FACULTAD DE DERECHO

Derecho Internacional Penal (Público y Corporativo) de Ciberseguridad – Comparativa y Aplicaciones

Estefanía Mendivil Coronel

4o, E-1, BL

Derecho Internacional

Tutor: José Ignacio Paredes Pérez

Madrid

Marzo 2019

Índice

Listado de Abreviaturas

- AEO: Estatuto de Operador Económico Autorizado
- APT: Advanced Persistant Threats
- CEO: Chief Executive Officer
- CFAA: Computer Fraud and Abuse Act
- CP: Código Penal
- CSIRT: Equipos de respuesta a incidentes de seguridad informática
- Directiva NIS: Directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión
- DNC: Democratic National Committee (Comité Democrático Nacional)
- DDoS: Distributed Denial of Service Attacks
- DPA: Servicio Federal de Supervisión en la Esfera de la Comunicación, la Tecnología de la Información y las Comunicaciones Masivas
- EC3: Centro Europeo de Ciberdelincuencia
- EE.UU: Estados Unidos
- ENISA: Agencia de Seguridad de las Redes y de la Información de la UE
- FBI: Federal Bureau of Investigation
- FSB: Servicio Federal de Seguridad de Rusia
- FSTEK: Federal Service for Technical and Export Control
- IOCTA: Internet Organised Crime Threat Assessment
- IP: Internet Protocol
- IT: Information Technology
- OTAN: Organización del Tratado del Atlántico Norte

- PRC: People's Republic of China
- RGPD: Reglamento General de Protección de Datos 2016/679 del Parlamento Europeo y del Consejo (también GDPR: General Data Protection Regulation)
- TIC: Tecnologías de la Información y la Comunicación
- TJUE: Tribunal de Justicia de la Unión Europea
- UE: Unión Europea

I. Introducción

1. Breve planteamiento

Desarrollos recientes en las alternativas legales de ciberdefensa para corporaciones internacionales ante las nuevas tecnologías y ciberataques desarrollados por individuos, con o sin el apoyo institucional de sus gobiernos, Rusia y China, entre otros. Botnets, ataques DDoS y el espionaje industrial. Alternativas de defensa bajo el derecho penal internacional administrativo ante el auge de los hackers y el 'black market,' y el estudio de casos trascendentales como por ejemplo el caso Morris (1991), Facebook (2016) y Yahoo (2016), entre otros.

2. Antecedentes

Según el informe de 2019 de DataReportal[1] (publicado conjuntamente por 'Hootsuite', plataforma gestora de redes sociales, y 'We are Social,' empresa internacional de marketing y servicios de comunicación), el número de personas que utiliza Internet ha aumentado drásticamente en los últimos años, pero específicamente en el último año; cada día que ha pasado desde enero del 2018 se estima se han conectado 1 millón de nuevos usuarios por primera vez a Internet (dicho de otra forma; 11 usuarios nuevos,

[1] Informe de Hootsuite y We are Social, "Digital 2019: Global Digital Overview," DataReportal, 31/01/19 (disponible en https://datareportal.com/reports/digital-2019-global-digital-overview ; última consulta 06/02/18)

cada segundo). El aumento de usuarios y crecimiento del 'Internet of Things' (en adelante IoT), aporta grandes ventajas pero también ha resultado en un aumento exponencial en la variedad de amenazas y posibles víctimas.

Como veremos, en algunos países la regulación pertinente para prevenir estos abusos es ambigua y escasa por lo que cada vez son más los casos de ciberataques que vemos en las noticias. Por ejemplo, España tiene una población de aproximadamente 46,42 millones de personas y cuenta con 42,96 millones de usuarios de Internet - cifra ésta última que ha aumentado un 9% entre Enero de 2018 y Enero 2019 de acuerdo con el Informe de DataReportal[2]. Por ello, su estudio es algo que debe interesar no solo a las comunidades de ciberseguridad y seguridad informática sino también a la comunidad legal.

3. Plan de Trabajo y Metodología

El estudio se ha realizado durante el segundo semestre del curso académico 2018-2019, y se han utilizado varias fuentes incluyendo; libros, artículos de internet, legislación y jurisprudencia reciente (ver Bibliografía al final del documento).

4. Palabras Clave

Regulación Ciberseguridad | Regulación Protección de Datos | Amenaza Cibernética | Hackback | Ley de Ciberseguridad | Ley de Protección de Datos

[2] Informe de Hootsuite y We are Social, "Digital 2019: Spain," DataReportal, 31/01/19, (disponible en https://datareportal.com/reports/digital-2019-spain?rq=spain, última consulta 05/02/19)

II. Desarrollo

1. Evolución del Ciberespacio

El ciberespacio es el espacio formado por componentes físicos y no-físicos para guardar, modificar e intercambiar información mediante la red informática. En cambio, internet es el sistema global de redes de ordenadores que utilizan el Internet Protocol Suite. Se dice que el Internet Protocol tiene varias 'capas'[3]: social (compuesta por los individuos y grupos que hacen uso del ciberespacio), lógica (compuesta de las aplicaciones, datos y protocolos que permiten el intercambio de información entre dispositivos) y física (componentes físicos de la red, es decir, hardware, routers, módems, ordenadores, e infraestructura parecida) y salvo que se apaguen, cada capa se puede 'hackear.'

Las amenazas cibernéticas suelen ser incidentes causados por 'threat actors' que utilizan algún tipo de acceso o vector de ataque para conseguir sus objetivos. Para llevar a cabo un 'hack' deben tener conocimiento de una vulnerabilidad, tener la capacidad suficiente para poder acceder a ella y poder 'drop the payload'. Existen distintas razones por las cuales un individuo o grupo quiera acceder al mercado negro/ 'Black Market' (compra y venta de productos de forma ilegal) o el mercado gris (productos legales pero comercializados de forma no autorizada). Una de las razones por las cuales ha proliferado el mercado negro y el mercado gris es por la facilidad de acceso; las barreras de entrada a estos mercados han disminuido drásticamente con el tiempo y la oferta de productos es muy variada. Esto ha ido acompañado de un aumento en la complejidad del mercado; ya que aunque las barreras de entrada son casi inexistentes (cualquier persona con un mínimo de conocimiento de ordenadores puede acceder a la 'dark web'), su crecimiento ha supuesto asimismo un aumento en la verificación y aprobación de los participantes.

