudida de los cimientos.

Jean Guitton

El Pensamiento y la Guerra

Introducción

Como hemos visto hasta el momento la evolución tecnológica generó, impulsó o forzó cambios jurídicos de relevancia. Analizaré en este capítulo cuáles son los principales problemas que presenta el quinto dominio respecto al ámbito jurídico de la ciberdefensa y la ciberseguridad, y describiré las adaptaciones legales que como respuesta se han dado, con mayor o menor alcance, en Argentina y la Comunidad Europea.

3.1. Seguridad y Defensa en el quinto dominio

Defensa y seguridad son dos conceptos claramente distinguidos en la legislación argentina. Como mencioné anteriormente, las leyes 23554 de Defensa Nacional y 24509 de Seguridad Interior establecen que la defensa nacional atañe a las Fuerzas Armadas (Ejército, Armada y Fuerza Aérea) ante agresiones de origen externo, y la seguridad interior atañe a las Fuerzas de Seguridad (Policía Federal, Gendarmería, Prefectura y Policía de Seguridad Aeroportuaria) ante agresiones internas. Esta separación es inherente a la realidad argentina y se encuentra en la raíz de nuestra realidad política actual. Como dice el Grl. Div. (R) Evergisto de Vergara:

> [...] mientras que en Europa y Norteamérica los términos de seguridad y defensa son intercambiables y nadie gasta un segundo en pensar si existe entre ellos alguna diferencia, en Latinoamérica y el Caribe es un tema que ha consumido toneladas de papel. (de Vergara, Las diferencias conceptuales entre Seguridad y Defensa, 2009, pág. 7)

Y agrega:

> Las consecuencias prácticas son que la persistente desconfianza mutua entre los líderes civiles y militares en muchos países de Latino América evitan que, en la región, las capacidades de las fuerzas armadas sean usadas al máximo en la lucha por obtener la seguridad multidimensional [...] la seguridad es multidimensional, porque las amenazas, riesgos y preocupaciones provienen ahora no solo de conflictos armados, sino que las nuevas amenazas revisten además otras características. Este concepto de seguridad multidimensional ha sido aceptado por todos los países de la OEA. (de Vergara, Las diferencias conceptuales entre Seguridad y Defensa, 2009, pág. 7 y 19)

El planteo del Grl. Div. (R) de Vergara respecto a la seguridad multidimensional está relacionado íntimamente con una forma de llevar a cabo los conflictos bélicos que ha surgido en las últimas décadas: la guerra híbrida. El Gral. Sánchez García la conceptualiza al afirmar que:

> Hace ya más de una década que el adjetivo híbrido se abrió paso en el lenguaje de algunos expertos en asuntos de defensa para calificar lo que consideraron como el nacimiento de un nuevo tipo de conflicto, diferente tanto de la guerra tradicional o convencional como de la guerra irregular, y que, en líneas generales, sería la resultante del empleo simultáneo de ambas formas de lucha. (Sánchez García, 2012, pág. 11)

Dentro de los elementos de la guerra irregular se encuentran las ciberoperaciones realizadas por *hackers* y las acciones de propaganda y manipulación a través de redes sociales e Internet en general, como el uso de *fake news*. Es por ello que el concepto de guerra multidimensional, en lo que al quinto dominio compete, implica una forma de guerra híbrida donde se conjugan ciberoperaciones realizadas por fuerzas armadas regulares y ciberoperaciones realizadas por fuerzas irregulares. No sería arriesgado afirmar que en este ámbito, por su naturaleza no espacial y su inherente dificultad para determinar la atribución, todas las guerras son híbridas. En consecuencia, el quinto dominio nos planta desafíos cuando queremos aplicar conceptos tradicionales, como el concepto de frontera, el

concepto de atribución fehaciente de un hecho, e incluso hasta el concepto mismo de ataque.

3.1.1 El problema de la dimensión espacial

El quinto dominio no se encuentra en un lugar físico determinado. Si bien podemos establecer dónde se encuentran físicamente los servidores, enrutadores y conexiones; dicha ubicación física resulta irrelevante en cuanto a su valor dentro del mundo virtual. Sin ir más lejos, Estonia posee una copia de resguardo de toda la información crítica y confidencial de su sistema informático de gobierno en Luxemburgo. Es lo que Estonia ha denominado una *data-embassy* [24].

Esta situación podría plantear el siguiente escenario: un ciberatacante bloquea los servicios de comunicación en Luxemburgo. ¿Podría considerarse, además, un ataque a Estonia? Por su parte los Estados Unidos de América, Rusia y China, entre otros, han creado edificios inteligentes que replican los datos como una medida de seguridad.

En el quinto dominio los bienes son intangibles y no poseen una ubicación espacial. En consecuencia los intereses de un país no están limitados al interior de sus fronteras. La ausencia de fronteras está reflejada en la reciente Estrategia Nacional de Ciberseguridad de España, donde dice: "Las ciberamenazas [...] afectan a la práctica totalidad de los ámbitos de la Seguridad Nacional, como son la Defensa Nacional, la seguridad económica, o la protección de infraestructuras críticas, entre otros, y no distinguen fronteras" (España, Estrategia Nacional de Ciberseguridad, 2019, págs. 23-24).

El problema de la ausencia de fronteras en el quinto dominio lo refleja Streltsov al analizar la Carta de las Naciones unidas:

> Por lo tanto, la ausencia de una definición clara de "territorio" en relación con el ciberespacio contribuye a las lagunas en el derecho internacional de seguridad. El párrafo 4 del artículo 2 de la Carta de las Naciones Unidas exige que todos los estados se abstengan de la amenaza o el uso de la fuerza contra la integridad territorial de otro estado. Se da a entender que existe un territorio físico sujeto a la

[24] Más información acerca de la embajada digital de Estonia disponible en https://e-estonia.com/estonia-to-open-the-worlds-first-data-embassy-in-luxembourg/, consultado el 2 de mayo de 2020.

> jurisdicción del estado y una frontera formal que separa ese territorio de otros estados. Sin embargo, no existen conceptos como frontera nacional y territorio en el ámbito de la información. Un estado podría considerar que toda la infraestructura de información global (o una parte de la misma) es su propio territorio, reclamar jurisdicción sobre los elementos relevantes de la infraestructura de información y, sobre esta base, tomar medidas para defender estos elementos. (Streltsov, 2007, pág. 11)

Por su parte, Jesús Sánchez Reguera afirma que:

> La regulación no será fácil debido a las características de esta realidad virtual. A la ya citada ausencia de fronteras (que acerca a las personas pero también a los delincuentes) y a la dificultad de identificar a los que están ciberactuando con intenciones maliciosas, habría que sumar la rápida difusión de las acciones (pero no necesariamente de los efectos), son prueba de la dificultad de su normalización. (Reguera Sánchez, 2015, pág. 6)

El Dr. Luis María González Day en su tesis doctoral, afirma respecto a la incumbencia territorial de las fuerzas armadas que:

> La Ley de Defensa, tal como se dijo, fue sancionada en 1988 pero no tuvo reglamentación durante 18 años hasta que en 2006 la Ministra Garré, durante la presidencia de N. Kirchner, estableció un límite [...] entre seguridad y defensa, que prohíbe taxativamente la participación de la esfera militar en incumbencias de seguridad, dejando una brecha aprovechable por organizaciones terroristas de carácter internacional. Incluso va más allá, fijando a las fuerzas armadas de terceros países como únicos adversarios de las Fuerzas Armadas Argentinas. (González Day, 2017, pág. 267)

Esta observación se aplica en el mismo sentido para las ciberoperaciones en el quinto dominio, donde la utilización del criterio de incumbencia geográfica es una tarea sumamente difícil. Más aún teniendo en cuenta el incremento de la participación de actores no estatales, como lo expresa Robles Carrillo:

> [en el quinto dominio] ha aumentado la presencia y el protagonismo de los agentes no estatales y [...] se ha incrementado hasta límites inimaginables su capacidad para actuar en el marco internacional en todos los ámbitos, incluido, el uso de la fuerza. Por otra parte [el arma cibernética se caracteriza por tener] la mayor accesibilidad y disponibilidad del medio cibernético; la variedad y diversidad de operativos; y la multifuncionalidad de las acciones cibernéticas. (Robles Carrillo, 2016, pág. 8)

3.1.2 El problema de la atribución u origen cierto

El segundo obstáculo es la problemática de la atribución, esto es, el determinar fehacientemente el origen de un ataque.

Una de las características del quinto dominio es su tolerancia a fallos. Sus protocolos de comunicación, en las diversas capas OSI [25], están preparados para que la comunicación en la red continúe aún, cuando se presenten fallos en algún punto de ésta. Una de las consecuencias de esta funcionalidad es que la comunicación entre dos puntos de la red, que atraviesa varios nodos, puede realizarse a través de diferentes rutas lo que implica que los nodos intermedios pueden variar. Esto hace que no siempre sea una tarea sencilla rastrear el origen de una comunicación; y más aún si el emisor de la comunicación desea mantenerse anónimo. Como dice William Banks:

> En el dominio cibernético, la atribución significa "identificar al agente responsable de la acción". Debido a que Internet facilita las comunicaciones anónimas y “no fue diseñado con el objetivo de disuasión en mente,” atribución de intrusiones cibernéticas puede ser un reto, especialmente cuando los explotadores elaboran sus intrusiones para confundir a la búsqueda de quién es el responsable. (Banks, 2017, pág. 1492)

En el mismo sentido, Streltsov afirma que:

> Otro factor complicado es cómo identificar de manera confiable al agente de un ataque de información. Es técnicamente desafiante localizar el lugar físico de donde

[25] El modelo de capas OSI (modelo de Interconexión de Sistemas Abiertos, por sus siglas en inglés) establece una estructura d e 7 capas para las actividades de red. Cada capa tiene asociados uno o más protocolos para la transferencia de datos.

se origina tal acto. Pero incluso si el origen de un ataque se puede localizar dentro de un estado en particular, sería difícil determinar si el atacante estaba actuando de manera individual, o en nombre de una organización criminal, el gobierno o las fuerzas armadas. En tales casos, el presunto autor de un acto agresivo podría ser acusado falsamente en lugar de ser verdaderamente identificado, como lo han demostrado los acontecimientos recientes. (Streltsov, 2007, pág. 11)

Y si tenemos en cuenta la velocidad con la que estos ataques se producen y la magnitud de su daño a pesar de su corta duración, concluiremos que intentar determinar el origen de un ataque como condición ineludible para determinar qué fuerza responderá ante el mismo tiene como consecuencia la inacción o, en el mejor de los casos, la respuesta tardía sin efecto alguno. Según lo declarado por el ex fiscal general adjunto de la División de Seguridad Nacional de los Estados Unidos, John Carlin:

> Atribuir actividad en Internet es un desafío. Los *hackers* a menudo enrutan[26] su tráfico malicioso a través de servidores proxy[27] de terceros que alquilan o comprometen. Un atacante en Europa del Este que usa una red de bots[28] de computadoras comprometidas en el Medio Oriente para llevar a cabo un ataque DDoS[29] (Denegación de Servicio distribuida, pos sus siglas en inglés) contra un objetivo estadounidense crea una falsa narrativa de que los actores ubicados en el Medio Oriente fueron responsables de ese acto. Incluso atribuir un ataque a la computadora de origen real puede ser insuficiente; podemos conocer la máquina utilizada para ejecutar un hack, pero no la persona o grupo que lo controló. Por lo tanto, la investigación técnica a menudo debe complementarse con inteligencia humana creíble. Y todo esto debe hacerse de manera rápida y consistente; La

[26] Enrutar: dirigir el tráfico de Internet a través de servidores específicos. Es una característica de Internet mediante la cual los datos son derivados a los servidores que están menos congestionados con el fin de lograr la mayor velocidad posible. En el caso de los hackers, configuran su tráfico (lo enrutan) para que atraviesen servidores que impidan que el origen real de su ubicación sea descubierto.

[27] Un servidor proxy es un servidor que recibe datos de un equipo de origen y los reenvía (como si fueran propios) hacia el equipo de destino. A través de ese proceso el equipo de origen permanece desconocido por el equipo de destino.

[28] Red de bots: es una red de computadoras y artefactos de IoT que han sido comprometidos por un hacker sin que sus propietarios lo sepan, con el fin de hacerles realizar diverso tipo de acciones. Se utilizan especialmente para generar ataques DDoS.

[29] El ataque DDoS (Ataque distribuido de denegación de servicio, por sus siglas en inglés) consiste en ordenar a una red de bots que realicen peticiones en forma constante y simultánea a un servidor determinado. Estas peticiones saturan al servidor que es blanco del ataque, el cual no puede atender las peticiones reales de los usuarios de Internet, para quienes el servidor atacado queda fuera de servicio.

> atribución es de poca utilidad si lleva años y solo identifica una pequeña fracción de atacantes. (Banks, 2017, pág. 1493)

3.1.3 El problema de las ciberoperaciones por debajo del umbral de la fuerza

No todas las acciones realizadas en el quinto dominio que afectan de alguna manera a una persona, entidad o país pueden ser consideradas ciberoperaciones o ciberataques. El Manual de Tallin 2.0 dedica la sección 5 de su Parte 1 a las "Ciberoperaciones no reguladas per se por el derecho internacional" (Schmitt & Vihul, 2017, pág. 186 y ss.). Su regla 32 establece 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". Esto implica que el ciberespionaje en tiempos de paz (es decir, no se incluye el ciberespionaje en tiempos de guerra) no viola el derecho internacional. El ciberespionaje es considerado tal cuando mediante el uso de capacidades cibernéticas se vigila, captura o filtra las comunicaciones, datos, u otra información transmitida o almacenada electrónicamente.

El Grupo Internacional de Expertos que redactó el Manual de Tallin acordó que el derecho internacional consuetudinario no prohíbe el espionaje *per se*. Por el contrario, varios Estados han autorizado por ley interna a sus servicios de seguridad a realizar actividades de espionaje, incluido el ciberespionaje. Sin embargo, si el ciberespionaje es realizado a través de medios que impliquen una violación al principio de soberanía o de no intervención, caería dentro de los actos violatorios del derecho internacional. Tal sería el caso si, para obtener información, se implementara un sistema que generase un daño en el Estado víctima; como, por ejemplo, la ejecución de un virus que dejara fuera de funcionamiento los sistemas de seguridad del Estado víctima con el fin de poder extraer la información.

Un notorio caso reciente de ciberespionaje fue el realizado por Rusia al partido demócrata de los Estados Unidos durante la campaña electoral de 2016. El 22 de julio de 2016, WikiLeaks filtró más de 18,000 correos electrónicos del Comité Nacional Demócrata (DNC por sus siglas en inglés) que evidenciaban una relación cercana entre el DNC y sus altos funcionarios con la campaña de Hillary Clinton, en desmedro del otro candidato del partido Demócrata, Bernie Sanders. Un poco más de 2 meses después, WikiLeaks comenzó a publicar más correos electrónicos enviados desde y hacia el jefe de

campaña de la Hillary Clinton. Esta filtración de correos duró hasta el final de la campaña. Estos correos generaron revuelo en los medios de comunicación y redes sociales por evidenciar tensiones internas dentro de la campaña de Hillary Clinton y opiniones desfavorables hacia ella como candidata. Esta operación que tuvo como fin erosionar a la candidata Clinton fue apoyada además mediante *fake news* propagadas en redes sociales.