El mercado hacker ha evolucionado desde principios de 2000 (centrándose en productos

[3] RAND Europe, "A Focus on Cybersecurity." Informe de RAND Corporation, (disponible en https://www.rand.org/content/dam/rand/pubs/corporate_pubs/CP800/CP871-1/RAND_CP871-1.pdf ; última consulta 04/02/19)

y servicios relacionados con el robo de la información de las tarjetas de crédito; Carder.su por ejemplo es un mercado de venta de tarjetas de crédito e identidades robadas), y hoy en día se ha convertido en un mercado en el cual se venden productos muy distintos. Aunque se siguen vendiendo productos relacionados con la información de las tarjetas de crédito, también se ofrecen servicios especializados, - los llamados 'storefronts.' Lo difícil es acceder a los rangos más altos de este mercado ya que los participantes están previamente evaluados y aprobados por otros participantes. Funcionan como si fuesen pequeños 'estados' - en el sentido de que están estructurados, tienen sus propias 'constituciones' y se auto-regulan. En consecuencia, individuos con distintos niveles de habilidad pueden acceder y optar por distintas metas que varían en función del nivel de dificultad.

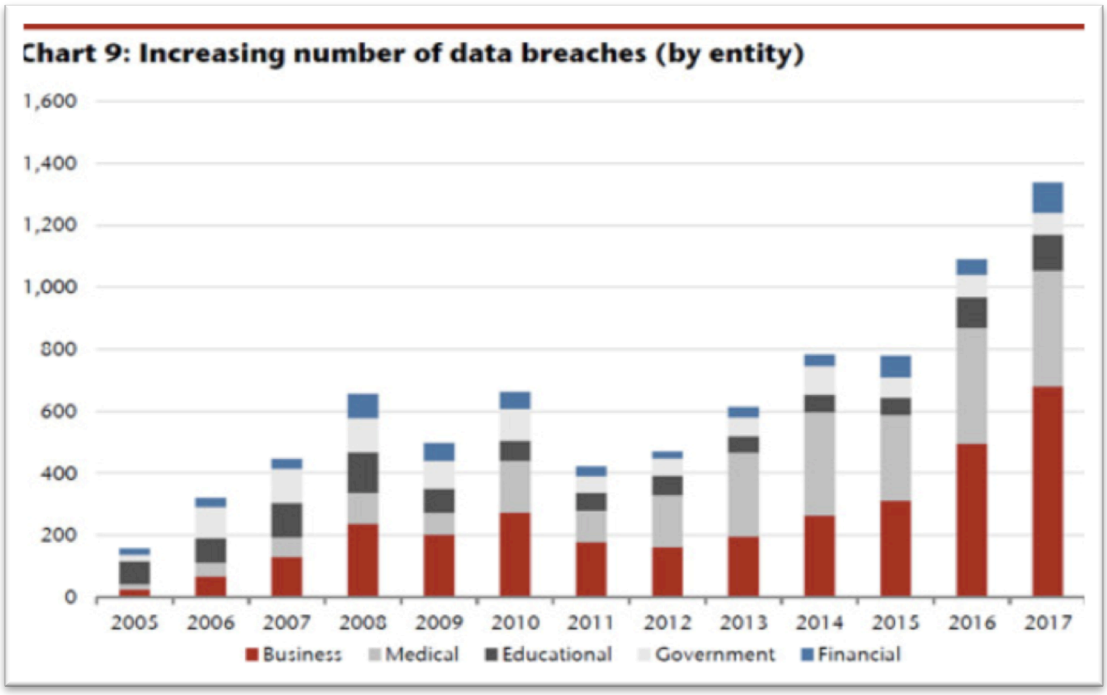
La mayoría opta por técnicas de 'smash and grab' y acceden a cualquier dispositivo hackeable. Los individuos más sofisticados son aquellos suficientemente inteligentes como para atacar sistemas específicos. Podrán por ejemplo, vender propiedad intelectual a aquellos que se dedican al espionaje industrial o vender credenciales a hackeadores con menos experiencia para su posterior venta. Aunque el mercado negro funciona en paralelo al mercado tradicional (la posibilidad de ganar beneficios empuja la innovación), se ha hecho más resistente en años recientes, y todo ello a pesar de que muchos han sido enjuiciados y desmantelados (por ejemplo; Liberty Reserve en Mayo de 2013, Blackhole Exploit Kit en Octubre de 2013, Silk Road en Octubre de 2013, Carder.su en Marzo de 2012, entre otros).

Según el estudio Rand[4] de 2014, una de las principales razones por las cuales se ha hecho tan resistente este mercado ha sido porque el propio mercado contiene tanto los frutos del hacking (por ejemplo: venta de datos personales de usuarios de Internet, drogas etc…) como los medios para realizar un 'hack.' Muestra de ello son los videos en Youtube sobre cómo generar 'Fatrat backdoors,' o dónde adquirir datos de tarjetas de crédito (ilícito).

[4] RAND Corporation Research Series, National Security Research Division "Markets for Cybercrime Tools and Stolen Data," RAND Study, 2014 (disponible en https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf , última consulta 06/02/19)

2. *Crecimiento de Delitos en el Ciberespacio*

Las amenazas cibernéticas han aumentado de forma preocupante en los últimos años. Por ejemplo, en EE.UU se estima que el número de robo de datos/ violación de datos personales en el 2017 estaba en torno a 1.300 – mientras que en el 2005, se estima que la cifra no llegaba ni a 200 (ver gráfico a continuación).



[5]

La tipología de amenazas en el ciberespacio es inmensa pero por lo general la regulación promulgada se 'concentra' en ciberseguridad y la protección de datos. Por tanto, el desarrollo en las alternativas legales realizado en este trabajo está dividido en dos bloques: por un lado, la normativa en el campo de la ciberseguridad (incluye la protección de sistemas y vulnerabilidades en el ámbito de las Tecnologías de la Información y de la Comunicación, TIC), y por otro lado, la normativa de protección de datos (protección de información/ datos que tienen algún significado).

[5] MarketWatch, "How the number of data breaches is soaring – in one chart," Victor Reklaitis, 25/05/18 (disponible en: https://www.marketwatch.com/story/how-the-number-of-data-breaches-is-soaring-in-one-chart-2018-02-26 ; última consulta 02/04/19)

3. Desarrollo en Alternativas Legales de Ciberdefensa, Normativa de Ciberseguridad y Protección de Datos

3.i Compilación de Normativa sobre Ciberseguridad y Protección de datos

Región	Normativa
U.E.	A. Ciberseguridad 1. Estrategia de Ciberseguridad: Un ciberespacio abierto, protegido y seguro, Consejo de la Unión Europea (2013) 2. Directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión Europea (2017) B. Protección de Datos 1. Reglamento 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (2016)
EE.UU	Ciberseguridad y Protección de Información 1. Computer Fraud and Abuse Act (1986)
China	A. Ciberseguridad 1. Ley de Ciberseguridad (2016)

	B. Protección de Datos 1. Proclamación del National People's Congress (2012) 2. Ley de Protección del Consumidor (enmendado 2013) 3. Gran Cortafuegos Chino
Rusia	A. Ciberseguridad 1. Ley sobre Seguridad de la Infraestructura de Información Crítica (2017) B. Protección de Datos 1. Ley de Datos Personales (2007) 2. Ley Federal sobre Información, Tecnología de la Información y Protección de la Información (2006)
Convenio Internacional	• El Convenio de Budapest (2001)

3.ii Unión Europea

A) Ciberseguridad

En materia de ciberseguridad, la UE cuenta con dos grandes estructuras, por un lado la Estrategia de Ciberseguridad de la Unión Europea[6] de 2013, y por otro lado la Directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un

[6] Comisión Europea, "Estrategia de Ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro," Consejo de la Unión Europea, 07/02/13 (disponible en http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=es ; última consulta 08/02/19)

elevado nivel común de seguridad de las redes y sistemas de información de la Unión[7] (en adelante la Directiva NIS).