La intrusión se atribuyó a *hackers* bajo el control del gobierno ruso, y así lo confirmó el gobierno de los Estados Unidos en un comunicado el 7 de Octubre de 2016:

> La Comunidad de Inteligencia de EE. UU. (USIC) tiene certeza de que el Gobierno ruso dirigió las filtraciones recientes de correos electrónicos de personas e instituciones estadounidenses, incluidas las organizaciones políticas estadounidenses. Las recientes revelaciones de presuntos correos electrónicos pirateados en sitios como DCLeaks.com y WikiLeaks y por el personaje en línea Guccifer 2.0 son consistentes con los métodos y motivaciones de los esfuerzos dirigidos por Rusia. Estos robos y divulgaciones tienen la intención de interferir con el proceso electoral de los Estados Unidos. Dicha actividad no es nueva para Moscú: los rusos han utilizado tácticas y técnicas similares en Europa y Eurasia, por ejemplo, para influir en la opinión pública allí. Creemos, con base en el alcance y la sensibilidad de estos esfuerzos, que sólo los altos funcionarios de Rusia podrían haber autorizado estas actividades. (Director of National Intelligence, 2016)

Sin embargo, la obtención de los correos electrónicos sin haber causado ningún daño físico ni informático a los sistemas del DNC encuadran dentro del espionaje, y por lo tanto no constituyen un acto ilegal internacional. Como señala Banks:

> Es importante colocar el pirateo del DNC en el contexto más amplio de las intrusiones cibernéticas. El pirateo del DNC claramente no fue un ataque armado o uso de la fuerza. [...] Tallinnn 2.0 afirma que los actos cibernéticos de estado a estado que son "perjudiciales, objetables o de otra manera hostiles" no son violaciones y no desencadenan la responsabilidad del Estado. [...] Las violaciones del derecho interno no pueden ser la base de un hecho internacionalmente ilícito, porque la existencia de una obligación legal está determinada únicamente por el

> derecho internacional. Basado en la evidencia disponible públicamente, el pirateo del DNC probablemente no fue una intervención ilegal. (Banks, 2017, pág. 1500)

Si la intervención rusa hubiera implicado la modificación de los resultados de la elección a partir de la alteración de las máquinas de votación, habría constituido una intervención ilegal por alterar un sistema informático. Pero el espionaje de correos electrónicos y su publicación a través de diferentes portales así como la propaganda mediante *fake news* no constituye una intervención ilegal conforme al derecho internacional. Como cita Banks:

> Un memorando de enero de 2017 del Consejo General del Departamento de Defensa a los Comandos Combatientes y otros abogados militares y civiles de alto rango en el Pentágono [...] concluyó que las actividades cibernéticas militares que están por debajo del uso de la fuerza umbral y no violan el principio de no intervención no están regulados en gran medida por el derecho internacional en este momento. (Banks, 2017, pág. 1501)

3.2 Aspectos legales en Argentina y la Comunidad Europea

Como hemos visto con el caso del correo epistolar y el correo electrónico, y en general en la evolución del derecho y la tecnología, resulta indispensable establecer legalmente las definiciones que permitan darle entidad jurídica a las acciones y entidades en el quinto dominio con el fin de poder delimitar adecuadamente los actores, los derechos y las obligaciones, y poder de esa manera establecer modos de acción legales ante las amenazas en dicho ámbito.

3.2.1 Marco jurídico Argentino

Argentina ha emitido una serie de normas de diverso calibre en relación a la ciberseguridad y la ciberdefensa que no han alcanzado aún el grado de especificidad requerido.

Podemos mencionar, por ejemplo, que en el año 2012 mediante Resolución 580/2011 de la Jefatura de Gabinete de Ministros se crea el Programa Nacional de Protección de Infraestructuras Críticas de Información y Ciberseguridad en el ámbito de la Oficina Nacional de Tecnologías de Información de la Subsecretaría de Tecnologías de

Gestión de la Secretaría de Gabinete de la Jefatura de Gabinete de Ministros, cuya finalidad era de:

> [...] impulsar la creación y adopción de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas del Sector Público Nacional, los organismos interjurisdiccionales y las organizaciones civiles y del sector privado que así lo requieran, y la colaboración de los mencionados sectores con miras al desarrollo de estrategias y estructuras adecuadas para un accionar coordinado hacia la implementación de las pertinentes tecnologías. (Resolución Nº 580/2011, 2011)

Por otro lado, el 28 de julio de 2017 mediante el Decreto N° 577 se creó el Comité de Ciberseguridad, integrado por los Ministerios de Seguridad y Defensa y por la Secretaría de Gobierno de Modernización (y presidido por ésta) con el objetivo de elaborar la Estrategia Nacional de Ciberseguridad. Posteriormente, mediante el Decreto N° 480/2019 se amplía el Comité de Ciberseguridad para integrar a los Ministerios de Relaciones Exteriores y Culto y de Justicia y Derechos Humanos y a la Secretaría de Asuntos Estratégicos de la Jefatura de Gabinete de Ministros. Este Comité de Ciberseguridad elaboró la Estrategia Nacional de Ciberseguridad de la República Argentina con fecha 24 de Mayo de 2019 (Resolución Nº 829/2019 - Estrategia Nacional de Ciberseguridad, 2019). Como parte del documento se enumeran los principios rectores que se tuvieron en cuenta o inspiraron su elaboración; y a continuación se establecen objetivos de tipo genéricos que enumeran una serie de acciones a realizar. Estos objetivos son 7:

> Objetivo 1) Concientización del uso seguro del Ciberespacio.
> Objetivo 2) Capacitación y educación en el uso seguro del Ciberespacio.
> Objetivo 3) Desarrollo del marco normativo.
> Objetivo 4) Fortalecimiento de capacidades de prevención, detección y respuesta.
> Objetivo 5) Protección y recuperación de los sistemas de información del Sector Público.
> Objetivo 6) Fomento de la industria de la ciberseguridad.
> Objetivo 7) Cooperación Internacional.
> Objetivo 8) Protección de las Infraestructuras Críticas Nacionales de Información.

El contenido de estos objetivos está compuesto de un sinnúmero de declaraciones de intenciones, tales como "Crear un plan programático de concientización" (objetivo 1), "Promover la formación de profesionales, técnicos e investigadores" (objetivo 2), "Ampliar y mejorar las capacidades de detección y análisis de ciberamenazas" (objetivo 4), "Promover el desarrollo de acuerdos a nivel regional e internacional" (objetivo 7), "Promover la definición, identificación y protección de las infraestructuras críticas nacionales de la información" (objetivo 8), "Articular los esfuerzos públicos-privados para la construcción de capacidades de detección, resguardo y respuesta" (objetivo 8). Estos objetivos no contienen definiciones atinentes a los elementos del quinto dominio, ni establecen criterio legal alguno.

Un avance relevante lo constituyó la Resolución 1523/2019 de la Jefatura de Gabinete de Ministros, que en ese momento encabezaba el Comité de Ciberseguridad, mediante la cual se abordó la definición del concepto de Infraestructura Crítica. En el Anexo I de dicha resolución se establece que:

> Las Infraestructuras Críticas son aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente. (Resolución Nº 1523/2019 - Infraestructuras Críticas, 2019)

La misma resolución establece el concepto de Infraestructuras Críticas de Información, el cual complementa al concepto anterior y cuya definición es muy necesaria para la ciberdefensa y la ciberseguridad. La resolución dice que: "Las Infraestructuras Críticas de Información son las tecnologías de información, operación y comunicación, así como la información asociada, que resultan vitales para el funcionamiento o la seguridad de las Infraestructuras Críticas" (Resolución Nº 1523/2019 - Infraestructuras Críticas, 2019). Este criterio no sólo abarca la infraestructura física, sino también la lógica (la información) asociados al funcionamiento de los sistemas y servicios.

Es necesario destacar en esta Resolución el mérito de haber establecido una definición tan precisa de un tema tan relevante y necesario para una nación, aún cuando haya sido enunciada recién en el año 2019. Sin embargo es también necesario decir que en el punto II del Anexo I de la Resolución se limita a considerar sólo a los ataques

informáticos como aquellos ataques susceptibles de impactar en las Infraestructuras Críticas, dejando de lado los ataques no informáticos o convencionales. Esta limitación no tiene razón de ser, ya que la definición de Infraestructuras Críticas enunciada no está limitada a las que dependen de servicios informáticos, como sí lo están las comprendidas dentro del concepto de Infraestructuras Críticas de Información. Dice, por ejemplo, que "Existe impacto para la vida humana, en aquellos casos en los cuales debido a la afectación de un sistema informático, se genere riesgo.." (Resolución Nº 1523/2019 - Infraestructuras Críticas, 2019), o que "Existe impacto económico para el país, en aquellos casos en los cuales debido a la afectación de un sistema informático se genere daño..." (Resolución Nº 1523/2019 - Infraestructuras Críticas, 2019), o que "Existe impacto en el ejercicio de las funciones del Estado, cuando debido a la afectación de un sistema informático, se afecte de manera sustancial..." (Resolución Nº 1523/2019 - Infraestructuras Críticas, 2019); y de la misma manera en todos los casos se define la existencia de impacto en las Infraestructuras Crítica a partir de un ataque a un sistema informático.

Esta resolución aborda también el aspecto de la soberanía y la integridad territorial en relación a las Infraestructuras Críticas de la siguiente manera:

> IMPACTO EN LA SOBERANIA NACIONAL:
> Existe impacto sobre la soberanía nacional, cuando mediante la afectación de un sistema informático se cuestione o restrinja el poder del Estado Nacional en el ámbito del territorio de nacional.
> IMPACTO EN MANTENIMIENTO DE LA INTEGRIDAD TERRITORIAL NACIONAL:
> Existe impacto en el mantenimiento de la integridad territorial nacional, cuando mediante la afectación de un sistema informático, se vulneren las fronteras territoriales, marítimas o espaciales de la nación.
> (Resolución Nº 1523/2019 - Infraestructuras Críticas, 2019)

El concepto de impacto en la soberanía queda definido a partir de la afectación del ejercicio del poder del Estado Nacional dentro del territorio; mientras que la integridad territorial se considera violada cuando mediante la afectación de sistema informático se producen efectos dentro de las fronteras físicas del territorio.

Otro importante hito en esta cuestión fue la Resolución Mº 1380/2019 del Ministerio de Defensa, donde establece la siguiente definición de ciberdefensa:

> Entiéndase por CIBERDEFENSA a las acciones y capacidades desarrolladas por el MINISTERIO DE DEFENSA, EL ESTADO MAYOR CONJUNTO y las FUERZAS ARMADAS para anticipar y prevenir ciberataques y ciberexplotación de las redes nacionales que puedan afectar al Ministerio de Defensa y al Instrumento Militar de la Defensa Nacional, como así también a las Infraestructuras Críticas operacionales soporte de los Servicios Esenciales de interés para la Defensa o a Infraestructuras operacionales soporte de procesos industriales de fabricación de bienes sensibles para la Defensa o que posibiliten el acceso a los activos digitales estratégicos adjudicados a su custodia. (Resolución Nº 1380/2019, 2019)

Además la resolución crea el Centro Nacional de Ciberdefensa en el ámbito de la Subsecretaría de Ciberdefensa, que funcionará en las instalaciones del Instituto de Investigaciones Científicas y Técnicas para la Defensa[30]. En dicho centro funcionarán el Centro de Respuesta ante Emergencias Informáticas del Ministerio de Defensa (CSIRT de Defensa), el Centro Inteligente de Operaciones de Seguridad (iSOC) del Comando Conjunto de Ciberdefensa del Estado Mayor Conjunto de las Fuerzas Armadas., y el Laboratorio de Análisis Cibernético (CyberLab)[31].

La función del Centro Nacional de Ciberdefensa es, conforme el texto del Anexo 4 de la resolución, la de:

> [...] asegurar la libertad de acción en este QUINTO DOMINIO evitando se vea afectada la confidencialidad, integridad y disponibilidad de la información que se transporta y/o procesa en las redes y sistemas TICs de las FFAA, el EMCO y el Ministerio de Defensa, y a su vez proteger las infraestructuras críticas de la Defensa Nacional, tanto las propias como las de interés para la Defensa. (Resolución Nº 1380/2019, 2019)

Resulta relevante en esta definición el hecho de que se está considerando a la información (un bien intangible) como algo que debe ser defendido junto con las

[30] Sitio oficial del Instituto de Investigaciones Científicas y Técnicas para la Defensa disponible en https://www.argentina.gob.ar/defensa/citedef, consultado el 18 de agosto de 2020.
[31] Las siglas son propias de la resolución citada.

infraestructuras críticas. Y dicha defensa no sólo implica evitar que sea dañado, es decir que se afecte su integridad; sino que también implica que no se viole su confidencialidad. En el mismo Anexo se filtra una definición de soberanía relacionada al ciberespacio, cuando el comienzo manifiesta que "A partir de conceptualizar al ciberespacio como un espacio soberano...", para más adelante establecer como una de las líneas de acción para cumplir sus objetivos el "Proteger la disponibilidad del ciberespacio como espacio soberano" (Resolución Nº 1380/2019, 2019). No queda aquí claro qué se define como soberanía en cuanto a lo que al quinto dominio se refiere. Parece no ser más que una extrapolación del concepto de soberanía del plano físico sin atender a las particularidades que el quinto dominio presenta, ya que si bien resulta claro el ejercicio de la soberanía sobre equipos informáticos ubicados en el territorio propio, no resulta tan claro cuando hablamos de información que está ubicada en lugares virtuales, o servicios que dependen de otros servicios brindados por otros países o por prestadoras virtuales, por poner un ejemplo.

Además de las normativas citadas, existen diversas Disposiciones de la ONTI referidas a la seguridad de la información, y decisiones administrativas y otras resoluciones de varios organismos públicos que abordan diferentes aspectos de la gestión pública en su intersección con el quinto dominio[32]. Todo este conjunto de normas no ha sido dictado en forma orgánica, sino más bien respondiendo a necesidades puntuales y, en muchos casos urgentes. No ha habido hasta el momento un planteo específico para definir conceptualmente la ciberdefensa y la ciberseguridad como marco general y específico, con sus entidades específicas.

En ese sentido, nos dicen Cornaglia y Vercelli en su trabajo "La ciberdefensa y su regulación legal en Argentina (2006-2015)":

> [...] la ciberdefensa no es fácilmente clasificable. Se encuentra aún en una etapa de expansión regulativa, de flexibilidad interpretativa y de amplio debate. Por ejemplo, entre otros puntos salientes, aún no está del todo claro qué significa la ciberdefensa y qué relaciones mantiene con el sistema de defensa nacional [...] En igual sentido, es importante avanzar sobre los siguientes cuestionamientos: ¿Qué actividades

[32] Un listado de las mismas está disponible en: https://www.argentina.gob.ar/jefatura/innovacion-publica/direccion-nacional-ciberseguridad/normativa, consultado el 16 de agosto de 2020.

> representan un ciberataque a nivel nacional, regional o internacional?, ¿Cuáles son las instituciones públicas y las autoridades competentes para su gestión? y ¿Cuenta la República Argentina con una legislación sistemática en materia de ciberdefensa? (Cornaglia & Vercelli, 2017, pág. 48)

Y concluyen su investigación, luego de realizar un profuso análisis de las leyes, decretos y resoluciones vigentes en Argentina, con la siguiente afirmación:

> Finalmente, la investigación permite concluir que el sistema legal argentino aún no dispone de una codificación general y sistemática sobre ciberdefensa. Una sistematización de los marcos jurídicos (y reglamentarios), así como una mayor definición de objetivos, competencias y funciones entre los diferentes organismos del Estado, podría ser de gran utilidad y ayudar a alcanzar múltiples objetivos estratégicos. Entre otros, a) definir qué significa y cómo debe entenderse el concepto de ciberdefensa nacional / regional; [...] c) favorecer procesos legislativos (del Congreso Nacional) que se orienten a regular tanto el sector público como las actividades críticas en manos del sector privado. (Cornaglia & Vercelli, 2017, pág. 59)

En este mismo sentido, pero en el marco de la seguridad interior y en relación a los delitos informáticos en cuanto a la adecuación de su tipificación penal, el abogado Diego Migliorisi dice:

> En el ámbito legislativo, es necesaria la adecuación de los tipos penales nacionales a las exigencias que presentan los avances tecnológicos. Esto se observa en varios países como los Estados Unidos, Gran Bretaña, Alemania, Francia, y en América del Sur, Chile, Venezuela y Ecuador.
> Pese a ello, cierto es que se advierte la falta de una teoría general sobre el punto. En ese sentido, media la necesidad de actualizar la legislación local, su coordinación en el ámbito regional y, por supuesto, global. (Migliorisi, 2015)

Argentina ha sancionado dos leyes que han sido de mucha utilidad para atacar algunas problemáticas del quinto dominio en el ámbito de la ciberseguridad, como la Ley de Delitos Informáticos (Ley 26388) y la Ley de Protección de Datos Personales (Ley

25326); y recientemente ha adherido al Convenio de Budapest sobre Ciberdelito [33]. La Ley 26388 tipifica los delitos más comunes en el ámbito de la ciberseguridad, desde la pornografía infantil hasta la intromisión en sistemas informáticos sin autorización o con por encima de la autorización otorgada, el daño de sistemas informáticos y el acceso indebido o no autorizado a comunicaciones electrónicas. Esta ley abarcó en su época toda la gama de delitos informáticos existentes, pero ya ha quedado desactualizada en cuanto a nuevos delitos como el secuestro de datos, también conocido como *ransomware*, que consiste en encriptar los datos de un sistema informático y pedir el pago de una suma de dinero para su desencriptación. Por su parte, la Ley 25326 establece los requisitos que debe cumplir una firma digital para tener la validez jurídica similar a la firma ológrafa y determina el valor probatorio *iuris tantum*[34] para dicha firma, en contraposición al valor probatorio para las firmas electrónicas, a las que define como aquellas firmas que se realizan mediante medios electrónicos pero que no cumplen con los requisitos establecidos por ley para ser consideradas firmas digitales, y por lo tanto obliga a quien la invoca presentar pruebas que avalen su veracidad.

Estos avances que impactan específicamente en materia de ciberseguridad no han resultado suficientes. El sistema legal argentino aún tiene mucho camino por recorrer en cuanto a definiciones esenciales para el quinto dominio tanto en relación a la ciberseguridad como a la ciberdefensa. Dentro de las definiciones que aún quedan por establecer se pueden mencionar las siguientes: ¿Qué es un ciberataque? ¿Qué es una ciberoperación? ¿Quiénes son los actores, partícipes necesarios, o partícipes secundarios que podrían ser sancionados? ¿Qué elementos son suficientes para determinar la atribución? ¿Cuáles son los elementos que determinan que un ataque es externo o interno? ¿Cuál es el alcance del concepto de soberanía en el quinto dominio?

3.2.2 Marco jurídico de la Comunidad Europea

A diferencia de la situación argentina, en la Comunidad Europea se ha recorrido un camino legislativo más largo en relación a la temática del quinto dominio. Es por eso que podemos observar más conceptos, definiciones y profundidad que la legislación nacional. Es por esto mismo que en muchos casos la legislación argentina ha tomado como modelo

[33] Mediante la Ley 27411, publicada en el Boletín Oficial el 15 de Diciembre de 2017, la Argentina adhirió (con reservas) al Convenio sobre Ciberdelito del Consejo de Europa, adoptado en la ciudad de Budapest, Hungría, el 23 de noviembre de 2001.
[34] Se refiere a las cosas que se presumen verdaderas salvo prueba en contrario.

la legislación europea especialmente en materias relacionadas con la evolución tecnológica. Tal es el caso de nuestra Ley 25326 de Protección de Datos Personales, para la cual se tomó como modelo la Directiva 95/46/CE de la Unión Europea.

Los países europeos no han sido la excepción en cuanto a que los ciberataques han sido los que han forzado la sanción de leyes relativas al quinto dominio. Tal fue el citado caso de Estonia en 2007:

> El caso de Estonia fue la primera vez que un país miembro solicitó apoyo a la OTAN por un ataque a sus sistemas de información y comunicaciones. En aquel momento la OTAN no disponía de un plan de acción para el caso de un ciberataque a un Estado miembro. El gobierno identificó con celeridad que estaban bajo un ataque de gran dimensión que podía derivar en una crisis de seguridad nacional. Formaron inmediatamente un equipo multifuncional para coordinar la respuesta; en el que se incluían expertos de la esfera técnica, política, militar, diplomática y jurídica [...] obligaron a la OTAN a reestructurar sus capacidades y crear equipos de respuesta inmediata frente a ciberataques considerada como una Nueva Amenaza al orden internacional los casos de Estonia y Georgia. (Fonseca, Perdomo, & Ansorena Gratacos, 2014)

En virtud de estos antecedentes revisaremos el resultado de la evolución legislativa a través de algunas de las normas relevantes en el continente europeo en relación a la ciberseguridad y la ciberdefensa, y cómo han definido jurídicamente las acciones y entidades en el quinto dominio.

El 16 de mayo de 2019 la Unión Europea estableció las directivas para enfrentar las agresiones cibernéticas debido a "la capacidad y disposición crecientes de agentes estatales y no estatales de perseguir sus objetivos mediante actividades cibernéticas malintencionadas" (Decisión del Consejo de la Unión Europea 7299/19 relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros, 2019). Dicha normativa comienza por establecer diversas definiciones sobre elementos del quinto dominio. En su artículo 1 define que debe considerarse los ataques como "externos" cuando se originen o cometan desde el exterior de la Unión, utilicen infraestructura fuera de la Unión, hayan sido cometidos por o con apoyo de personas que tengan actividad fuera de la Unión.

Es importante analizar aquí que el concepto es el más amplio posible, ya que la persona agresora puede estar dentro de la Unión pero originar un ataque desde equipos fuera de la Unión; o puede estar fuera de la Unión y originar un ataque con equipos dentro de la Unión; o con el sólo hecho de utilizar infraestructura fuera de la Unión o ser apoyado por personas físicas o jurídicas con actividades fuera de la Unión, ya queda configurado el ataque como externo. A continuación, el mismo artículo define el concepto de ciberataque, el cual se configura cuando existe una acceso o intromisión (obstaculización o interrupción, borrado, dañado o alteración) a sistemas de información o datos; o interceptación de datos. Y establece que los sujetos responsables son aquellos directamente responsables del ataque, también quienes brindan apoyo financiero, técnico o material; y todos los sujetos asociados con los involucrados, lo cual amplía el alcance de las sanciones a toda la red criminal, que en el quinto dominio suele ser compleja y extensa.

Por su parte, el Manual de Tallin 2.0 aborda esta temática en sus reglas 15 a 18:

> Regla 15 - Atribución de las operaciones cibernéticas por parte de los órganos del Estado. Las operaciones cibernéticas realizadas por órganos de un Estado, o por personas o entidades facultadas por la ley nacional para ejercer elementos de autoridad gubernamental, son atribuibles al Estado. (Schmitt & Vihul, 2017, pág. 87)

Esto implica un criterio amplio, en el cual cualquier actividad cibernética realizada por organismo de inteligencia, las fuerzas armadas y de seguridad, u otras agencias estatales implica la responsabilidad del Estado. También incluye, conforme la regla 42, a cualquier persona u organismo que tuviera el estatus de estatal conforme el derecho internacional; por lo cual un Estado no puede deslindar su responsabilidad (cuando la tuviere) simplemente mediante el desconocimiento de un organismo, o persona, o grupos de personas que actúen en ciberataques (Schmitt & Vihul, 2017, pág. 87). Esto impacta fundamentalmente en la responsabilidad generada por la actividad de los grupos denominados APT (Amenza Avanzada Persistente, por sus siglas en inglés). Los APT son grupos de *hackers* autodenominados independientes, pero que se sospecha son financiados por gobiernos. Ejemplos de estas sospechas son el APT28 o "Fancy Bear", el cual se sospecha que es financiado por el gobierno ruso; el APT1, sospechado de ser financiado por el gobierno chino; el APT 38 o "Lazarus Group" sospechado de ser financiado por el

gobierno de Corea del Norte; y el APT32 o "Ocean Lotus" sospechado de ser financiado por el gobierno de Vietnam[35]. También se considera responsable a un Estado cuando un miembro de un grupo u organismo estatal actúa en violación de las órdenes recibidas (Schmitt & Vihul, 2017, pág. 89).

La regla 17 reafirma lo establecido por la Regla 15, al definir la atribución en el caso de actores no estatales:

> Las operaciones cibernéticas realizadas por un actor no estatal son atribuibles a un Estado cuándo:
> (a) participa de conformidad con sus instrucciones o bajo su dirección o control; o
> (b) el Estado reconoce y adopta las operaciones como propias.
> Como regla general, las operaciones cibernéticas de personas o grupos privados no son atribuibles a los Estados. Sin embargo [...] la conducta de una persona o grupo de personas se considerará un acto de un Estado según el derecho internacional si la persona o grupo de personas actúa de hecho siguiendo las instrucciones de ese Estado o bajo su dirección o control al llevar a cabo el acto. (Schmitt & Vihul, 2017, págs. 94-95)

Finalmente, la Regla 18 define la responsabilidad de un Estado que asiste a otro Estado que realiza una operación cibernética:

> Con respecto a las operaciones cibernéticas, un Estado es responsable de:
> (a) su ayuda o asistencia a otro Estado en la comisión de un acto internacionalmente ilícito cuando el Estado proporciona la ayuda o asistencia conociendo las circunstancias del acto internacionalmente ilícito y el acto sería internacionalmente ilícito si fuera cometido por él;
> (b) el hecho internacionalmente ilícito de otro Estado que dirige y controla si la dirección y el control se realizan con conocimiento de las circunstancias del hecho internacionalmente ilícito y el acto sería internacionalmente ilícito si fuera cometido por él; o

[35] Una lista extensa de APT está disponible en: https://attack.mitre.org/groups/ y en https://www.fireeye.com/current-threats/apt-groups.html, consultados el 12 de abril de 2020. Es importante tener en cuenta que si bien las denominaciones coinciden en muchos casos, no existe un acuerdo global sobre las mismas. Esto se dificulta aún más por el anonimato en el cual estos grupos se escudan.

(c) un acto internacionalmente ilícito que obliga a otro Estado a cometer. (Schmitt & Vihul, 2017, pág. 100)

Respecto a la prueba requerida para determinar la atribución, el Manual de Tallin 2.0 determina criterios muchos más laxos que los requeridos en general por el derecho interno de los países. Establece que los Estados deben realizar una atribución *ex ante* previo a generar una respuesta, y dicha atribución podrá ser revisada *ex post facto*. Esto se debe a que un Estado puede estar sometido a situaciones en las que debe responder en un período muy corto de tiempo y sin la totalidad de la información. Respecto a la atribución *ex ante*, se considera que los Estados deben responder en forma razonable teniendo en consideración el tipo y la calidad de la información con la que se cuenta para realizar la atribución y actuando como esperaría que el otro Estado actuara si la situación fuera inversa. También debe considerarse la proporcionalidad de la respuesta, esto es, la gravedad del daño recibido en relación a la gravedad del daño provocado como consecuencia; y si el tipo de ciberoperación permite acumular más evidencia antes de realizar la atribución (Schmitt & Vihul, 2017, págs. 81-82). Un ejemplo de esto último podría consistir en derivar una intrusión cibernética a una red señuelo (conocida como *honeypot* [36]) al efecto de recopilar información sobre el atacante sin sufrir daño alguno.

En síntesis, el Manual de Tallin 2.0 asume que es inevitable cierto nivel de incertidumbre al momento de determinar la atribución de un ciberataque. Dada la velocidad del mismo, la gravedad del daño que causa, la información técnica con la que se cuenta sobre su origen, la existencia o no de otro tipo de información que ratifique o rectifique la información técnica (como inteligencia humana, inteligencia de fuentes abiertas, etc.) y otros factores accesorios, el Manual considera cada situación como única, y define como criterio la razonabilidad, lo cual en opinión de algunos expertos constituye una vara muy baja (Banks, 2017, pág. 1504).

Dado que la atribución puede incluir información secreta, aún en los casos de atribuciones comprobadas no siempre los países pueden hacer públicos los elementos que determinaron la atribución. Tal sería el caso en el que un espía infiltrado en un grupo APT

[36] Una *honeypot* es una red que aparece ante un ciberatacante como legítima y tiene como fin atraer los ataques dirigidos a redes reales. Este tipo de redes está aislada y monitoreada con el fin de recopilar información sobre el ciberataque y su perpetrador.

brindara información a un Estado sobre un ataque a ser realizado. La divulgación de dicha fuente de información pondría en riesgo la vida del agente y la estructura que permitió la infiltración en primera instancia.

Un hecho que se encuadra en ese escenario se produjo en el año 2019, cuando las Fuerzas de Defensas de Israel respondieron con un ataque misilístico a un ciberataque. Informaron medios periodísticos internacionales que en Mayo de 2019 Israel sufrió un ataque informático a sus servidores, y respondió mediante un ataque con misiles al centro ciber de Hamas en la Franja de Gaza [37]. Conforme la poca información que se filtró al respecto, Israel tenía identificado previamente el cuartel de los ciberatacantes de Hamas, por lo que la información técnica recabada sólo confirmó la información que previamente tenían provenientes de fuentes tradicionales.

Según palabras de quienes intervinieron en la operación "la operación cibernética fue un esfuerzo de colaboración entre la Unidad de élite 8200 de Inteligencia Militar, la Dirección de Teleprocesamiento de las FDI y el servicio de seguridad Shin Bet". Detalles sobre el ciberataque recibido por Israel no fueron revelados a la prensa para no dar a potenciales atacantes detalles sobre las capacidades cibernéticas de Israel [38].

Es en parte por escenarios como el citado que la prueba de atribución es más laxa que la que los tribunales nacionales exigen. En este sentido, afirma Banks:

> El derecho internacional, tal como se resume en Tallinn 2.0, requiere mucha menos prueba de atribución de lo que los abogados tradicionalmente esperan. Por supuesto, los abogados esperan rigurosos estándares para la prueba en juicios civiles y penales, no necesariamente en investigaciones de seguridad nacional, dependiendo del método de investigación. La prueba necesaria para la atribución cibernética que implica la responsabilidad del Estado no tiene por alcanzar un estándar válido en los tribunales. De hecho, la evidencia de atribución nunca puede

[37] Israel respondió a un ciberataque de Hamas con un ataque aéreo, disponible en https://www.washingtonpost.com/politics/2019/05/09/israel-responded-hamas-cyberattack-with-an-airstrike-thats-big-deal/, consultado el 21 de julio de 2020.
[38] Israel dice que frustró un ataque cibernético de Hamas durante la batalla del fin de semana, disponible en https://www.timesofisrael.com/idf-says-it-thwarted-a-hamas-cyber-attack-during-weekend-battle/, consultado el 21 de julio de 2020.

> hacerse pública debido a la sensibilidad de las fuentes de inteligencia y los métodos utilizados en la investigación. (Banks, 2017, pág. 1510)

3.3 Conclusiones parciales

En este capítulo hemos visto las principales problemáticas que en el campo jurídico plantea el quinto dominio, y de qué manera y en qué profundidad la Argentina, la Comunidad Europea, y el Grupo Internacional de Expertos que redactó el Manual de Tallin han abordado dicha problemática.

En Argentina el legislador se encuentra con una división tajante entre las áreas de seguridad y defensa basada en un criterio geográfico, el cual no es de aplicación en el quinto dominio debido a su naturaleza no especial, y un criterio de atribución, el cual hemos visto que es de muy difícil determinación en dicho ámbito.

Sin haber abordado las dificultades antedichas, el legislador argentino ha corrido siempre detrás del avance tecnológico, cubriendo algunos de los huecos jurídicos que se generaban con cada nuevo producto o servicio digital. La impronta de ese avance se ha caracterizado por la dispersión, en virtud de haberse constituido a partir de normativas de diferente nivel jerárquico que fueron emanadas de diversos organismos estatales; desde leyes sancionadas por el Congreso Nacional y resoluciones de nivel ministerial, hasta normativas de menor jerarquía provenientes de entes autárquicos. En consecuencia, Argentina no ha evidenciado hasta el momento un análisis y tratamiento específico y dedicado a la problemática del quinto dominio. Cabe destacar que si bien en los últimos años se han establecido definiciones esenciales como la de Infraestructuras Críticas, Infraestructuras Críticas de la Información, y se ha establecido la necesidad de proteger la información en el quinto dominio; estas iniciativas legales y/o doctrinarias han sido independientes, es decir, no han conformado parte de un todo orgánico destinado a definir qué elementos y categorías deben ser utilizados para abordar la problemática del quinto dominio. Podríamos afirmar que se ha partido de lo existente en el mundo físico (organismos y leyes) y se han adaptado a lo que, dentro del quinto dominio, les compete en cada caso en particular.

Por su lado, la Comunidad Europea ha iniciado más tempranamente la legislación en la materia y ha evidenciado un avance más estructurado en el abordaje de la problemática del quinto dominio; a partir de las normativas citadas como la Directiva 95/46/CE y la Decisión del Consejo 7299/19 citadas y la redacción del Manual de Tallin en sus versiones original y 2.0. Este último realiza un abordaje amplio e integral de la problemática del quinto dominio y constituye el más importante documento compilado en cuanto a conceptos jurídicos de ciberdefensa y ciberseguridad existente hasta el momento; por lo que puede tomarse como ejemplo a seguir no sólo en cuanto a los conceptos que del mismo emanan, sino también como ejemplo de aproximación completa y abarcativa de la temática.

Es por todo lo dicho que los aportes realizados en el siguiente capítulo tendrán como inevitable fundamento el marco jurídico argentino actual, que es el punto de partida; pero también se nutrirá de los conceptos utilizados en la Comunidad Europea y el Manual de Tallin.

Esta página ha sido dejada en blanco intencionalmente.

Capítulo IV - Aportes para el marco jurídico argentino

Las leyes inútiles debilitan a las necesarias.
Charles Louis de Secondat, Señor de la Brède y Barón de Montesquieu,
Del espíritu de las leyes, Libro XXIX.