La Estrategia de Ciberseguridad de 2013, establece varias pautas para conseguir un ciberespacio seguro y fortalecer los mecanismos de defensa, detección y respuesta a los ciberataques. También se centra en la concienciación de los ciudadanos de la UE para luchar contra la ciberdelincuencia. Muchos países de la UE carecían de la estructura necesaria para combatir ciberataques por lo que esta estrategia representó un cambio importante para luchar contra la delincuencia organizada en Internet.

Además también se inauguró en el 2013, el Centro Europeo de Ciberdelincuencia (EC3) que publica cada año el IOCTA (Internet Organised Crime Threat Assessment) sobre desarrollos en el frente de la ciberseguridad que afectan a los gobiernos, las empresas y los ciudadanos de la UE. Su reporte de 2018[8] concluyó que la mayoría de los ciberataques que afectan a Europa siguen emanando desde dentro de Europa, de los cuales el principal vector de ataque son los correos electrónicos maliciosos con malware, y subrayó la alta tasa de spam - sobretodo proveniente de Alemania y Francia.

La Directiva NIS, entró en vigor en agosto de 2017 y estableció un plazo de 1 año para que los estados miembros lo incorporasen a sus respectivos ordenamientos (traspuesto por España el pasado 8 de septiembre). Tiene como objetivo principal el "lograr un elevado nivel común de seguridad de las redes y sistemas de información dentro de la Unión a fin de mejorar el funcionamiento del mercado interior," (artículo 1).

La Directiva NIS es de obligado cumplimiento para las empresas/ operadores de servicios esenciales y digitales (dentro de esta categoría se incluyen desde empresas en el sector de la industria química, hasta aquellas en los sectores de transporte, sistema financiero, salud, infraestructura digital, alimentación etc…), y sus principales novedades son:

[7] Directiva 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (19/07/16)

[8] Informe IOCTA, Internet Organised Crime Assessment, 2018, Europol, EC3 European Cybercrime Centre

- Cooperación entre países mediante la creación de CSIRT (equipos de respuesta a incidentes de seguridad informática) como mecanismo de respuesta rápida y para canalizar las notificaciones de ciberataques (artículos 10, 11, 12 y anexo I). En este sentido, la Directiva NIS también establece que todos los Estados deberán adoptar estrategias de seguridad en las redes y de información.
    - En relación con el segundo punto, España cuenta con una Estrategia de Ciberseguridad Nacional[9] desde el 2013 cuyo fin es "implantar de forma coherente y estructurada acciones de prevención, defensa, detección y respuesta" a las ciberamenazas."[10]
- Crea ENISA (Agencia de Seguridad de las Redes y de la Información de la UE).
- Obliga a las empresas a notificar incidentes de seguridad (artículos 14, 20) y a adoptar ciertos tipos de medidas técnicas y organizativas para prevenir ciberataques (artículos 16, 17).

B) Protección de Datos

En el 2016, la Unión Europea sustituyó la Directiva 95/46/EC del Parlamento Europeo[11], por el Reglamento 2016/679 del Parlamento Europeo y del Consejo[12] , conocido como el Reglamento General de Protección de Datos (conocido por las siglas: RGPD, o GDPR: 'General Data Protection Regulation').

Partiendo de que la protección de datos se considera un derecho fundamental (defendido tanto por el artículo 8, apartado 1 de la Carta de los Derechos Fundamentales de la Unión Europea, y el artículo 16, apartado 1 del Tratado de Funcionamiento de la Unión

[9] Estrategia de Ciberseguridad Nacional, 2013 (disponible en https://www.ccn-cert.cni.es/publico/dmpublidocuments/EstrategiaNacionalCiberseguridad.pdf ; última consulta 05/04/19)
[10] Id. Página 3
[11] Directiva 95/46/EC del Parlamento Europeo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (23/11/1995)
[12] Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (04/05/2016)

Europea), el RGPD establece requisitos más estrictos que otros regímenes legales, entre ellos el de EE.UU, y detalla los pasos que deben seguir las empresas para procesar y tratar datos personales. Además, únicamente aplica a las personas físicas e independientemente de su nacionalidad o lugar de residencia (capítulo 1, artículo 3, RGPD).

En este sentido, su artículo 4 define 'datos personales' como "toda información sobre una persona física identificada o identificable," y seguidamente detalla los mecanismos que deben seguir las empresas cuando procesan (es decir; recolectan, utilizan, guardan o divulgan) los datos personales de residentes de la UE, e independientemente de si el procesamiento tiene lugar en la UE, o en otra jurisdicción, además de las situaciones en las cuales se considera licito su tratamiento (artículo 6).

El RGPD aplica a dos clases de empresas, los primeros se denominan 'responsables' o 'responsables del tratamiento' (en inglés 'controllers') y son aquellos que "determinan los fines y medios del tratamiento" (artículo 4, apartado 7), y los segundos son los 'encargados' o 'encargados del tratamiento' (en inglés 'processors') y son aquellas entidades que tratan los datos personales por cuenta de los responsables del tratamiento (artículo 4, apartado 8). Sin embargo son los responsables del tratamiento quienes tienen el deber de asegurarse de que los encargados traten los datos de tal forma que se cumplan los requisitos establecidos en el RGPD (artículo 28, apartado 1).

El tratamiento de datos personales sólo se considera lícito si se cumple alguna de las condiciones enumeradas en el artículo 6 (cuando el interesado da su consentimiento, o si es necesario para ejecutar un contrato, dar cumplimiento a una obligación legal, proteger intereses vitales, cumplir una misión realizada en interés público, o si es necesario para satisfacer intereses legítimos del responsable del tratamiento o de un tercero) y de acuerdo con los principios del artículo 5. Además, el artículo 9 impone ciertas restricciones sobre categorías especiales de datos, lo cual incluye datos que revelan los orígenes étnicos, opiniones políticas, convicciones religiosas o filosóficas, entre otros. Por lo general, ésta segunda categoría de datos sólo puede ser procesada si el interesado

da su consentimiento o aplican algunas de las excepciones detalladas en el mismo artículo.