Introducción

El análisis histórico de la evolución del derecho y la tecnología, el análisis de los hechos recientes en el quinto dominio y la legislación europea nos permiten proponer conceptos que definan aspectos esenciales de un marco jurídico para el quinto dominio que logren regular adecuadamente las interacciones en el ciberespacio en materia de ciberdefensa y ciberseguridad.

Estas propuestas se basan no sólo en la situación presente sino también en la proyección de un vector de evolución tecnológica que nace en el pasado, atraviesa el presente y se proyecta hacia el futuro. Se asume un futuro en el cual cada vez más los bienes y servicios considerados valiosos sean entidades que existan en el quinto dominio. Un futuro donde las relaciones entre las personas se desarrollen en mayor medida en dicho ámbito, o lo utilicen como factor determinante en sus actividades.

Como premisa básica para la definición del marco jurídico resulta necesario reconocer la entidad única y novedosa del quinto dominio, donde la normativa a aplicarse debe tener en cuenta el cambio veloz y permanente, así como su naturaleza no espacial[39]. Como ya anticipaba Anzit Guerrero en el año 2010:

> Como conclusión, considerando su particular objeto, sus categorías propias y la existencia de fuentes dedicadas, así como la importancia que revisten los bienes de

[39] Pensar en el quinto dominio como algo no espacial es tal vez el desafío más importante para la mente humana. Kant, en su "Crítica de la razón pura" determinó que todo pensamiento generado por un individuo se encuadran en un tiempo y un espacio. Tanto tiempo como espacio son para Kant categorías *a priori*, es decir, elementos que el individuo agrega a las percepciones externas e internas, dándole un contexto Eliminar el espacio como elemento es atacar una de las raíces de la estructura de pensamiento occidental.

> la sociedad de la información y su específico sustrato físico o ámbito en el cual se producen los hechos, es decir, el sustrato tecnológico, podemos determinar que el derecho informático ha devenido en una rama independiente del derecho, la cual, sin lugar a dudas, irá creciendo en importancia proporcionalmente a la injerencia de la tecnología en el quehacer humano. (Anzit Guerrero, Profumo, & Tato, 2010, pág. 13)

Hemos visto en el capítulo precedente que en los últimos años se han establecido algunas definiciones esenciales relativas al quinto dominio, pero de manera inorgánica. No se ha partido de concebir al quinto dominio como un espacio que requiere elementos y categorías propias, y con el mismo peso que los cuatro dominios precedentes. Considero necesario revertir esa idea y definir elementos adecuados para su gestión y a partir de allí se adapten o se creen los organismos que se avoquen a la misma.

4. 1 Definiciones esenciales: Ciberoperación y ciberataque

Con el objeto de constituir un marco jurídico adecuado para la ciberdefensa y la ciberseguridad se deben distinguir claramente los conceptos de ciberoperación y ciberataque; ya que actualmente en la doctrina y la literatura en general estos términos son usados indistintamente. Esta distinción debe basarse en sendas definiciones que contemplen la relación entre ambos, basadas en los documentos internacionales de mayor relevancia.

La Unión Europea, en su directiva 7299/19 (Decisión del Consejo de la Unión Europea 7299/19 relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros, 2019) utiliza el concepto de ciberataque en sentido amplio, al incluir dentro de éste a la mayoría de las acciones ilegales en el quinto dominio, como el acceso o intromisión a un sistema informático, la interferencia en las comunicaciones, o el borrado de archivos.

Sin embargo, el Manual de Tallin 2.0 en su Regla 92 define al ciberataque como "una operación cibernética, ya sea ofensiva o defensiva, que se espera razonablemente que cause lesiones o la muerte de personas o daños o destrucción de objetos." (Schmitt & Vihul, 2017, pág. 415). Sobre este punto, aclara que:

> La limitación en esta Regla a las operaciones contra individuos u objetos físicos no debe entenderse como una exclusión de las operaciones cibernéticas contra datos (que son entidades no físicas) del ámbito del término ataque. Siempre que un ataque a datos previsiblemente resulte en lesiones o muerte de personas o daños o destrucción de objetos físicos, esas personas u objetos constituyen el "objeto de ataque" y, por lo tanto, la operación califica como un ataque. Además [...] una operación contra datos en los que se basa la funcionalidad de los objetos físicos a veces puede constituir un ataque. (Schmitt & Vihul, 2017, pág. 416)

Agrega el Manual que una operación no necesariamente requiere el efecto destructivo previsto para calificar como ataque. En apoyo a esto, cita la discusión sobre las minas terrestres en la cual se determinó que se configura un ataque cada vez que una persona es puesta en peligro por una mina establecida. De la misma manera, la introducción de malware o defectos a nivel de producción que se activan en un momento determinado o ante un evento determinado configuran un ataque cuando las consecuencias perseguidas alcanzan el umbral establecido en la Regla 92 (Schmitt & Vihul, 2017, pág. 419). De acuerdo a este criterio, la operación autorizada por Ronald Reagan en 1982 constituyó in ciberataque en términos modernos.

Por otro lado, para diferenciarlas de los ciberataques, el Manual de Tallin establece el concepto de ciberoperaciones. Es un concepto más genérico, el cual engloba a todas las operaciones ofensivas en el quinto dominio. En la primera versión del Manual de Tallin el enfoque se centró en las operaciones cibernéticas que ocurrían en el contexto de un conflicto armado. Sin embargo, en la versión 2.0 del Manual, que es la citada en este trabajo, se reconoce que los Estados tienen que lidiar a diario con problemas cibernéticos que se encuentran por debajo del umbral de uso de la fuerza. Por este motivo se buscó ampliar el alcance del Manual para incluir el derecho internacional público que rige las operaciones cibernéticas durante tiempos de paz. Con esa intención, la versión 2.0 del Manual se denominó "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations" (Manual de Tallin 2.0 sobre la ley internacional aplicable a las ciberoperaciones) en contraposición a la primera versión, denominada "Tallinn Manual on the International Law Applicable to Cyber Warfare" (Manual de Tallin 2.0 sobre la ley internacional aplicable a la ciberguerra). Y en su glosario el Manual de Tallin 2.0 define a

las ciberoperaciones como "el empleo de capacidades cibernéticas para lograr objetivos en o a través del ciberespacio" (Schmitt & Vihul, 2017, pág. 564)

Estos conceptos tienen, en consecuencia, una relación de género a especie. Mientras que una ciberoperación se define como el empleo de capacidades cibernéticas para lograr objetivos en o a través del ciberespacio; un ciberataque es una ciberoperación, ya sea ofensiva o defensiva, que razonablemente se espera que cause lesiones o la muerte de personas o daños o destrucción de objetos.

Como hemos visto anteriormente, una ciberoperación puede incluso no ser ilegal conforme al derecho internacional, como los casos generales de ciberespionaje o el caso particular del hackeo al DNC. Un ciberataque, en cambio, genera un daño físico, como el producido en la planta nuclear iraní de Natanz por el virus Stuxnet.

El Manual de Tallin también define un concepto más amplio que ciberoperación, que la incluye. Es la ciberactividad, que consiste en "cualquier actividad que implique el uso de infraestructura cibernética o emplee medios cibernéticos para afectar el funcionamiento de dicha infraestructura" (Schmitt & Vihul, 2017, pág. 564). Es citada en este trabajo no por su relación con la ciberdefensa y la ciberseguridad, sino por definir en forma clara la actividad realizada por una persona en el quinto dominio; y ser el concepto genérico del cual se desprenden la ciberoperación y el ciberataque. Es por ello que esta definición también debería adoptarse en nuestro ordenamiento jurídico.

Como conclusión, resulta necesario para el marco jurídico argentino establecer el alcance de las actividades en el quinto dominio conforme el criterio adoptado en el Manual de Tallin, mediante la distinción de las ciberoperaciones y ciberataques con el fin de que dicha terminología permita adecuar nuestro marco jurídico a los conceptos internacionales de mayor aceptación; lo cual no sólo permitirá establecer una terminología común con la legislación internacional, sino que le dará al derecho interno una relevancia ponderada adecuadamente a las operaciones en el quinto dominio. Asimismo, el término ciberactividad debería ser adoptado, tal como lo define el Manual de Tallin, como concepto jurídico que defina las actividades de las personas (físicas y jurídicas) en el quinto dominio. Estos tres términos quedan relacionados en el siguiente cuadro:

<table>
<tr><td colspan="3">Ciberactividad</td></tr>
<tr><td rowspan="3">Cualquier actividad que implique el uso de infraestructura cibernética o emplee medios cibernéticos para afectar el funcionamiento de dicha infraestructura</td><td colspan="2">Ciberoperación</td></tr>
<tr><td rowspan="2">Empleo de capacidades cibernéticas para lograr objetivos en o a través del ciberespacio</td><td>Ciberataque</td></tr>
<tr><td>Una ciberoperación que se espera razonablemente que cause lesiones o la muerte de personas o daños o destrucción de objetos</td></tr>
</table>

De la misma manera que en la mayoría de las leyes relacionadas con el quinto dominio (como las citadas Ley 26388 de Delitos Informáticos y Ley 25506 de Firma Digital) comienzan con definiciones de los términos utilizados; los conceptos de ciberactividad, ciberoperación y ciberataque deberán ser incluidos como definiciones iniciales dentro del sistema legislativo que contemple esos criterios.

4.2 Atribución

Como hemos visto, los juristas internacionales están de acuerdo en considerar que el elemento de atribución en el quinto dominio con el fin de permitir una respuesta cibernética es más laxo que el requerido en los tribunales judiciales, debido principalmente a la velocidad del ataque y la consecuente velocidad con la que debe responderse, y a la enorme dificultad de establecer con total precisión el origen de un ataque. Nuestro sistema jurídico debería adecuarse a la particular realidad del quinto dominio y contemplar como válida una respuesta inmediata basada en un proceso de atribución *ex ante* que permita detener un ataque aún, cuando esa respuesta implique inutilizar el o los equipos desde donde se origina dicho ataque. Como complemento del concepto de atribución debe definirse en forma restrictiva el alcance de una respuesta ante un ciberataque para que sea considerada válida, es decir, proporcionada en términos legales.

Al definir el marco de la respuesta válida se debería:

a) Establecer un marco de proporcionalidad entre el daño recibido y el daño infringido, en relación al daño mínimo necesario para hacer cesar el ataque.

b) Establecer el límite a partir del cual sea aceptable una respuesta en el plano físico ante un ataque cibernético, basado en el daño recibido, la ineficacia de la sola repuesta cibernética, y los elementos mínimos requeridos para establecer la atribución más específica correspondiente a una respuesta en el plano físico.

Al hablar del concepto de atribución, un párrafo aparte merece considerar la dificultad en establecer fehacientemente en el quinto dominio el origen de una ciberoperación.

Puede tomar un tiempo considerable determinar (y en muchos casos nunca se llega a saber con certeza) cuál es el origen real de una ciberoperación; o qué persona, personas, organizaciones o Estados lo llevaron a cabo. De allí que establecer un ámbito de incumbencia de las Fuerzas Armadas o las Fuerzas de Seguridad basados en si el origen del ataque es dentro de nuestras fronteras o fuera de nuestras fronteras, o si el atacante es una persona, grupo o Estado; no es de aplicación a la realidad del quinto dominio.

Hemos visto en este trabajo ciberoperaciones realizadas por Estados y por individuos o grupos, así como ciberoperaciones realizadas por individuos o grupos de las cuales se sospecha con un alto grado de certeza que fueron realizadas o patrocinadas por Estados. Los hechos demuestran que resulta prácticamente imposible realizar una atribución precisa de una ciberoperación en un tiempo útil.

La legislación argentina deberá rever esta división de incumbencias para las áreas de seguridad y defensa en lo relativo al quinto dominio, ya sea mediante la eliminación del requisito de exigir la definición de un origen basada en aspectos geográficos y de un tipo de atacante, con lo cual quedarían habilitadas indistintamente las Fuerzas Armadas o de Seguridad para actuar en este ámbito; o mediante la creación de una nueva ciberfuerza específica para el quinto dominio que no se enmarque dentro de los conceptos de seguridad y defensa a la cual, en consecuencia, no se le apliquen las limitaciones relativas al origen geográfico del ataque y la atribución. Esta última opción resulta además la más eficaz en términos de recursos humanos y económicos; y permite la especialización del personal en áreas de conocimiento y con esquemas de servicio y entrenamiento que son propias y exclusivas de la naturaleza del quinto dominio..

4.3 Soberanía

Como conclusión de lo expuesto en este trabajo podemos decir que el concepto de soberanía en el quinto dominio resulta más difuso que en el plano físico. La Estrategia Nacional de Ciberseguridad de España de 2019 define como características del quinto dominio la ausencia de soberanía y débil jurisdicción.

Al considerar los intereses nacionales, la ley de Defensa Nacional establece en su artículo 2º, que "La defensa nacional [...] tiene por finalidad garantizar de modo permanente la soberanía e independencia de la Nación Argentina, su integridad territorial y capacidad de autodeterminación; proteger la vida y la libertad de sus habitantes." (Ley N° 23554 de Defensa Nacional, 1988). En consecuencia, resulta imperioso definir el concepto de soberanía en el quinto dominio desde una perspectiva legal.

Como hemos visto, la Resolución 1523/2019 aborda los conceptos de Soberanía e Integridad Territorial al hablar de aquellas acciones que al afectar un sistema informático generen efectos dentro del territorio nacional o "cuestione o restrinja el poder el Estado Nacional en el ámbito del territorio nacional" (Resolución Nº 1523/2019 - Infraestructuras Críticas, 2019). De esta manera establece que implícitamente que un ataque informático afecta la soberanía sólo en esos casos. Sin embargo considero que dicha definición no resulta suficiente.

El concepto de soberanía es abordado por el Manual de Tallin al comienzo de su articulado, al definir que éste es aplicable al ciberespacio. A lo largo de su articulado va a definir los tres aspectos de la soberanía: la soberanía sobre la capa física, la soberanía sobre la capa lógica, y la soberanía sobre la capa social.

En primer lugar debe considerarse algo que, afirma el Manual, se evidencia por sí mismo: que el Estado ejerce su soberanía sobre la capa física del quinto dominio, es decir, sobre la infraestructura que le da soporte dentro de su territorio. (Schmitt & Vihul, 2017, pág. 14).

El Manual de Tallin aplica al V domino el concepto físico de soberanía ampliándolo a su naturaleza: "Para los propósitos de este Manual, las capas físicas, lógicas y sociales del ciberespacio están abarcadas por el principio de soberanía" (Schmitt & Vihul, 2017, pág. 12). La capa lógica está constituida por las conexiones existentes entre

los dispositivos, así como los programas que gestionan dichas conexiones; y la capa social comprende las actividades de las personas en el V domino, conforme al término ciberactividad definido anteriormente.

Si bien podría considerarse, como lo hizo Estonia, una ciberembajada donde almacenar información de resguardo; esta no es la única manera posible de aplicar el concepto de soberanía al quinto dominio, ni contempla la infinidad de casos en los cuales la información no se encuentra en un servidor en particular, sino que está "en la nube". Cuando hablamos de "la nube" nos referimos a una o más granjas de servidores[40] que almacenan información en un lugar que no es fijo, es decir, que puede estar en cualquier lugar físico aunque están en un único lugar virtual. Esto significa que, si bien la información siempre está en un lugar físico, ese lugar físico puede cambiar debido a necesidades de infraestructura sin que el usuario de los datos tome conocimiento del cambio.

Este cambio resulta invisible para el usuario o, como se dice habitualmente, es una gestión "transparente" de los servicios y la información, que tiene como finalidad ofrecer una forma más eficiente de acceso a los datos a pesar de los cambios en el entorno físico o lógico. Un ejemplo de lo antedicho es el servicio de Google. Google posee granjas de servidores en diversos lugares del mundo. Las consultas son respondidas por el servidor más disponible para el usuario, que puede ser el más cercano o el que esté sometido a menor carga de trabajo en ese momento. En consecuencia, una consulta puede ser respondida por un servidor en España y la siguiente, realizada unos segundos después, por un servidor en México. Para la gran mayoría de los usuarios esto es desconocido. Esto es porque Google se encuentra "en la nube". Esto implica que la ubicación física de un servidor o una granja de servidores no es una manera eficiente de determinar la soberanía en el quinto dominio.

Dado que la relevancia del quinto dominio, lo que lo constituye esencial en esta era, está dada por el valor de la información y las comunicaciones; una de las maneras de ejercer la soberanía en este ámbito consiste en la utilización de protocolos de encriptación

[40] Se denomina granja de servidores a un grupo de servidores que proveen uno o más servicios. Estas granjas pueden tener redundancia y/o dedicarse a procesos que requieran gran capacidad de procesamiento.

de las comunicaciones y de los datos almacenados. Esto otorga control y soberanía sobre la capa lógica.

Dice el Manual de Tallin:

> Por ejemplo, un Estado puede promulgar legislación que requiera que ciertos servicios electrónicos empleen protocolos criptográficos particulares, como el protocolo de Seguridad de la capa de transporte, para garantizar comunicaciones seguras entre los servidores web y los navegadores. Del mismo modo, un Estado puede exigir legislativamente firmas electrónicas para cumplir requisitos técnicos particulares, como la dependencia del cifrado basado en certificados o que los certificados incluyan cierta información, como su huella digital criptográfica, el propietario o la fecha de vencimiento. (Schmitt & Vihul, 2017, pág. 14)

La Argentina ha sancionado en el año 2001 la ley de firma electrónica. Dicha ley distingue la firma electrónica de la firma digital [41] y establece los requisitos para que una firma sea considerada digital. La firma digital tiene como principal característica jurídica el dar fe del contenido de un documento electrónico y de la identidad del firmante. A partir de la sanción de esta ley un documento firmado digitalmente hace presunción *iuris tantum*, lo que implica que quien afirme que un documento firmado digitalmente no fue firmado por el titular de la firma digital o su contenido fue adulterado, debe presentar evidencias para sostener dicha afirmación (Ley Nº 25506 de Firma Digital, 2001). Esta ley cubre sólo uno de los aspectos mencionados por el Manual de Tallin. Otro aspecto ha sido cubierto por la Ley de Protección de Datos Personales, que exige a quienes almacenen datos personales (Ley Nº 25326 de Protección de Datos Personales, 2000) y sensibles que tomen los recaudos técnicos necesarios para proteger dicha información.

Estas dos leyes han sido sancionadas de manera independiente, para atacar problemáticas puntuales, y no teniendo en mira resolver la cuestión de la soberanía en el quinto dominio.

[41] Es importante tener en cuenta que la ley argentina intercambia los términos de firma electrónica y firma digital respecto a la denominación internacional. Nuestra ley denomina firma electrónica a lo que en el resto del mundo se denomina firma digital; y denomina firma digital a lo que en el resto del mundo se denomina firma electrónica.

Argentina carece en la actualidad de legislación específica referida al quinto dominio respecto a medidas de seguridad y protocolos de encriptación que permitan garantizar la soberanía sobre los datos y las comunicaciones; y en contrapartida carece de legislación que determine de qué manera las comunicaciones y los datos pueden estar violando la soberanía lógica cuando estén en uso de la capa física soberana.

Sobre este último punto, los Estados Unidos sancionaron en el año 2001, poco después del atentado a las Torres Gemelas, una ley denominada USA PATRIOT, por el acrónimo *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*, (107th United States Congress, 2001) que introdujo modificaciones a la Ley de Vigilancia de Inteligencia Extranjera del año 1978 con el fin de proteger la seguridad de la población norteamericana al desenmascarar a terroristas internacionales presentes en suelo nacional a partir de datos e información en posesión de terceros o empresas, orientado especialmente al quinto dominio. En ese sentido, el artículo 215 de dicha ley dice:

> SEC. 215. ACCESO A REGISTROS Y OTROS ARTÍCULOS BAJO LA LEY DE VIGILANCIA DE INTELIGENCIA EXTRANJERA.
>
> Título V de la Ley de Vigilancia de Inteligencia Extranjera de 1978
>
> (50 U.S.C.1861 et seq.) Se modifica eliminando las secciones 501 a 503 e insertando lo siguiente:
>
> SEC . 501. ACCESO A DETERMINADOS REGISTROS COMERCIALES PARA INVESTIGACIONES DE INTELIGENCIA EXTERIOR Y TERRORISMO INTERNACIONAL.
>
> ‘‘ (a) (1) El Director de la Oficina Federal de Investigación o una persona designada por el Director (cuyo rango no será inferior al de Agente Especial Asistente a Cargo) puede realizar una solicitud para una orden que requiera la producción de cualquier cosa tangible (incluyendo libros, registros, papeles, documentos y otros artículos) para una investigación que tenga como fin proteger contra el terrorismo internacional o actividades de inteligencia clandestinas, siempre que dicha investigación de contra una persona de los Estados no sea realizada únicamente sobre la base de actividades protegidas por la primera enmienda a la Constitución.
>
> [...]

(C) (1) Tras una solicitud realizada de conformidad con esta sección, el juez ingresará una orden ex parte según lo solicitado, o según lo modificado, aprobando la divulgación de registros si el juez determina que la solicitud cumple con los requisitos de esta sección.

(2) Una orden bajo esta subsección no revelará que se emite a los fines de una investigación descrita en la subsección (a)

(D) Ninguna persona deberá revelar a ninguna otra persona (que no sea aquellas personas necesarias para producir cosas tangibles bajo esta sección) que la Oficina Federal de Investigación ha buscado u obtuvo cosas tangibles amparada en esta sección.

[...] (107th United States Congress, 2001)

Este artículo de la ley es el que llevó a la Junta del Tesoro de la Secretaría de Canadá a afirmar que:

> Bajo el artículo 215 de la Ley Patriota de los Estados Unidos, el FBI podría potencialmente obtener registros bajo el poder de sociedades ubicadas en los Estados Unidos de Norteamérica, o registros a los que tienen acceso empresas ubicadas en los Estados Unidos de Norteamérica, y exigir que las empresas no divulguen estas acciones. (Lecours, 2007)

Nos encontramos aquí ante un caso explícito de aplicación de la soberanía sobre la capa lógica del quinto dominio no desde una actitud pasiva de protección de datos y comunicaciones, sino desde la actitud activa de acceder a información que se encuentra dentro del ámbito soberano lógico de una nación, que podría constituir un peligro para los ciudadanos, dentro del marco de una investigación de inteligencia exterior o terrorismo internacional. El alcance de esta acción es sumamente amplio, según como afirma Lecours en relación a las facultades del Poder Judicial ante un requerimiento basado en el artículo 215:

> [...] los Tribunales en la práctica no tienen albedrío con relación a la emisión de la orden solicitada. De hecho, siempre y cuando se cumpla con los requisitos para la emisión de la orden (es decir, la existencia de una investigación en curso sobre actividades terroristas o de inteligencia secreta, llevada a cabo bajo las directivas del Procurador General), el Juez debe emitir la orden. Asimismo, las autoridades

> norteamericanas no tienen la obligación de probar causa probable (es decir, la existencia de hechos específicos que conducen a la creencia de que se cometió un delito o que está a punto de cometerse). Lo único que deben invocar las autoridades es el hecho de que la información a ser comunicada podría estar relacionada a una investigación en curso relativa a actividades terroristas o de inteligencia secreta; no es necesaria la prueba de un nexo real, probatorio. (Lecours, 2007)

Respecto a la soberanía sobre la capa social del quinto dominio, el Manual de Tallin define la soberanía dentro de la regulación legal de las ciberactividades de las personas dentro de su territorio:

> En cuanto a la capa social del ciberespacio, un Estado puede regular las actividades cibernéticas de quienes se encuentran en su territorio, incluidas las personas físicas y jurídicas. Por ejemplo, un Estado puede criminalizar la publicación de material como pornografía infantil o aquello que incita a la violencia en línea. Se debe advertir que la censura estatal o las restricciones a las comunicaciones y actividades en línea están sujetas a la legislación internacional de derechos humanos. (Schmitt & Vihul, 2017, pág. 14)

Podemos concluir que el aspecto de la soberanía en el quinto dominio debe definirse en sus tres aspectos: soberanía sobre la capa física, soberanía sobre la capa lógica y soberanía sobre la capa social; teniendo en cuenta que cada una de estas capas se apoya en la capa subyacente.

Nivel 3 - Capa Social
Nivel 2- Capa Lógica
Nivel 1- Capa Física

Con respecto a la capa física el concepto de soberanía no es diferente al establecido con anterioridad a la creación del quinto dominio. El mismo criterio es aplicable a la capa

social, en la cual las conductas de los individuos están regidas por las mismas leyes que las rigen en el mundo físico.

En relación a la capa lógica, que es tal vez la capa más relevante en cuando a novedad y valor del quinto dominio, el concepto de soberanía debe establecerse a partir de la protección de la información y las comunicaciones. Soberanía debe definirse, en este ámbito, como el control sobre los datos propios tanto en su transporte como en su almacenamiento. Así como en el espacio físico existen los puestos fronterizos que protegen el territorio de accesos no autorizados, en el quinto dominio deben existir protocolos de encriptación que protejan a los datos de accesos no autorizados.

En forma análoga a la Ley 23968 de Espacios Marítimos, que en su artículo tercero establece que "La Nación Argentina posee y ejerce soberanía plena sobre el mar territorial, así como sobre el espacio aéreo, el lecho y el subsuelo de dicho mar" (Ley Nº 23968 de Espacios Marítimos, 1991), una ley de similares características debe sancionarse con el fin de establecer la soberanía sobre la capa lógica en el quinto dominio.

Esta ley debe establecer claramente que el Estado ejerce soberanía sobre los datos en el quinto dominio, debe definir las políticas de seguridad sobre los datos bajo un esquema de actualización permanente, debe establecer con claridad bajo qué circunstancias y con qué alcances una orden judicial puede permitir revelar datos protegidos por un protocolo de encriptación, y debe determinar cuáles son las ciberactividades que violan el ejercicio de la soberanía en la capa lógica del quinto dominio.

4.4 Ciberarmas

Un elemento que aún no ha sido legislado en el mundo es el relativo a las ciberarmas. Asistimos actualmente a la distribución gratuita de programas para intrusión y sistemas de virus[42], troyanos[43] y ransomware[44] genéricos que pueden adaptarse por el usuario para sus objetivos particulares. En especial, en tiempos recientes, hemos visto

[42] Un virus es un programa que cuenta con capacidad de reproducción y tiene como finalidad causar un daño.
[43] Un troyano es un programa que tiene como finalidad otorgar acceso al atacante a un sistema informático. También son conocidos como RAT (*Remote Access Tool*, o Herramienta de Acceso Remoto).
[44] Un ransomware es un programa que encripta los datos de un sistema informático haciéndolos inaccesibles para el usuario, con la finalidad de exigir el pago de una suma de dinero para obtener la clave que permita desencriptarlos.

como programas de tipo ransomware han sido reutilizados por diversos cibercriminales y han causado daños económicos de envergadura en empresas y gobiernos.

Existen actualmente empresas privadas que desarrollan o adquieren de otros *hackers* ciberarmas, y las venden a gobiernos, fuerzas de seguridad estatales y agencias de inteligencia. Ejemplos son Hacking Team y NSO Group.

Hacking Team es una empresa italiana dedicada al espionaje web cuyas herramientas brindan acceso a documentación en computadores y celulares, que en 2015 fue hackeada. Dicha intrusión dejó al descubierto 400 gigabytes de información entre la que se encontraban los datos de sus clientes y la duración, precio y servicios incluidos en sus contratos. Se expuso que la empresa tenía como clientes a los gobiernos de México, Colombia, Chile, Ecuador, Honduras, Panamá, Marruecos, Nigeria, Sudán, Arabia Saudí y Egipto. También contaba entre sus clientes al departamento de Defensa de Estados Unidos, el FBI, la DEA y el Centro Nacional de Inteligencia de España, este último con un contrato de 6 años por 3,4 millones de euros. (Jiménez Cano, 2015)

Por su parte, NSO Group fue acusada recientemente de estar detrás de un fallo en WhatsApp que permitía espiar a los usuarios con sólo hacerles una llamada perdida.

Otra empresa dedicada a la fabricación y compra de ciberarmas es Zerodium. Esta empresa afirma que "Desarrollamos y compramos *exploits* [programas maliciosos] para las plataformas, aplicaciones y dispositivos más populares. Damos soporte a Windows, Linux, Mac, iOS, Android y también a cualquier tipo de servidor o aplicación de escritorio". Dar soporte, en este contexto, significa que sus herramientas son capaces de atacar esos sistemas operativos. Afirman también que "Nuestros clientes son Gobiernos occidentales en Europa y Norteamérica y usan nuestras capacidades para su seguridad nacional, solo para luchar contra el terrorismo y el crimen organizado o conducir operaciones de inteligencia, como siempre han hecho desde antes de Internet" (Bejerano, 2019).

Estas empresas, en sus contratos con los gobiernos y agencias gubernamentales, se mueven en un terreno legal. Pero la falta de legislación específica coloca en un plano indefinido las restricciones al accionar de dichas empresas cuando investigan y desarrollan una ciberarma y cuando llevan adelante su giro comercial. Esta falencia en la legislación incluye la falta de control en cuanto a la trazabilidad de las ciberarmas desarrolladas.

El primer problema que enfrentamos al hablar de ciberarmas es que, en el plano físico, las armas se distinguen entre armas convencionales y armas de guerra; siendo estas últimas altamente reguladas. En el quinto dominio las ciberarmas de cualquier magnitud están al alcance tanto de Estados como de individuos. Nos dice Robles Carrillo, en referencia al sistema legal español:

> Jurídicamente se ha operado estableciendo una distinción genérica entre los conceptos de "arma" y "arma de guerra" que responde a los paradigmas de un mundo físico donde se diferencia, conceptual y funcionalmente, entre actos criminales y acciones bélicas y donde siempre ha resultado más simple atribuir la autoría de los mismos, respectivamente, a los individuos y a los Estados.[...] Esta distinción no resulta operativa en el espacio cibernético por la naturaleza multifuncional de las acciones y dispositivos desarrollados en el mismo y porque, además, por su efecto igualador o reductor de las asimetrías, el ciberespacio capacita a muchos sujetos -y no sólo a los Estados- para acceder a un arma cibernética con una función bélica y no sólo criminal y para realizar acciones susceptibles de ser calificadas como acciones de guerra, ataques armados, agresiones o usos de la fuerza armada en el contexto internacional". (Robles Carrillo, 2016, pág. 13)

Las ciberarmas, al igual que las armas físicas, requieren una regulación particular en la cual no resulta aplicable la distinción entre los tipos de armas en función del daño realizado. En el quinto dominio los bienes y servicios tienen un alto valor *per se* además del valor que radica en las consecuencias de sus fallas en el mundo físico. Un arma cibernética "puede tener consecuencias más disfuncionales o disruptivas que destructivas y más temporales que permanentes. Ello obliga a superar el criterio de la capacidad destructiva" (Robles Carrillo, 2016, pág. 17) ya que dichas consecuencias disruptivas pueden traducirse en un enorme daño económico y social en una comunidad, como hemos visto en los ejemplos citados en este trabajo.

El concepto de arma cibernética no puede obtenerse a partir de la adaptación al quinto dominio del concepto tradicional de arma. Como concluye Robles Carrillo:

> El concepto de arma cibernética debería definirse desde una aproximación funcional por varios motivos: en primer lugar, por la naturaleza multi o polifuncional de las acciones cibernéticas y por la importancia que esa circunstancia imprime en el uso que se hace del medio o dispositivo cibernético y de la intencionalidad que subyace a ese uso; en segundo término, porque la calificación de una acción cibernética como acción armada en el sentido del Derecho internacional obliga a operar combinando los componentes subjetivo, material y teleológico porque va a depender no sólo de la acción en sí misma sino, también y muy particularmente, del autor, el destinatario, la intención y los efectos; y, en tercer lugar, no en orden de importancia, porque el concepto de arma cibernética debe ser un concepto funcional dinámico, en lugar de instrumental o estático, y capacitado, además, para absorber los potenciales resultados del avance tecnológico futuro en esta materia que, aun siendo todavía desconocidos, no pueden ni han de ser inesperados. (Robles Carrillo, 2016, pág. 18 y 19)

En consecuencia de lo antedicho, resulta necesario catalogar las ciberarmas de acuerdo a la capacidad de intrusión, distribución y daño; y establecer sanciones para quienes las creen, las posean o las distribuyan a título gratuito u oneroso; así como un agravante para quienes al cometer el delito informático lo realicen mediante el uso de una ciberarma, lo que podría aplicarse al art. 153 bis de Código Penal argentino, que tipifica el acceso indebido a cualquier sistema informático; al art. 157 bis del mismo cuerpo normativo que tipifica el acceso indebido a bases de datos; y al art. 183, segundo párrafo, que tipifica el daño informático. Además, quienes produzcan ciberarmas legalmente y para uso legítimo, como el de las Fuerzas Armadas y de Seguridad, o para empresas que se dedican a la seguridad informáticas, deberán estar registrados con el fin de garantizar el cumplimiento de estándares legales y de seguridad especiales, deberán estar sometidos a controles de auditoría y deberán establecer mecanismos de trazabilidad de las ciberarmas producidas.