El artículo 13 establece que cuando se obtengan datos personales de una persona física, la empresa responsable del tratamiento le deberá facilitar información sobre los tipos de datos recogidos, información sobre el delegado de protección de datos, los fines del tratamiento, y en su caso, los destinatarios de los datos personales. Sin embargo, lo que quizá no queda claro son los mecanismos concretos y políticas que deben emprender estas empresas para satisfacer estas obligaciones ya que el RGPD no enumera prácticas empresariales concretas. Únicamente alude a la necesidad de aplicar "medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo,[13]" en su artículo 32, lo cual es preocupante desde el punto de vista de las empresas. En 'empresas' cabe mencionar que incluimos a los gigantes como Google, Microsoft, Apple etc… Al no especificar cuáles son las medidas específicas a tomar, no contamos con un estándar concreto.

Quizá lo más preocupante para las empresas es el contenido del artículo 17, sobre el derecho al olvido, según el cual, en algunas circunstancias las personas físicas pueden solicitar la supresión de sus datos personales sin dilación indebida (circunstancias tales como las siguientes; cuando los datos no son necesarios para los fines originales, si el interesado retira su consentimiento, los datos son tratados de forma ilícita, entre otros).

Algunos argumentan que el establecer estas nuevas condiciones es una forma de hacer frente al miedo que tienen muchos europeos a que sus datos sean utilizados de manera "indiscriminada" o acaben en las manos de terceros[14]. Por este motivo, muchos individuos han estado recibiendo correos de distintos servicios solicitando su consentimiento para seguir disponiendo o almacenando sus datos personales, ya que la

[13] También enumera algunos ejemplos breves en el mismo artículo (entre ellos; cifrado de datos personales, tener la capacidad de garantizar la confidencialidad etc…)
[14] Redacción, "GDPR: La nueva regulación de protección de datos impulsará el mercado único digital," Revista electrónica TechWeekly, 20/ 04/18, (disponible en http://www.techweek.es/seguridad/analisis/1018894004801/gdpr-regulacion-proteccion-datos-ue-impulsa-mercado-unico-digital.1.html ; última consulta 06/02/19)

nueva normativa pone en cuestión muchas prácticas y el modo de funcionamiento de los registros internos de las empresas. Algunos especialistas recomiendan[15] lo siguiente; "Si una organización no puede demostrar que tiene el consentimiento expreso del titular para ese fin y uso concreto, es mejor que no los use o que los borre, porque la Agencia Española de Protección de Datos le va a pedir la documentación si le inspecciona."

Además, las consecuencias de no acatar estas normas pueden ser muy gravosas para las empresas ya que se enfrentan a sanciones de hasta 20.000.000 euros o de una cuantía equivalente al 4%, como máximo, del volumen de negocio total anual global del ejercicio financiero anterior (artículo 83). Supone un gran cambio para empresas como Google o Facebook que hasta entonces podían, dentro de ciertos límites, eludir los controles de las agencias nacionales de protección de datos[16]. Google, por ejemplo almacena los datos personales de los individuos que utilizan sus productos (Gmail, Youtube, Google Drive, Google Maps, y Google Search) y cuantos más productos sean utilizados por un individuo, más información reúnen[17], hasta tal punto que escanean los correos enviados para mejorar las sugerencias publicitarias que aparecen en nuestros dispositivos y optimizar a su vez las capacidades de aprendizaje automático de sus sistemas. Está en su cultura el recolectar y almacenar toda la información que puedan sobre sus usuarios[18]. Facebook, por su lado, continúa registrando nuestra información incluso si hemos cerrado la página (salvo que salgamos de nuestro perfil de forma manual)[19].

Uniendo estas aclaraciones al alcance que tienen estas empresas (ambos gigantes tecnológicos ya que se encuentran en el 'club de los mil millones,' - por ejemplo, Google cuenta con 800 millones de usuarios activos cada día), no es de extrañar que el RGPD

[15] José Manuel Rodríguez, Beatriz Page, "Cómo te afecta la nueva ley de protección de datos," Revista electrónica LaVanguardia, 24/05/18 (disponible en https://www.lavanguardia.com/tecnologia/20180524/443785604531/rpgd-proteccion-datos-privacidad-multas-ciudadano.html ; última consulta 06/02/19)
[16] Id.
[17] Ben Popken, "Google sells the future, powered by your personal data," NBCNews, 10/05/18 (disponible en https://www.nbcnews.com/tech/tech-news/google-sells-future-powered-your-personal-data-n870501 ; última consulta 06/02/19)
[18] Id.
[19] Gemma Galdon Clavell , "Qué hacen con nuestros datos en internet?", El País, 11/06/15https://elpais.com/tecnologia/2015/06/12/actualidad/1434103095_932305.html ; última consulta 06/02/19)

establezca un régimen más riguroso para el almacenamiento de datos.

3.iii EE.UU

Ciberseguridad y Protección de Información

La regulación Americana en materia de ciberseguridad lo encontramos en la 'Computer Fraud and Abuse Act' de 1986 (CFAA o 'la ley anti-hacking' como es conocida coloquialmente en EE.UU) y actualmente en vigor.

En junio de 1983, el Presidente Ronald Reagan vio la película 'Juegos de Guerra' ('Wargames') – la cual trata sobre un adolescente que sin querer hackea unos misiles y casi ocasiona la tercera guerra mundial. Tras ver la película Reagan le preguntó a sus asesores más cercanos si existía alguna posibilidad de que este escenario se materializase y aunque hubo muchas bromas al respecto, tras un periodo de una semana sus asesores le contestaron que 'sí,' y a raíz de ello promulgaron legislación en el área de ciberseguridad. El resultado fue la promulgación del 'Comprehensive Crime Control Act' de 1984, antecedente de la CFAA.

El artículo 1 de la CFAA prohíbe el acceso (voluntario o involuntario) de un ordenador protegido (con autorización o excediendo autorización), y mediante el cual se obtiene información, se comete un fraude, se obtiene algo de valor, se comete extorsión, se transmite información engañosa, causa daños o se trafica en contraseñas. Al contener definiciones tan ambiguas de lo que significa 'acceder a un ordenador privado' el CFAA permite el enjuiciamiento de múltiples modalidades de ciberataques, hasta tal punto que se ha criticado por extralimitarse y atribuirse jurisdicción cuando no la tiene. Lo cierto es que por mucho que un tribunal americano condene a un individuo ruso, por ejemplo contratado por el gobierno de Putin, no tendrá muchos efectos porque Rusia no tiene tratado de extradición con EE.UU.

El contraargumento es que aunque tal vez no se consiga siempre enjuiciar a estos 'hackeadores,' bien porque no exista tratado de extradición o porque no interese hacer una acusación formal por motivos políticos o interés nacional - pienso que el comenzar una investigación y abrir expediente sigue teniendo valor por los siguientes motivos: a) señala a Rusia (y a la comunidad internacional) que los americanos se están tomando esta clase de infracciones en serio, b) el iniciar trámites legales nos acerca más a la fase de condena y la imposición de una pena (más que lo contrario), c) también es una señal para futuros hackeadores (si se sube la pena impuesta por ejemplo, tendrá un efecto disuasorio sobre quienes en un futuro quieran cometer dichas infracciones), d) puede tener un efecto disuasorio indirecto, por ejemplo, se puede imponer prohibiciones de viaje o congelación de fondos (se podría, por ejemplo, congelar la cuenta de Paypal o cualquier cuenta que caiga bajo jurisdicción americana), y e) aunque no exista tratado de extradición, en ocasiones estos individuos se equivocan y viajan a países con los cuales sí existe tratado de extradición.

Por ejemplo, en el ataque cibernético a Yahoo[20] de 2016 – cuatro individuos rusos emprendieron su proyecto con el objetivo de acceder a información sobre individuos de interés para el gobierno de Putin (entre ellos: funcionarios de los países fronterizos con Rusia, funcionarios del gobierno estadounidense, políticos rusos, proveedores de servicios de internet de EE.UU cuyas cuentas podían facilitar el acceder a muchas otras cuentas, y ciudadanos y periodistas rusos) pero acabó resultando en el robo de datos más grande de la historia; afectó a más de 3.000 millones de usuarios. Sin embargo, Karim Baratov fue el único que pisó los tribunales americanos por haber tenido la (des)gracia de haber nacido en Canadá (país con el cual EE.UU tiene un tratado de extradición), mientras que los otros 3 rusos (Dmitry Dokuchaev, Igor Suschin, y Alexsey Belan) involucrados siguen 'ausentes.' A Baratov le condenaron bajo la CFAA a 5 años de prisión (de acuerdo con los Federal Guidelines) y a una multa de $2.500.000 (lo cual abarca todos sus activos restantes) - por robo de identidad agravado (18 USC. § § 982(a)(2)(B) y 1030(i) y (G)). y conspiración de violar la CFAA (18 USC. § 1030(b)).

[20] United States of America v. Dmitry Dokuchaev, Igor Suschin, Alexsey Belan and Karim Baratov, US District Court, Northern District of California, San Francisco Division, 2017 Indictment

Es de destacar que dos de los individuos involucrados en el caso de Yahoo, Dokuchaev y Suschin, eran miembros de la agencia de investigación cibernética del gobierno ruso (el equivalente a la división cibernética del F.B.I. de EE.UU).

3.iv China

A comparación de la normativa analizada antes, la regulación China es muy detallada y aunque se puede dividir en dos bloques (normativa sobre ciberseguridad en general y normativa sobre protección de datos), existen muchas incertidumbres en cuanto a su aplicación porque a pesar de que el gobierno del PRC (People's Republic of China) tiene un alto grado de control sobre la utilización de Internet dentro del país, no persigue de forma activa las amenazas de ciberseguridad o robo de datos – a comparación de otras potencias, como por ejemplo UE, o Canadá - al menos cuando no interesan o no está relacionado con los objetivos del gobierno comunista.

A. Ciberseguridad

La normativa en materia de ciberseguridad entró en vigor tarde en comparación con otros países. En el 2016 la Comisión Permanente del Congreso Nacional de la PRC promulgó la nueva Ley de Ciberseguridad[21] – y es la primera ley que se dedica exclusivamente a la regulación de ciberseguridad. Es de notar el aumento drástico que se atribuye en cuanto a jurisdicción en asuntos concernientes a la ciberseguridad, se centra sobre todo en los 'operadores de la red' y 'operadores de infraestructura crítica de información,' y aplica a todas las empresas que operan en China y aquellas que tienen negocios con empresas en China. Además, esta ley es preocupante por los potenciales altos costes que puede

[21] Cybersecurity Law of the People's Republic of China, passed November 6, 2016, effective June 1, 2017, (http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm), traducida: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ , última consulta 25/03/19

conllevar para las empresas en caso de su incumplimiento (analizados a continuación) y las incertidumbres existentes sobre las directrices que publique el gobierno en el futuro, en desarrollo de esta ley.

La ley prohíbe a las empresas utilizar productos o servicios que no hayan pasado previamente por los controles de seguridad y no hayan sido aprobados. Subraya tanto la 'protección de información' como la "soberanía sobre el ciberespacio,"– expresión, esta última acuñada por la PRC (artículos 1 y 12).

Es de destacar el artículo 37 ya que establece requisitos sobre la localización de la información; toda información personal o cualquier otro tipo de información 'clave' recopilada por estas empresas solo puede guardarse en servidores que se encuentran en territorio Chino y en caso de querer mover esta información fuera de China, las empresas deberán pedir permiso previamente al Gobierno y pasar por una prueba de seguridad. Además, la ley impone distintas penalizaciones para las empresas en caso de que no cumplan esta obligación; desde un aviso, revocación de permiso, o cierre de su página web, hasta multas de hasta US $72.500 para las empresas o US $14.500 para los particulares.

Además, la Ley de Ciberseguridad establece varios requisitos (de cumplimiento obligatorio) que deben acatar los operadores de la red – entre ellos, las empresas deben instituir protocolos para protegerse a sí mismos y sus usuarios (deberán adoptar medidas de seguridad específicas como por ejemplo: clasificar información, encriptación, instituir medidas para prevenir ataques a la red o prevenir virus, establecer claramente quienes son las personas que deberán responsabilizarse de estos controles etc…) y entregar códigos fuente. Empresas extranjeras que operan en China deberán evaluar y mejorar sus estructuras de IT, y en su caso invertir los recursos necesarios. También podría impedir el desarrollo de competitividad de empresas extranjeras con empresas chinas (muchas se opondrán a la entrega de sus códigos fuente al gobierno, sobre todo por el alto potencial de abusos generalizados en materia de derechos de propiedad intelectual), pero por otro lado, favorece a las empresas domésticas.

Según algunos comentaristas[22] aunque la ley "aparentemente (...) apunta a proteger la privacidad de los 730 millones de usuarios de Internet en China (...) en realidad, consagra el derecho del Estado a espiar a cualquiera que se conecte a la red mundial de datos y obligará a todas las compañías que operan en el país a ser cómplices de eso."