En virtud de que una ciberarma puede utilizarse también para el conflicto armado, esta la legislación referida a las ciberarmas deberá dictarse teniendo en cuenta el Primer Protocolo Adicional a los Convenios de Ginebra, el cual establece que los Estados deben evaluar la legalidad de las nuevas armas utilizando los criterios establecidos en los siguientes artículos:

Artículo 35 - Normas fundamentales

1. En todo conflicto armado, el derecho de las Partes en conflicto a elegir los métodos o medios de hacer la guerra no es ilimitado.

2. Queda prohibido el empleo de armas, proyectiles, materias y métodos de hacer la guerra de tal índole que causen males superfluos o sufrimientos innecesarios.

3. Queda prohibido el empleo de métodos o medios de hacer la guerra que hayan sido concebidos para causar, o de los que quepa prever que causen, daños extensos, duraderos y graves al medio ambiente natural.

Artículo 36 - Armas nuevas

Cuando una Alta Parte contratante estudie, desarrolle, adquiera o adopte una nueva arma, o nuevos medios o métodos de guerra, tendrá la obligación de determinar si su empleo, en ciertas condiciones o en todas las circunstancias, estaría prohibido por el presente Protocolo o por cualquier otra norma de derecho internacional aplicable a esa Alta Parte contratante.

Artículo 51 - Protección de la población civil

1. La población civil y las personas civiles gozarán de protección general contra los peligros procedentes de operaciones militares [...]

2. No serán objeto de ataque la población civil como tal ni las personas civiles. Quedan prohibidos los actos o amenazas de violencia cuya finalidad principal sea aterrorizar a la población civil.

[...]

4. Se prohíben los ataques indiscriminados. Son ataques indiscriminados:

a) los que no están dirigidos contra un objetivo militar concreto;

b) los que emplean métodos o medios de combate que no pueden dirigirse contra un objetivo militar concreto; o

c) los que emplean métodos o medios de combate cuyos efectos no sea posible limitar conforme a lo exigido por el presente Protocolo;

y que, en consecuencia, en cualquiera de tales casos, pueden alcanzar indistintamente a objetivos militares y a personas civiles o a bienes de carácter civil.

[...]

> 5. Se considerarán indiscriminados, entre otros, los siguientes tipos de ataque:
> [...]
> b) los ataques, cuando sea de prever que causarán incidentalmente muertos y heridos entre la población civil, o daños a bienes de carácter civil, o ambas cosas, que serían excesivos en relación con la ventaja militar concreta y directa prevista.
> [...] (Comité Internacional de la Cruz Roja, 1977)

4.5 Inteligencia artificial

La velocidad y complejidad de las ciberoperaciones obliga a respuestas inmediatas que no pueden ser abordadas en forma eficiente por seres humanos, por lo cual se delega en sistemas de inteligencia artificial. Dicha respuesta puede ser estrictamente defensiva, como el bloqueo del tráfico proveniente de una o más IPs determinadas; u ofensiva, mediante la inhabilitación a través de una ciberarma del sistema informático que origina la ciberoperación. En este último supuesto el marco jurídico debe definir claramente el escenario que configura la legalidad de una respuesta ofensiva automática realizada por un sistema de inteligencia artificial, y conformar así un marco de seguridad jurídica para los desarrolladores y técnicos que estén a cargo de la creación, implementación, entrenamiento y uso de ese tipo de sistemas defensivos-disuasorios.

Cabe destacar que la inteligencia artificial no sólo es aplicada al ámbito del quinto dominio. Actualmente se aplica para ayudar y potenciar la capacidad de ataque y respuesta de armas en el plano físico y en un futuro cercano no sólo restringirá parcialmente la intervención humana en su uso, sino que probablemente llegue a prescindir de ella. En estos casos, las propuestas de este trabajo respecto a las ciberarmas en el quinto dominio resulta aplicable también a la inteligencia artificial utilizada por el armamento en el plano físico.

La Inteligencia Artificial ha despertado un sinnúmero de emprendimientos en cuento a su regulación ética. Dice Brent Mittelstadt:

> En los últimos años, han surgido una gran cantidad de iniciativas público-privadas a nivel mundial para definir valores, principios y marcos para el desarrollo ético y el despliegue de la IA. [...] Hasta la fecha, al menos 84 de estas iniciativas de "Ética de IA" han publicado informes que describen principios éticos de alto nivel,

> principios, valores u otros requisitos abstractos para el desarrollo e implementación de IA. (Mittelstadt, 2019, pág. 1)

El Comité Internacional de la Cruz Roja plantea las problemáticas que podría acarrear el uso de la inteligencia artificial en sistemas de armas, partiendo de las preocupaciones éticas sobre la pérdida de la injerencia humana en las decisiones de usar la fuerza, y la difusión de la responsabilidad moral:

> Los estados también deben abordar las preocupaciones fundamentales sobre los sistemas de armas que pueden introducir imprevisibilidad inherente, como los que emplean algoritmos de aprendizaje automático de inteligencia artificial (IA).
> [...] El Comité Internacional de la Cruz Roja acoge con beneplácito los esfuerzos para mejorar la aplicación del Derecho Internacional Humanitario, incluso mediante la mejora de los mecanismos para revisar la legalidad de las nuevas armas. La realización de revisiones legales de sistemas de armas con autonomía en sus funciones críticas puede plantear desafíos, en particular con respecto a los estándares de previsibilidad y confiabilidad. (Grupo de expertos gubernamentales en "Sistemas letales de armas autónomas", 2018)

El Comité Internacional de la Cruz Roja aboga en el documento citado por acordar límites a la autonomía en los sistemas de armas, lo que implica límites en la implementación de sistemas de inteligencia artificial. Si bien sus razones pueden ser atendibles, la experiencia de las últimas décadas y la evolución citada en este mismo trabajo nos han demostrado que no es posible detener el avance tecnológico, y la evolución de la inteligencia artificial y su aplicación a todos los ámbitos del quehacer humano, incluyendo la ciberguerra, no será una excepción.

La problemática planteada respecto a la implementación de la inteligencia artificial en nuestro país se presentó en forma temprana en el año 2008 cuando se debatió la Ley 26388 de Delitos Informáticos. En las sesiones se tuvo que tener en cuenta la legalidad del desvío o la eliminación de un correo electrónico cuando no lo realiza una persona sino un

sistema automático como un antivirus o un sistema anti-spam[45]. El artículo finalmente sancionado establece que:

> Artículo 153: Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.
> En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

El término "indebidamente" en el artículo 153 del código Penal tiene como fin manifiesto dejar a salvo de la sanción penal los desvíos o eliminación de correos electrónicos o comunicaciones de otra naturaleza (como los mensajes en los sistemas de mensajería instantánea) realizados por sistemas de inteligencia artificial en forma automática y bajo criterios válidos. Es decir, no indebidamente.

En palabras de Anzit Guerrero:

> [...] la ley 26.388, cuando tipifica la violación del correo electrónico, incluye la expresión "indebidamente" en el tipo, para que no le queden dudas al intérprete respecto de requerir la finalidad dolosa del autor del delito, y evitar cualquier hermenéutica que pudiera tender a considerar comprendidos en el tipo a quienes, en procura de mejorar el servicio que prestan a sus usuarios, activan mecanismos de protección tales como antivirus, filtros o algoritmos de desvío de correo electrónico para evitar lo que se conoce como spam, o la recepción de correos no deseados por sus clientes. (Anzit Guerrero, Profumo, & Tato, 2010, págs. 108-109)

[45] Se denomina SPAM al correo electrónico no deseado, el cual generalmente es enviado en forma masiva con fines publicitarios.

Otro aspecto incipiente del uso de la inteligencia artificial que plantea debates éticos es el relacionado a los automóviles de conducción autónoma, también denominados *self-driving cars*. Quien desarrolle n sistema de inteligencia artificial para un automóvil de manejo autónomo deberá establecer cuáles son los criterios a adoptar ante situaciones de riesgo especiales, como el cruce imprevisto de uno o más peatones cuando la maniobra para evitar el daño a los peatones pone en riesgo la salud o la vida de los ocupantes del vehículo ¿Deberá utilizar un criterio numérico según el cual la acción a tomar dependerá de la cantidad de vidas en juego en la calzada y en el vehículo? ¿Deberá ponderar el grado de culpa del transeúnte? ¿Deberá ponderar la edad del transeúnte versus la edad de los ocupantes del vehículo? Si el escenario contempla que quien se cruza en el camino del vehículo es el hijo del conductor y el conductor sin lugar a dudas preferiría asumir él el riesgo antes que poner en peligro la vida de su hijo ¿Debería esto también tenerse en cuenta? Estas y otras variables que también podrían incluirse en la consideración hacen que este dilema ético respecto a los automóviles de conducción autónoma aún no tenga solución.

Esta problemática se aplica, *mutatis mutandis*, a la inteligencia artificial en las ciberarmas. En principio, la regulación legal deberá procurar que las ciberarmas que actúen mediante sistemas de inteligencia artificial consideren las precauciones en el ataque y los efectos del ataque establecidas en los artículos 57 y 58 del Protocolo I adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales del año 1977:

> Artículo 57 - Precauciones en el ataque
>
> 1. Las operaciones militares se realizarán con un cuidado constante de preservar a la población civil, a las personas civiles y a los bienes de carácter civil.
>
> 2. Respecto a los ataques, se tomarán las siguientes precauciones:
>
> a) quienes preparen o decidan un ataque deberán:
>
> i) hacer todo lo que sea factible para verificar que los objetivos que se proyecta atacar no son personas civiles ni bienes de carácter civil, ni gozan de protección especial, sino que se trata de objetivos militares en el sentido del párrafo 2 del artículo 52 y que las disposiciones del presente Protocolo no prohíben atacarlos;
>
> ii) tomar todas las precauciones factibles en la elección de los medios y métodos de ataque para evitar o, al menos, reducir todo lo posible el número de muertos y de

heridos que pudieran causar incidentalmente entre la población civil, así como los daños a los bienes de carácter civil;

iii) abstenerse de decidir un ataque cuando sea de prever que causará incidentalmente muertos o heridos en la población civil, daños a bienes de carácter civil, o ambas cosas, que serían excesivos en relación con la ventaja militar concreta y directa prevista;

b) un ataque será suspendido o anulado si se advierte que el objetivo no es militar o que goza de protección especial, o que es de prever que el ataque causará incidentalmente muertos o heridos entre la población civil, daños a bienes de carácter civil, o ambas cosas, que serían excesivos en relación con la ventaja militar concreta y directa prevista;

c) se dará aviso con la debida antelación y por medios eficaces de cualquier ataque que pueda afectar a la población civil, salvo que las circunstancias lo impidan.

3. Cuando se pueda elegir entre varios objetivos militares para obtener una ventaja militar equivalente, se optará por el objetivo cuyo ataque, según sea de prever, presente menos peligro para las personas civiles y los bienes de carácter civil.

4. En las operaciones militares en el mar o en el aire, cada Parte en conflicto deberá adoptar, de conformidad con los derechos y deberes que le corresponden en virtud de las normas de derecho internacional aplicables en los conflictos armados, todas las precauciones razonables para evitar pérdidas de vidas en la población civil y daños a bienes de carácter civil.

5. Ninguna de las disposiciones de este artículo podrá interpretarse en el sentido de autorizar ataque alguno contra la población civil, las personas civiles o los bienes de carácter civil.

Artículo 58 - Precauciones contra los efectos de los ataques

Hasta donde sea factible, las Partes en conflicto:

a) se esforzarán, sin perjuicio de lo dispuesto en el artículo 49 del IV Convenio, por alejar de la proximidad de objetivos militares a la población civil, las personas civiles y los bienes de carácter civil que se encuentren bajo su control;

b) evitarán situar objetivos militares en el interior o en las proximidades de zonas densamente pobladas;

c) tomarán las demás precauciones necesarias para proteger contra los peligros resultantes de operaciones militares a la población civil, las personas civiles y los

> bienes de carácter civil que se encuentren bajo su control. (Comité Internacional de la Cruz Roja, 1977)

Un aspecto de especial relevancia radica en la determinación legal de la responsabilidad en el caso del uso de inteligencia artificial en las ciberarmas. ¿Son responsables los usuarios de las ciberarmas? ¿Son responsables quienes las instalaron y configuraron? ¿Son responsables quienes entrenaron la inteligencia artificial? ¿Son responsables quienes diseñaron y programaron el sistema de inteligencia artificial?

> En el caso de una autonomía total de los sistemas de armas de IA sin ningún control humano, aquellos que decidan emplear sistemas de armas de IA, normalmente comandantes militares de alto rango y funcionarios civiles, tienen la responsabilidad penal individual por cualquier posible violación grave del Derecho Internacional Humanitario. Además, los Estados a los que pertenecen incurren en responsabilidad del Estado por violaciones tan graves que podrían atribuirse a ellos. (Li & Xie, 2019)

Como referencia puede tomarse el caso planteado en Argentina por María Belén Rodríguez respecto a la responsabilidad de los buscadores (Google y Yahoo!) cuando el resultado mostrado contiene información difamatoria para una persona. Este caso ha resultado emblemático porque fue el primero en llegar hasta la Corte Suprema de Justicia de la Nación, con audiencias públicas celebradas el 21 y 29 de mayo de 2014. En dicho caso se determinó que no existía responsabilidad objetiva de los buscadores, lo que implica que el efecto disvalioso o daño que pudiera causar la actividad de los buscadores cuando muestra al usuario los resultados de búsqueda no genera una obligación de resarcimiento a menos que se pueda demostrar que hubo culpa (acción u omisión involuntaria basada en la imprudencia o falta de cuidado) o dolo (intención) al provocar el daño generado. La resolución de la Corte Suprema estableció que la inteligencia artificial que constituía el algoritmo de búsqueda y selección de resultados no era responsable por el contenido que dichos resultados mostraba; y la responsabilidad surgía recién a partir de que la empresa era notificada del daño causado por su plataforma.

Esta definición no es trasladable en forma directa a la inteligencia artificial de las ciberarmas, pero es un punto de partida que permite comenzar a debatir hasta qué punto es

responsable un desarrollador o un usuario de un sistema de inteligencia artificial cuando los elementos externos de los que se vale, es decir, los elementos de los que se alimenta para tomar una decisión no están bajo su control.

En relación directa con la ética de la Inteligencia Artificial, las iniciativas al respecto sólo han producido "declaraciones vagas, basadas en principios y valores de alto nivel que prometer sr guías de acción, pero en la práctica brindan pocas recomendaciones específicas y no logran abordar tensiones fundamentales normativas y políticas contenidas en conceptos clave" (Mittelstadt, 2019). Las directivas de la Unión Europea con respecto a los sistemas de inteligencia artificial no escapan al mismo esquema de vaguedad, con conceptos como "agencia y supervisión humana", "robustez técnica y seguridad", "privacidad y gobernanza de datos", entre otros. Como afirma Ortega Klein "se está maniobrando mucho en torno a la ética, pero pocos hablan de verdad de cómo se aplica la IA. La proliferación de *guidelines* no acerca a cómo implementarlos" (Ortega Klein, 2020). En el mismo sentido, Mittlestadt dice:

> La gran diversidad de partes interesadas e intereses involucrados necesariamente empuja la búsqueda de valores y normas comunes hacia un alto nivel de abstracción. Los resultados son declaraciones de principios o valores basados en conceptos abstractos y vagos, por ejemplo, compromisos para garantizar que la IA sea "justa" o respete la "dignidad humana", que no son lo suficientemente específicos como para guiar la acción. (Mittelstadt, 2019, pág. 5)

El sistema legal argentino debe considerar que en un futuro no muy lejano habrá un auge de la industria de la inteligencia artificial; y en consecuencia deberá establecer leyes claras respecto a la responsabilidad de los creadores de sistemas de inteligencia artificial, los entrenadores y los usuarios de dichos sistemas, con el fin de evitar que el vacío legal al respecto desemboque en situaciones de injusticia, y evitar también que la falta de definiciones legales se convierta en un obstáculo para el desarrollo o la utilización de sistemas de inteligencia artificial dejando a la Argentina rezagada respecto al desarrollo del resto del mundo.