B. Protección de Datos

En material de protección de datos, contamos con dos directrices: por un lado la proclamación[23] de 2012 del 'National People's Congress' sobre fortalecer la protección de información, y por otro lado las enmiendas del 2013 a la Ley de Protección del Consumidor.

La proclamación de 2012 impuso obligaciones a las empresas (aquellas proveedoras de servicios de internet y empresas que recopilan o utilizan datos personales sobre sus usuarios) en relación con la privacidad y protección de datos, pero es muy ambigua ya que únicamente obliga a que dichas entidades cumplan con los principios de legalidad, legitimidad, y necesidad (punto II). Además, específica que las empresas deberán indicar el objetivo, método de recopilación y uso que le darán a la información, obtener permiso de los individuos cuyos datos recopilan y asegurarse de que dicha información no se divulga o se pierde – pero no específica los mecanismos que utilizará China para conseguir estos objetivos o la penalización (si acaso existe) para las empresas que no acaten estas normas.

[22] El Cronista, "Nueva ley de ciberseguridad china implica más censura," 02/06/17 (disponible en https://www.cronista.com/financialtimes/Nueva-ley-de-ciberseguridad-china-implica-mas-censura-20170602-0059.html ; última consulta 27/03/19)
[23] National People's Congress Standing Committee Decision concerning Strengthening Network Information Protections, China Copyright and Media, 28/12/12 (disponible en https://chinacopyrightandmedia.wordpress.com/2012/12/28/national-peoples-congress-standing-committee-decision-concerning-strengthening-network-information-protection/ ; última consulta 25/03/19)

La UE publicó un informe[24] en 2015 criticando la proclamación de China por ser insuficiente debido a que únicamente se centra en protección de datos (y hay más áreas que merecen protección), no cuenta con un mecanismo para ejecutarlo y se basa en un número escaso de principios comparado con el listado de principios en los que se basa la normativa análoga europea. Sin embargo, concede que si se ha proclamado como primer paso para eventualmente promulgar normativa en materia de protección de datos, entonces tendría su mérito (página 20).

Por su lado, en el 2013 se realizaron enmiendas a la Ley de Protección del Consumidor para integrar y hacer eco de la proclamación de 2012 similares a aquellas reflejadas en el Reglamento General de Protección de Datos de la UE. Sin embargo nos debemos preguntar sobre la eficacia real de estas enmiendas ya que China no cuenta con autoridades que se dedican exclusivamente (y de forma activa) a la protección de datos – tal y como existe en la UE.

C. Gran Cortafuegos Chino

Por último, cabe hacer mención al Gran Cortafuegos Chino (también conocido a nivel mundial como 'The Great Firewall' - juego de palabras en relación con 'The Great Wall of China') ya que se trata de normativa introducida por el partido comunista para bloquear el acceso de sus ciudadanos a ciertas páginas web, información, redes sociales y ciertas empresas (como por ejemplo Google, Twitter, Instagram etc...) - pero no solo impide su acceso a estas páginas web sino que monitoriza el acceso a internet en el territorio, de ahí que frecuentemente se compare el Internet en China con 'una gran Intranet.'

El gobierno dice no estar dispuesto a permitir que estas compañías operen en China pero almacenen los datos fuera del país, pero también hay otros motivos detrás de la impulsión de este programa, el más importante de ellos es la censura en China y el almacenamiento

[24] European Parliament, Directorate-General For Internal Policies, Policy Department, Citizens' Rights and Constitutional Affairs, The Data Protection Regime in China (2015) (disponible en: http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA%282015%29536472_EN.pdf ; última consulta 23/03/19)

de datos fuera del país. Como hemos visto en el desarrollo normativo anterior, ciertas leyes como por ejemplo la Ley de Ciberseguridad establecen varias restricciones al almacenamiento de datos y claramente reflejan que el gobierno no permite almacenamiento de datos de los usuarios de estos servidores fuera de China.

Según el ex-Presidente Deng Xiaoping, "Si abrís la ventana para que entre un poco de aire fresco, también se van a meter algunas moscas,"[25] - refiriéndose precisamente a las grandes empresas tecnológicas americanas, como por ejemplo Google o Facebook, como 'moscas.' Al mismo tiempo que consigue dar cumplimiento a la política de censura, también consigue dar un impulso a las empresas tecnológicas chinas que compiten con las americanas (entre muchas otras).

3.v Rusia

A. Ciberseguridad

La Ley sobre Seguridad de la Infraestructura de Información Crítica [26] de 2017 establece la normativa necesaria para proteger 'infraestructura crítica para Rusia' (en esta categoría incluye a empresas del sector de telecomunicaciones, transporte, comunicación, energía, finanzas etc…). La ley obliga a dichas empresas a registrarse con la FSTEK ('Federal Service for Technical and Export Control,' autoridad que supervisa cumplimiento con esta ley) y a introducir medidas para protegerse contra las amenazas cibernéticas.

B. Protección de Datos

[25] Perfil, "La Gran Burbuja: redes sociales en China," Facundo F. Barrio, 14/07/18(disponible en https://www.perfil.com/noticias/elobservador/la-gran-burbuja-redes-sociales-en-china.phtml ; última consulta 27/03/19)
[26] Ley sobre Seguridad de la Infraestructura de Información Crítica para Rusia, N. 187-FZ, 26/07/17

En materia de protección de datos, la Ley de Datos Personales[27] que entró en vigor en 2007 (conocida como la 'Ley de Localización de Datos' y enmendado en 2015) obligó a las empresas que recopilan datos a guardar y utilizar bases de datos ubicados en Rusia. Supuso en cambio drástico y un aumento en los costes para muchas empresas que desde entonces tuvieron que rediseñar la infraestructura de almacenamiento de datos. Aplica tanto a empresas como individuos.

Algunos argumentan[28] que a pesar de que la Ley de Datos Personales establezca requisitos estrictos e imponga penalizaciones en caso de incumplimiento, no se cumple íntegramente dadas las sanciones leves que conlleva, el hecho de que las autoridades de protección de datos trabajen lentamente y por falta de claridad de la normativa (lo cual dificulta su cumplimiento).

Adicionalmente, la Ley Federal sobre Información, Tecnología de la Información y Protección de la Información[29] (en adelante Ley de Información) establece requisitos rigurosos para aquellas compañías en el sector de comunicación (video/audio/texto) – entre ellos impuso la obligación de registrarse con las autoridades de protección de datos, ya sea la DPA (Servicio Federal de Supervisión en la Esfera de la Comunicación, la Tecnología de la Información y las Comunicaciones Masivas) o FSB (Servicio Federal de Seguridad de Rusia) y almacenamiento de datos (grabaciones de todas las llamadas telefónicas, contenido de todos los mensajes de texto etc…) sobre sus usuarios durante un periodo de 6 meses. A raíz de ello, bloquearon Blackberry Messenger y otras plataformas de mensaje instantáneo en territorio Ruso (Imo, Vchat, WeChat etc..). Además esta ley obliga a que las empresas proporcionen a las autoridades cualquier información/ datos personales de sus usuarios (o de las claves necesarias para descifrar mensajes encriptados) en caso de que el gobierno de Putin lo solicite – todo ello fundamentado en 'fines de investigación.'

[27] Ley de Datos Personales, N. 152-FZ, 27/07/06
[28] The Law Reviews Magazine, The Privacy, Data Protection and Cybersecurity Law Review – Edition 5 (disponible en https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-5/1175638/russia ; última consulta 24/03/19)
[29] Ley Federal sobre Información, Tecnología de la Información y Protección de la Información, N. 149-FZ, 27/07/06

Al contrario que la normativa China, la Ley de Información sí impone penalizaciones en caso de incumplimiento, como por ejemplo la imposición de multas (hasta 75.000 rublos), interrupción de su funcionamiento en territorio ruso o sanciones penales. Por ejemplo, la famosa aplicación de mensajes instantáneos China: 'WeChat' se bloqueó en Rusia y solamente se desbloqueó una vez que se había registrado con la DPA.

3.vi Convenios Internacionales, El Convenio de Budapest

El Convenio de Budapest[30] de 2001, también conocido como el Convenio sobre Ciberdelincuencia o Cibercriminalidad busca homogeneizar la definición de cibercriminalidad y "llevar a cabo una política penal común (...) mediante la adopción de una legislación apropiada y la mejora de la cooperación internacional" (preámbulo). Desde su introducción en el 2001 se han unido 62 estados (entre ellos España, EEUU, Inglaterra, y Canadá)[31]. Ni China ni Rusia son estados miembros - pero se considera a Rusia un miembro 'observador' por su cualidad de miembro del Consejo de Europa.

El Convenio de Budapest es el primer intento intercontinental normativo en integrar leyes de varios Estados y cooperar en materia de ciberseguridad y protección de datos. El Convenio tiene varias ventajas, pero como veremos a continuación tiene más inconvenientes que ventajas.

Ventajas

1. La investigación y persecución de los delitos en el ciberespacio muchas veces involucra a más de un país, por lo que puede presentar obstáculos por problemas de jurisdicción, competencia y herramientas necesarias para su adecuada persecución. En este sentido, el Convenio proporciona una vía para la

[30] Convenio sobre Cibercriminalidad, hecho en Budapest, de 23 de noviembre de 2001
[31] Council of Europe, Parties/ Observers to the Budapest Convention and Observer Organisations to the T-CY (disponible en https://www.coe.int/en/web/cybercrime/parties-observers ; última consulta 27/03/19)

cooperación de los Estados miembros en la persecución de los delitos en el ciberespacio y esto ayudará a disminuir la cantidad de delitos impunes que hay.

- El Convenio apoya el que los Estados miembros compartan información.
- Precisamente por la naturaleza transfronteriza de los delitos en el ciberespacio, es imposible que un Estado luche contra la ciberdelincuencia de manera unilateral - por lo que sin su adhesión al Convenio de Budapest (o Convenios similares en materia de ciberseguridad y protección de datos) difícilmente podrá atajar estos problemas.

2. Constituye un estándar que pueden (es decir, es opcional) utilizar los países para adaptar su normativa interna o desarrollar legislación en esta materia. De esta manera los Estados miembros cuentan con mucha flexibilidad para desarrollar esta normativa.
    - El Convenio establece ciertas pautas para que cada Estado miembro legisle y adapte su legislación interna, por lo que en este sentido sí puede llegar a ser vinculante su contenido.
3. Introduce varias categorías [32] de delitos y normas procesales (sobre procedimiento):
    a. Delitos que utilizan la tecnología como fin (en lo referente a la confidencialidad, integridad de la información etc..), por ejemplo, acceder de manera ilícita a un sistema
    b. Delitos que utilizan la tecnología como un medio (se refiere a delitos 'tradicionales' que meramente se cometen a través de un sistema informático), como por ejemplo la falsificación de datos
    c. Delitos relacionados con el contenido, por ejemplo la posesión o distribución de materiales prohibidos
    d. Delitos relacionados con la propiedad intelectual (se refiere al contenido protegido) por ejemplo la piratería
    - Los países miembros del Convenio de Budapest se 'comprometen' a tipificar estos tipos de delitos en sus respectivas legislaciones

[32] WeLiveSecurity, "Convenio de Budapest: beneficios e implicaciones para la seguridad informática," Cecilia Pastorino, 06/12/17 (disponible en https://www.welivesecurity.com/la-es/2017/12/06/convenio-budapest-beneficios-implicaciones-seguridad-informatica/ ; última consulta 27/03/19)

4. Establece mecanismos de revisión y monitorización - por ejemplo, su artículo 46 incita a los Estados miembros a que se reúnan de manera periódica para facilitar el cumplimiento del Convenio de Budapest, intercambio de información y diálogo sobre posibles reformas del Convenio. También permite la propuesta y realización de enmiendas (artículo 44).
5. El Convenio en sí fue el producto de negociaciones y trabajo de expertos (especializados en el estudio de delitos en el cibersespacio) de varios Estados - tanto miembros de la UE, como no-miembros. El hecho de que los expertos provengan de otros Estados (tanto Estados miembros de Consejo de Europa, EE.UU, Canadá, Japón etc...) es lo que permite que se unan al Convenio Estados no-miembros de la UE.
6. El Convenio de Budapest es el único acuerdo internacional que cubre todas las áreas 'relevantes' de la ciberdelincuencia, hasta el momento de su promulgación no existía un acuerdo internacional que cubriese las áreas de derecho procesal, derecho penal y la cooperación internacional en lo relativo a la ciberseguridad. Además el texto prioriza la tipificación de los delitos en el ciberespacio y la política penal que deben tener los Estados miembros. Cuestión distinta es si consideramos que la cobertura es suficiente (analizado más adelante).
    - De esta forma reduce parcialmente el problema transfronterizo inherente en los casos de ciberdelincuencia.
7. El Convenio cuenta con un procedimiento sencillo para la adhesión de nuevos países. Para adherirse al Convenio de Budapest un Estado deberá ser invitado por un Estado miembro del Convenio (artículo 37), y no es necesario ni haber participado en la fase de elaboración del Convenio ni ser miembro del Consejo de Europa.