Esto último sería especialmente desfavorable en el ámbito de la ciberdefensa y la ciberseguridad, donde la evolución de la tecnología de las ciberarmas ya ha alcanzado un

nivel tal que sin la asistencia de sistemas de inteligencia artificial no es posible presentar una defensa eficaz antes las ciberoperaciones y los ciberataques.

La legislación a emitir deberá seguir el esquema legislativo aplicado en la Ley 26388 citada, en la cual la responsabilidad está claramente establecida al definir como punible sólo la conducta indebida. Seguir esta metodología, aún cuando la redacción tuviera que llegar a un nivel de detalle cercano a la casuística, será imprescindible para el desarrollo y uso de las ciberarmas y la inteligencia artificial que el marco legal esté claramente definido.

Conclusiones parciales

Resulta imperioso avocarse a la tarea legislativa de incorporar el quinto dominio a nuestro sistema jurídico con definiciones y terminologías claras. Pero esta incorporación no debe ser inorgánica ni como consecuencia de problemas inmediatos que surjan a causa de la incorporación funcional de una nueva tecnología. Tal como en su momento se hizo con la Ley 26388 ya citada, donde en primer lugar se definen los elementos propios del quinto dominio que competen a dicha ley, y luego se analizan en forma profunda elementos que hasta el momento se trataban de una manera (como la responsabilidad) para adaptarlos a la nueva realidad; la incorporación legal del quinto dominio debe surgir de una iniciativa específica, con el fin de crear un plexo normativo del cual se deriven luego las diferentes normas que particularmente requieran incorporar los diferentes organismos estatales.

Dicho plexo normativo debería iniciar con el establecimiento del concepto de acción en el quinto dominio, definiendo las acciones de manera tal que se pueda determinar claramente cuando una acción cae dentro del concepto de ciberactividad, ciberoperación o ciberataque.

También debería conformar el plexo normativo una redefinición del concepto de atribución en cuanto a su aplicación en el quinto dominio. La exigencia legal habitual para establecer la atribución sobre una acción no puede ser aplicada de manera eficaz en este ámbito. Hemos visto como la comunidad internacional acepta estándares más bajos de prueba de atribución, y al mismo tiempo estos estándares condicionan el tipo de respuesta

que habilitan a realizar en base a los elementos de atribución existentes y la magnitud del daño que dicha respuesta podría ocasionar.

Finalmente, en cuanto a las definiciones esenciales, debe redefinirse el término de soberanía con el fin de que contemple las capas física, lógica y social del quinto dominio, debido a la especial importancia económica y estratégica que dichas capas han adquirido en los últimos años. Una definición de soberanía que sólo contemple la soberanía sobre el espacio físico deja fuera del marco legal un ámbito en el cual las personas, las organizaciones privadas y el Estado realizan acciones diariamente.

Fuera del plexo normativo de definiciones esenciales, hay dos elementos que por su peso y proyección deben ser legisladas de manera inmediata. Las ciberarmas, que hace algunas décadas nacieron como simples virus informáticos, son hoy en día un elemento que, utilizado por particulares, grupos o estados, provoca graves daños económicos en el mundo y como tal deben ser reguladas análogamente a como son reguladas las armas físicas. Por otro lado, la inteligencia artificial conforma otro elemento de relevancia que en forma incipiente ha penetrado en nuestra vida cotidiana y en el funcionamiento de organizaciones y Estados, sobre el cual resulta imperioso legislar para determinar el alcance de la responsabilidad de los desarrolladores, implementadores, entrenadores y usuarios sobre los daños que dichos programas produzcan; de lo contrario, y dado que el avance tecnológico no se detendrá, se generarán situaciones que queden en un limbo jurídico, fallos judiciales injustos, y una burocracia judicial que afectará la investigación y desarrollo en este área, dejando al país en desventaja respecto a este importante avance tecnológico.

Conclusiones finales

Al comenzar este trabajo me propuse realizar aportes que contribuyeran a adaptar el sistema legal argentino a la realidad del quinto dominio en materia de seguridad y defensa, partiendo de la hipótesis que indica que este dominio requiere normas que especialmente contemplen su particular entorno y situaciones, es decir, un esquema legal específico que actualmente no es provisto por el sistema legal argentino. Previo al aporte, y con el fin de que el mismo fuera realista, en primer lugar tomé en consideración la manera en que el derecho se ha adaptado a los cambios tecnológicos en el último siglo; y en segundo lugar consideré la adaptación que han realizado la Argentina y otros países recientemente en la materia.

A partir de los casos históricos analizados he llegado a la conclusión de que la sociedad, cuando ha incorporado los avances tecnológicos, al mismo tiempo ha generado nuevas situaciones y nuevas formas de relaciones interpersonales que debieron ser abordados desde la ciencia jurídica. Pero el derecho ha demorado considerablemente en catalogar estos nuevos escenarios, incluso con posiciones muy diferentes a lo largo del tiempo, lo que produjo períodos de tiempo con lagunas legales o soluciones injustas o inapropiadas. Esto me permite aseverar que la falta de regulación adecuada sobre los nuevos elementos que han surgido hasta ahora y surgirán en el futuro en el quinto dominio llevará a situaciones de similar laguna legal e injusticia. Es importante, en consecuencia, considerar que las propuestas que se realicen no deben dejar de tener en cuenta la experiencia pasada en relación a la resistencia al cambio que en el ámbito jurídico se ha producido ante los avances tecnológicos en el último siglo.

Al analizar la situación en Argentina he encontrado que la división tajante entre defensa y seguridad ha presentado un obstáculo de considerable magnitud a la hora de intentar abordar el quinto dominio como un todo. En Argentina se habla por un lado de Ciberdefensa y por otro lado de Ciberseguridad. De allí que las áreas de defensa y seguridad han establecido normativas propias e independientes sobre lo que considero un ambiente único; y además estas normas hasta hace no muy poco tiempo han surgido como reacción a problemas puntuales y no han sido fruto del resultado de una estrategia de abordaje específico para el quinto dominio. Al realizar este trabajo he encontrado en la pluralidad de normas de diverso nivel jerárquico un obstáculo importante a la hora de

analizar la normativa local e intentar establecer cuáles son los criterios y conceptos vigentes. Este obstáculo ha reforzado la idea de la necesidad de establecer criterios genéricos que conformen un basamento legal para el quinto dominio. Por otro lado, considero que debe abordarse la cuestión de la necesidad y/o eficacia de separación entre Seguridad y Defensa, al menos en lo relativo al quinto dominio; y en qué medida sería posible superar dicha dicotomía. Abordar esta división, tan arraigada en nuestra historia y nuestra política, permitirá diseñar un esquema superador que se adapte a la realidad del quinto dominio en forma eficaz y eficiente.

Por su parte la Comunidad Europea, que ha comenzado el camino en el quinto dominio con mayor anticipación, al momento ha logrado constituir una aproximación legal específica en la redacción del Manual de Tallin 2.0. Considero que esta obra debe ser un punto de partida y modelo para un esquema legal local que aborde esta problemática.

En virtud de haber concluido que el avance en nuestro país respecto al ámbito legal sobre el quinto dominio es aún escaso y se ha dado a partir de diversas iniciativas individuales, he considerado adecuado focalizar los aportes de este trabajo en la definición de conceptos fundamentales que necesariamente deben ser definidos *a priori*, tales como los conceptos de ciberactividad, ciberoperación, ciberataque, atribución y soberanía. Estos conceptos son *conditio sine qua non* para el dictado de leyes más específicas que conformen un todo coherente. Además consideré necesario tratar aquellos elementos del quinto dominio cuya regulación requiere una acción inmediata, como la inteligencia artificial y las ciberarmas, debido a su importancia en el mundo actual y la urgencia del dictado de su regulación. Estos aportes, en tanto que novedosos, han sido dados desde un punto de vista doctrinario con el fin de poner sobre la mesa la necesidad de una aproximación jurídica específica al quinto dominio, con sus propias categorías; y con la intención de que estos aportes sean utilizados como punto de partida para que los legisladores los plasmen en un cuerpo normativo específico.

Del análisis realizado en este trabajo surge que la hipótesis principal planteada al comienzo del mismo es correcta, en tanto que no es posible aplicar los esquemas normativos preexistentes a la realidad del quinto dominio. En este sentido los ejemplos citados han demostrado que los intentos de forzar criterios y definiciones legales del mundo tradicional al quinto dominio no han resultado adecuados.

De la misma manera se ha corroborado la hipótesis secundaria a través del análisis realizado, motivo por el cual las aportes realizados para el marco jurídico tienen como fin ser el puntapié inicial para conformar un esquema legal específico que reduzca el riesgo de situaciones no contempladas y facilite acciones preventivas y reactivas eficaces en el ámbito de la ciberdefensa y la ciberseguridad.

Sin perjuicio del aporte realizado en este trabajo, la legislación argentina en materia de ciberdefensa y ciberseguridad aún tiene un largo camino que recorrer. Considero que tomar los modelos planteados en la Comunidad Europea y en el Manual de Tallin 2.0 sería acertado a la hora de generar normas puntuales que abarquen el plano de realidad virtual que denominamos quinto dominio, ya que estos modelos se han creado a partir de situaciones que pronto serán comunes en nuestro país (si no lo son ya); dado que la evolución de las actividades humanas en el quinto dominio es constante en todo el mundo y el vuelco de actividades desde el mundo físico hacia el quinto dominio no ha cesado de aumentar en los últimos 30 años.

Lamentablemente no existe en Argentina un cuerpo normativo similar al Manual de Tallin en cuanto a la ciberdefensa y la ciberseguridad. Las leyes que pueden citarse son (como indiqué más arriba) iniciativas mayormente independientes que cumplen una función específica; y las otras referencias al quinto dominio que se pueden encontrar se dan en el contexto de normas referidas a temáticas más generales (como la Directiva de Política de Defensa Nacional).

Legislativamente aún no se ha tomado el quinto dominio como una entidad digna de ser legislada en forma independiente. Esa es aún una asignatura pendiente para nuestro sistema jurídico, la cual deberá realizarse en un tiempo relativamente cercano a riesgo de que el empuje de la evolución tecnológica, como hemos visto que aconteció en el pasado, obligue una adaptación forzada y desordenada; especialmente si tenemos en cuenta que la importancia relativa de un dominio radica en el uso que se le da tanto en su plano social como económico. Esto se verifica cuando consideramos la importancia del espacio exterior en comparación con los tres dominios tradicionales. En este sentido, se ha visto como crecen en forma constante la cantidad de bienes y servicios que en el quinto dominio se comercian, y es al mismo tiempo cada vez más utilizado en el relacionamiento personal y social. Su importancia alcanzará, en un futuro no muy lejano, a rivalizar con los hasta ahora tres dominios convencionales, tierra, aire y agua; y es por eso que considero que

resulta urgente abarcarlo desde el punto de vista legislativo con una perspectiva propia. Esta perspectiva deberá estar fundada en los conceptos aportados en el último capítulo de este trabajo, que tienen como fin conformar los componentes básicos de construcción para un sistema legal específico sobre el quinto dominio.

Glosario

Base de Datos: en el ámbito informático, se refiere a la compilación ordenada de información que generalmente es gestionada por un programa específico, denominado "motor de base de datos". Los motores más utilizados con SQLServer y Oracle en el ámbito comercial, y MySQL en el ámbito del software libre.

Big Data: se refiere a la compilación y manipulación de muy grandes volúmenes de información, que generalmente exceden las capacidades de las Bases de Datos tradicionales y requieren programas específicos.

Ciberespacio: el ámbito que se conforma a partir de la interconexión de sistemas informáticos. Se conforma por la palabra "espacio" precedida por el prefijo ciber, creado por acortamiento del adjetivo cibernético, que forma parte de términos relacionados con el mundo de las computadoras u ordenadores y de la realidad virtual.

Ciberdelincuente: delincuente que actúa en el ciberespacio.

Ciberejército: ejército que actúa en el entorno ciberespacio.

Ciberterrorista: terrorista que actúa en el entorno ciberespacio.

Cross-Site Scripting (Secuencia de comandos cruzados): Es un ataque que consiste en enviar datos a un sistema informático (lo que se denomina "inyectar"), el cual lo ejecutará y presentará a los usuarios información cuyo objetivo final es el beneficiar al atacante. Como consecuencia el código inyectado podría, por ejemplo, engañar a la víctima para que ingrese su usuario y contraseña de manera tal que quedara en poder del atacante.

Denegación de Servicio (DoS, por sus siglas en ingles): es un ataque que se realiza contra un servidor con el fin de saturarlo y que deje de brindar servicios. Consiste

en enviar una gran cantidad de requerimientos en forma automatizada y constante, de modo tal que los requerimientos de usuarios legítimos no sean respondidos.

Denegación de Servicio Distribuida (DDoS, por sus siglas en ingles): con una técnica de ataque y resultado similar a la Denegación de Servicio, esta variante consiste en que los requerimientos son enviados desde cientos o miles de dispositivos, aumentando el volumen.

Enrutador: es un dispositivo informático que forma parte del sistema de interconexión de servidores. Se encarga de recibir información y enviarla por la ruta adecuado para que alcance el servidor de destino.

Gusano: unos de los primeros tipos de virus informáticos. Su particularidad consiste en que se distribuyen automáticamente dentro de una red. Sus fines van desde hacer colapsar un sistema informático hasta robar pequeñas cantidades de dinero en sistemas bancarios.

Malware: todo tipo de programa informático destinado a causar un daño. Es una denominación que se creó posteriormente a la de virus, e incluye otros tipos de programad dañinos, como el ransomware.

Phishing: es el envío de correos electrónicos en forma masiva a diferentes destinatarios con el fin de que, mediante un contenido engañoso, los destinatarios ejecuten una acción determinada en su sistema informático. Una de las formas más comunes consiste en enviar falsos correos de suspensión una de cuenta bancaria, con un enlace para supuestamente evitar esa suspensión. Dicho enlace no dirige al sitio del banco sino un sitio con la misma estética pero cuyo fin es almacenar las contraseña ingresadas por las víctimas.

Quinto dominio: es una de las formas de denominar al ciberespacio. Surge del ámbito de la defensa, donde se consideran los cuatro dominios de aparición anterior a la tierra, el aire, el mar y el espacio exterior.

Ransomware: es un tipo de malware que encripta la información de un sistema informático y emite un mensaje a la víctima en el cual le exige un pago en criptomonedas para obtener la clave que permita desencriptar los archivos. El término es la suma de *ransom* (término inglés que refiere al retener una persona y pedir rescate para su liberación) y software.

SCADA (Supervisión, Control y Adquisición de Datos, por sus siglas en inglés): comprende varios tipos de programas informáticos cuya finalidad es controlar sistemas industriales.

Servidor: computadora especialmente diseñada para brindar servicios, en contraposición a las computadoras personales cuyo finalidad esencial es ser utilizada por una persona. El ciberespacio se compone en gran parte por la interconexión de servidores.

Spearphishing: es una variante del phishing. Su particularidad es que está dirigido a una persona en particular, y el engaño está especialmente diseñado para esa víctima. Suele requerir acciones de inteligencia previa para diseñar un engaño efectivo.

SQL (Lenguaje de Consulta Estructurado, por sus silgas en inglés): es un lenguaje informático que permite trabajar con bases de datos. Es el más utilizado en el mundo en la actualidad.

SQL Inyection (Inyección SQL): es un tipo de ataque que consiste en enviar al sistema informático datos específicos (inyectar) que, al interactuar con la base de datos de dicho sistema, logran que se realicen acciones específicas en favor del atacante. En la mayoría de los casos el objetivo es lograr que el atacante adquiera privilegios de administrador sobre el sistema. En otros casos se ha logrado obtener información de la base de datos, o borrarla.

TIC: Tecnología de Información y las Comunicaciones. Se utiliza este término para referir a todos los bienes y servicios relacionados con el quinto dominio. Pueden denominarse como "las TICs" a las empresas cuyo giro comercial está relacionado con la tecnología y/o las comunicaciones.

Troyano: es un tipo de virus que, luego de infectar un equipo informático, abre un canal de comunicación con el victimario y le otorga el acceso y control del sistema. Su nombre se debe al caballo de madera que construyeron los griegos mediante el cual se infiltraron en Troya, descripto en la "La Ilíada" por Homero.

Virus: término de carácter general que referencia a cualquier programa informático malintencionado que se reproduce automáticamente y tiene como fin infectar distintos dispositivos para causar un daño o poner los mismos a servicio del victimario.

Web defacement: es un tipo de ataque que consiste en modificar el contenido de un sitio web con el fin de mostrar algún mensaje. Este tipo de ataque es utilizado generalmente por activistas de Internet con el fin de generar un mensaje político.

Wearables (dispositivos): comprende los dispositivos tecnológicos que se usan en el cuerpo o como su nombre en inglés lo indica, se "visten"; como por ejemplo las pulseras que miden los pasos y el ritmo cardíaco.

Bibliografía

Libros, revistas y artículos

Adkins, B. N. (Abril de 2001). The spectrum of Cyberconflict. From hacking to information warfare. What is law enforcement´s role? Maxwell Air Force Base, Alabama, EE.UU.

Amaral, A. C. (2014). La amenaza cibernética para la seguridad y defensa de Brasil. *Visión Conjunta - Nº 10* , 19-22.

Antezana de Guzman, P. (2012). Historia del derecho laboral. *Fides et ratio* , 67-78.

Anzit Guerrero, R., Profumo, S., & Tato, N. S. (2010). *El Derecho Informático - Aspectos Fundamentales.* Buenos Aires: Cathedra Jurídica.

Banks, W. (2017). State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0. *Texas Las Review Vol. 95* , 1487-1513.

Baretto, J. F. (2017). La defensa nacional y la estrategia militar de seguridad cibernética.

Barnes, I. A. (Diciembre de 2018). Implementation of active cyber defense measures by private entities: the need for an international accord to address disputes. Monterrey, California, EE.UU.: Naval postgraduate school.

Bejerano, P. G. (28 de Mayo de 2019). *Así se compran y venden las 'ciberarmas'*. Recuperado el 7 de Junio de 2020, de El País: https://elpais.com/tecnologia/2019/05/28/actualidad/1559031474_402185.html

Caro Bejarano, M. J. (2011). Alcance y ámbito de la seguridad nacional en el ciberespacio. *Cuadernos de Estrategia Nº 149* , 47-82.

Cea D' Ancona, M. Á. (1996). *Metodología Cuantitativa. Estrategias y Técnicas de Investigación Social.* . Madrid: Síntesis.

Clarke, R. A., & Knake, R. K. (2019). *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats.* Penguin.

Collier, D. (2011). *Comprender el seguimiento de procesos.* Political Science and Politics, 44, No. 4. .

Cornaglia, S., & Vercelli, A. (2017). La ciberdefensa y su regulación legal en Argentina (2006 - 2015). *URVIO - Revista Latinoamericana de Estudios de Seguridad* , 46-62.

de Vergara, E. *El derecho internacional y la seguridad cibernética.* Buenos Aires: Instituto de Estudios Estratégicos de Buenos Aires.

de Vergara, E. (2009). *Las diferencias conceptuales entre Seguridad y Defensa.* Buenos Aires: Instituto de Estudios Estratégicos de Buenos Aires.

Díaz, R. (24 de Febrero de 2020). *El Mundo*. Recuperado el 25 de Febrero de 2020, de https://www.elmundo.es: https://www.elmundo.es/tecnologia/2020/02/24/5e4fb4c3fc6c83821f8b4642.html

Dorfman, Z., Zetter, K., McLaughlin, J., & Naylor, S. D. (15 de Julio de 2020). *Yahoo News.* Recuperado el 16 de Julio de 2020, de Exclusive: Secret Trump order gives CIA more powers to launch cyberattacks: https://news.yahoo.com/secret-trump-order-gives-cia-more-powers-to-launch-cyberattacks-090015219.html

Dov Bachmann, S., & Gunneriusson, H. (2015). Russia's Hybrid Warfare in the East. The Integral Nature of the Information Sphere. *Georgetown Journal of International Affairs* , 198-211.

Duhigg, C. (16 de febrero de 2012). *The New York Times.* Recuperado el 25 de febrero de 2020, de https://www.nytimes.com: https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

El móvil, líder en el consumo de internet. (Noviembre de 2017). Recuperado el 11 de Octubre de 2019, de Think with Google: https://www.thinkwithgoogle.com/intl/es-es/insights/el-m%C3%B3vil-l%C3%ADder-en-el-consumo-de-internet/

Fonseca, C. E., Perdomo, I. L., & Ansorena Gratacos, M. (2014). El Manual de Tallin y la Aplicabilidad del Derecho Internacional a la Ciberguerra. *Revista de la Escuela Superior de Guerra Nº 588* , 127-145.

Fox, C., & Kelion, L. (16 de Julio de 2020). *BBC News.* Recuperado el 16 de Julio de 2020, de Coronavirus: Russian spies target Covid-19 vaccine research: https://www.bbc.com/news/technology-53429506

Freita Gómez, J. (Mayo de 2019). El Quinto Dominio: Una Amenaza Inusual y Extraordinaria para los Estados. Venezuela: Universidad de Defensa Nacional - Colegio Internacional de Estudios de Defensa.

González Day, L. M. (1 de Noviembre de 2017). La motivación del ciudadano para ingresar como Oficial a la Armada Argentina - Gonzalez Day. Buenos Aires, Argentina.

Grispo, M. B. (2017). Derecho internacional y seguridad cibernética. *Visión Conjunta Nº 16* , 65-68.

Grupo de expertos gubernamentales en "Sistemas letales de armas autónomas". (9 de Abril de 2018). *Towards limits on autonomy in weapon systems.* Recuperado el 7 de Junio de 2020, de Comité Internacional de la Cruz Roja: https://www.icrc.org/en/document/towards-limits-autonomous-weapons

Hernández Sampieri, R., Fernández Collado, C., & Bpatista Lucio, P. (2014). *Metología de la investigación.* México: Mc Graw Hill.

Hodgson, Q. E., Ma, L., & Marcinek, K. K. (2019). *Fighting Shadows in the Dark - Understanding and Countering Coercion in Cyberspace.* RAND Corporation.

HSU, J. (1 de Enero de 2018). *Wired.* Recuperado el 25 de Febrero de 2020, de https://www.wired.com: https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/

Jasper, S. (2018). *Strategic Cyber Deterrence: The Active Cyber Defense Option.* Rowman & Littlefield.

Jaunarena, H. (2015). Ciberseguridad y Ciberdefensa. *Centro de Estudios para la Defensa Nacional* , 10.

Jaunarena, H. (2018). La seguridad y la defensa en la Argentina del siglo XXI. *Anales 2018 - Tomo XLV* , 423-440.

Jiménez Cano, R. (7 de Julio de 2015). *La policía y el CNI, entre los clientes de una firma de 'hackers'*. Recuperado el 7 de Junio de 2020, de El País: https://elpais.com/politica/2015/07/07/actualidad/1436284983_731864.html

Keohane, R. (1993). *Instituciones internacionales y poder estatal.* Grupo Editor Latinoamericano. Colección estudios internacionales.

Krekel, B. (2009). *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation.* McLean: Northrop Grumman.

Lecours, A. p. (2007). LEY PATRIOTA DE LOS EE.UU. (USA PATRIOT ACT). *La Crónica Jurídica* .

Li, Q., & Xie, D. (2 de Mayo de 2019). *Humanitarian law and policy.* Recuperado el 05 de Junio de 2020, de Legal regulation of AI weapons under international humanitarian law: A Chinese perspective: https://blogs.icrc.org/law-and-policy/2019/05/02/ai-weapon-ihl-legal-regulation-chinese-perspective/

Lynn III, W. J. (2010). Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs* , 97-108.

Medvedev, S. A. (Marzo de 2015). Offense-defense theory analysis of Russian. Monterrey, California, EE.UU: Dudley Know Library / Naval Postgraduate School.

Migliorisi, D. F. (2015). *Crímenes en la web.* Buenos Aires: Del nuevo extremo.

Mittelstadt, B. (2019). Principles alone cannot guarantee ethical AI. *Nature Machine Intelligence* .

Ortega Klein, A. (2020). Geopolítica de la ética en Inteligencia Artificial. *Real Instituto Elcano* .

Ottis, R. (2008). Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective. *Proceedings of the 7th European Conference on Information Warfare and Security* , 163-168.

Pastor Acosta, O., Pérez Rodríguez, J. A., de la Torre, D. A., & Taboso Ballesteros, P. (2009). *Seguridad Nacional y Cberdefensa.* Madrid: Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones.

Pérez Colomé, J. (06 de Marzo de 2020). *Cuando la batalla tecnológica contra el coronavirus amenaza el derecho a la privacidad.* Recuperado el 07 de Marzo de 2020, de El País: https://elpais.com/tecnologia/2020-03-07/cuando-la-batalla-tecnologica-contra-el-coronavirus-amenaza-el-derecho-a-la-privacidad.html

Pessino, M. (15 de Nomviembre de 2017). Las políticas en ciberseguridad de la Organización del Tratado del Atlántico Norte (OTAN). Córdoba, Córdoba, Argentina.

Real Academia Española. (2005). *Diccionario Prehispánico de Dudas*. Recuperado el 1 de Marzo de 2020, de ciber-: http://lema.rae.es/dpd/srv/search?key=ciber-

Reguera Sánchez, J. (2015). Aspectos legales en el ciberespacio. La ciberguerra y el Derecho Internacional Humanitario. *Grupo de Estudios en Seguridad Internacional* , 1-30.

Robles Carrillo, M. (3 de Octubre de 2016). *El concepto de arma cibernética en el marco internacional: una aproximación funcional*. Recuperado el 14 de Marzo de 2020, de Instituto Español de Estudios Estratégicos: http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO101-2016_Arma_Cibernetica_MargaritaRobles.pdf

Sánchez García, F. (2012). El conflicto híbrido ¿Una nueva forma de guerra? *El enfoque multidisciplinar en los conflictos híbridos* , 11-24.

Schmitt, M. N., von Heinegg, W. H., & Boothby, W. H. (2013). *Tallin Manual.* Cambridge: Cambridge University Press.

Schmitt, M., & Vihul, L. (2017). *Tallin Manual 2.0.* Cambrigde: Cambridge University Press.

Schreier, F. (2012). On Cyberwarfare. *DCAF Horizon 2015 Working Papers* .

Segu-Info. (28 de Febrero de 2020). *Presuntos narcotraficantes liberados por un ransomware*. Recuperado el 29 de Febrero de 2020, de Segu-Info: https://blog.segu-info.com.ar/2020/02/presuntos-narcotraficantes-liberados.html

Sharma, A. (2010). Cyber Wars: A Paradigm Shift from Means to Ends. *Strategic Analysis* , 62-73.

Silvestrini, J. (3 de diciembre de 2019). *iProUP*. Recuperado el 25 de Febrero de 2020, de https://www.iproup.com: https://www.iproup.com/innovacion/8985-inventos-tecnologicos-tecnologia-negocios-innovadores-Seguridad-Ciudad-de-Buenos-Aires-uso-de-reconocimiento-facial

Streltsov, A. A. (2007). International information security: description and legal aspects. *Disarmament forum 3* , 5-13.

Terlato, A. N. (Agosto de 2018). Estrategia y decisiones en ambientes VICA: Implicancias de este entorno para las empresas. *Serie Documentos de Trabajo, No. 699* .

Tikk, E., Kaska, K., & Vihul, L. (2010). *International Cyber Incidents: Legal Considerations.* Tallinn: Cooperative Cyber Defence Centre of Excellence.

Ugarte, J. M. (2001). Los conceptos de defensa y seguridad en América Latina: sus peculiaridades respecto de los vigentes en otras regiones, y las consecuencias políticas de tales peculiaridades. Washington D.C., EE.UU.: Latin American Studies Association.

Van Creveld, M. (2007). *La transformación de la guerra.* Buenos Aires: José Luis Uceda.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review* , 193–220.

Normativa, fallos y declaraciones gubernamentales

Argentina

Autodesk, Inc. s/recurso de casación (Corte Superma de Justicia de la Nación Diciembre 23, 1997).

Decreto Nº 683/18 - Defensa Nacional. (23 de Julio de 2018). *Boletín Oficial de la República Argentina* . Buenos Aires.

Decreto Nº 703/2018 - DPDN. (31 de Julio de 2018). *Boletín Oficial de la República Argentina* . Buenos Aires, Argentina.

Decreto Nº 727/2006 - Defensa Nacional. (12 de Junio de 2006). *Boletn Oficial de la República Argentina* . Buenos Aires, Argentina.

Lanata, Jorge s/ Desestimación, 10.389 (CAMARA NACIONAL DE APELACIONES EN LO CRIMINAL Y CORRECCIONAL. CABA. Sala 6. 4 de Marzo de 1998).

Ley Nº 23968 de Espacios Marítimos. (5 de Diciembre de 1991). *Boletin Oficial de la República Argentina* . Buenos Aires, Argentina.

Ley N° 23554 de Defensa Nacional. (13 de Abril de 1988). *Boletín Oficial de la República Argentina* . Buenos Aires, Argentina.

Ley Nº 23968 de Espacios Marítimos. (5 de Diciembre de 1991). *Boletin Oficial de la República Argentina* . Buenos Aires, Argentina.

Ley Nº 24509 de Seguridad Interior. (18 de Diciembre de 1991). *Boletín Oficial de la República Argentina* . Buenos Aires, Argentina.

Ley Nº 25326 de Protección de Datos Personales. (4 de Octubre de 2000). *Boletín Oficial de la República Argentina* . Buenos Aires, Argentina.

Ley Nº 25506 de Firma Digital. (14 de Noviembre de 2001). *Boletín Oficial de la República Argentina* . Buenos Aires, Argentina.

Resolución Nº 1380/2019. (25 de Octubre de 2019). *Boletín Oficial de la República Argentina* . Buenos Aires, Argentina.

Resolución Nº 1523/2019 - Infraestructuras Críticas. (12 de Septiembre de 2019). *Boletín Oficial de la República Argentina* . Buenos Aires, Argentina.

Resolución Nº 580/2011. (28 de Julio de 2011). *Boletín Oficial de la República Argentina* . Buenos Aires, Argentina.

Resolución Nº 829/2019 - Estrategia Nacional de Ciberseguridad. (24 de Mayo de 2019). *Boletín Oficial de la República Argentina* . Buenos Aires, Argentina.

Resolución Nº 829/2019 - Estrategia Nacional de Ciberseguridad. (24 de Mayo de 2019). *Boletín Oficial de la República Argentina* . Buenos Aires, Argentina.

Resolución SGM N° 829/2019 - Estrategia Nacional de Ciberseguridad. (2019). *Boletín Oficial de la República Argentina* . Buenos Aires, Argentina.

Estados Unidos

107th United States Congress. (2001, Octubre 26). *USA Patriot Act.* Retrieved Julio 12, 2020, from Discover U.S. Government Information: https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

115th United States Congress. (16 de Noviembre de 2018). Cybersecurity and Infrastructure Security Agency (CISA). Washington D.C., EE.UU.

Director of National Intelligence. (7 de Octubre de 2016). *Office of the Director of National Intelligence.* Recuperado el 7 de Marzo de 2020, de Joint DHS and ODNI Election Security Statement: https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2016/item/1635-joint-dhs-and-odni-election-security-statement

Federal Information Security Management Act. (17 de Diciembre de 2002). *107th United States Congress* . Washington DC, Estaods Unidos.

Joint Chiefs of Staff (CJCS). (2018). *Cyberspace Operations.* Whashington D.C.

The White House. (Septiembre de 2018). National Cyber Strategy of the United States of America.

Organismos internacionales

Comité Internacional de la Cruz Roja. (1977, Junio 8). *Protocolo I adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales, 1977.* Retrieved Junio 7, 2020, from Comité Internacional de la Cruz Roja: https://www.icrc.org/es/document/protocolo-i-adicional-convenios-ginebra-1949-proteccion-victimas-conflictos-armados-internacionales-1977

Unión Europea

Decisión del Consejo de la Unión Europea 7299/19 relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros. (16 de Mayo de 2019).

Directiva (UE) 2016/1148. (6 de Julio de 2016). *Diario Oficial de la Unión Europea* . Luxemburgo: Oficina de Publicaciones de la Unión Europea.

España, G. d. (2013). *Estrategia Nacional de Ciberseguridad.* Madrid.

España, G. d. (2019). *Estrategia Nacional de Ciberseguridad.* Madrid.

HM Government. (2016). *National Cyber Security Strategy 2016 - 2021 (Spanish).* Londres.

Páginas web y sitios web institucionales

United States Cyber Command. (23 de Junio de 2009). *U.S. Strategic Command.* Recuperado el 25 de 07 de 2020, de United States Cyber Command: https://www.stratcom.mil/Portals/8/Documents/CYBERCOM_Fact_Sheet.pdf