Inconvenientes

1. Aunque el Convenio de Budapest constituye un estándar que pueden utilizar los Estados para adaptar su normativa interna, su utilización es potestativa y el tratado es lo suficientemente ambiguo como para que cada miembro interprete las

disposiciones de la manera que más le convenga. En consecuencia no logra homogeneizar verdaderamente la legislación en materia de ciberseguridad.

- Por ejemplo, aunque el preámbulo y el artículo 15, apartado 3 se fundamentan en "proteger intereses legítimos," el Convenio no define qué son intereses legítimos y cada país podrá considerar lo que más le convenga.
- La definición de 'intereses legítimos' cambiará en función de quien se trate.

2. No responde a la pregunta; ¿qué debemos hacer si en lugar de ser un particular detrás de las amenazas, es un país/ gobierno extranjero quien es responsable?
    - El Convenio únicamente proporciona un estándar para desarrollar normativa en lo referente a casos en los cuales son los particulares o el sector privado quien comete estos delitos, pero no aborda la cuestión sobre qué ocurre cuando es el gobierno de otro Estado quien permite u ordena el ciberataque.
3. Aunque recomienda criminalizar ciertas conductas, no tiene en cuenta que no todos los Estados miembros son iguales, es decir, algunos Estados son más democráticos que otros, algunos Estados son más o menos transparentes que otros y desde luego no todos respetan o garantizan de la misma forma derechos humanos. Por tanto presenta la posibilidad de abuso y posibles restricciones arbitrarias del derecho a la libertad de expresión.
    - En este sentido, entre sus miembros hay Estados tan diversos como; Turquía, Ucrania, Lituania, Alemania, Francia, etc...
    - Por ejemplo, en los últimos años han salido a la luz varias pruebas de que el gobierno de México (Estado 'observador' del Convenio - no es formalmente un Estado miembro) ha emprendido un programa de espionaje avanzado contra sus propios ciudadanos - justificado por el gobierno en la búsqueda de criminales y terroristas. Según el New York Times[33], desde el 2011, (al menos) 3 agencias federales se han gastado casi US $ 80 millones en programas de espionaje desarrollados por una empresa de origen israelí. Dicho software (conocido como 'Pegasus') permite la monitorización del día a día de los individuos - desde la vigilancia de los mensajes de texto y correos

[33] New York Times,"Somos los nuevos enemigos del Estado: el espionaje a activistas y periodistas en México," Azam Ahmed y Nicole Perlroth, 19/06/17 (disponible en: https://www.nytimes.com/es/2017/06/19/mexico-pegasus-nso-group-espionaje/ ; última consulta 27/03/19)

electrónicos hasta la utilización de la cámara o micrófono del dispositivo. Según el artículo, el software se ha utilizado para vigilar a activistas y periodistas en México.

- También en relación con el problema de desigualdad, la adhesión al Convenio (debe) presuponer un aumento de gastos considerable (inyección de capital) para destinarlo a llevar a cabo sus provisiones (por ejemplo: adquisición de nuevos equipos, personal con conocimientos específicos y especialistas, gastos judiciales en relación con los delincuentes, monitorización de las iniciativas emprendidas etc...). En este sentido, no todos los Estados miembros tienen la misma capacidad financiera, como por ejemplo, EE.UU en comparación con Panamá, ambos son Estados miembros del Convenio pero EE.UU cuenta con mayores recursos para invertir en la persecución de la ciberdelincuencia, instituir mecanismos y promulgar legislación en relación con el Convenio de Budapest.

Obviamente existe mucha complejidad técnica y es muy difícil coordinar la normativa entre varios Estados pero el Convenio de Budapest no parece ser lo suficientemente preciso como para ayudar a reducir la cibercriminalidad a nivel internacional. Quizá lo más importante es que falta un componente necesario; transparencia e imparcialidad (impuesta por lo menos de forma obligatoria) para así prevenir abusos de derechos humanos. De lo contrario su ratificación podría llegar a ser contraproducente para los individuos y empresas de algunos países.

Sin duda es conveniente ser miembro del Convenio de Budapest - dado el aumento y preocupación en años recientes en lo referente a las amenazas en el ciberespacio, y como primer intento hacía la homogeneización normativa en materia de ciberseguridad y protección de datos es un logro, pero a día de hoy es insuficiente. Por otro lado, reducir la ciberdelincuencia beneficia a todos.

4. Aplicación de la Normativa Desarrollada a las Amenazas en el Ciberespacio

4.i Aplicación de la Normativa de la U.E.

1. Nowak v. Data Protection Commissioner (2017)

En Nowak v. Data Protection Commissioner[34], el TJUE (Tribunal de Justicia de la UE) resolvió una disputa sobre el significado de 'datos personales' y la aplicación del Reglamento 2016/679 RGPD (anteriormente la Directiva 95/46) analizado anteriormente.

El señor Peter Nowak, de origen irlandés realizó varios exámenes para formar parte del Instituto de Auditores Públicos. Sin embargo, después del cuarto suspenso de uno de estos exámenes: 'Contabilidad de Gestión y Finanzas Estratégicas,' presentó una solicitud para acceder a todos los datos de carácter personal que le concernían y estaban en posesión del Instituto de Auditores Públicos. Seguidamente el Instituto le reenvío los documentos a excepción del examen del Señor Nowak, aludiendo que 'no contenía datos personales.'

Después de varias reclamaciones y pasar por los tribunales nacionales, el Tribunal Supremo de Irlanda decidió suspender el procedimiento y plantear al Tribunal Europeo de la UE varias cuestiones prejudiciales sobre si la información contenida en las respuestas de un candidato durante un examen profesional constituye un 'dato personal' basado en la regulación europea pertinente, y (en caso de respuesta afirmativa a la anterior cuestión prejudicial) los factores que se deben tener en cuenta para determinar si, en un caso concreto, un examen escrito constituye un dato personal, además de la importancia que se debe atribuir a dichos factores.

[34] Sentencia del Tribunal de Justicia de la Unión Europea de 20 de diciembre de 2017, asunto: C-434/16, ECLI: EU:C:2017:994

El TJUE concluyó que para que un dato pueda ser calificado como 'dato personal' de acuerdo con el artículo 2 RGPD, "no es necesario que toda la información que permita identificar al interesado deba encontrarse en poder de una sola persona (…)" y en el presente caso, aunque el examinador no conociese la identidad del candidato al evaluar las respuestas de su examen, la entidad que organiza las pruebas; el Instituto de Auditores Públicos sí podía disponer de los datos necesarios para identificar al candidato (mediante su número de identificación incluido en el examen) y así atribuir las respuestas al candidato.

Esta sentencia muestra el objetivo de legisladores de la UE de aumentar el alcance de la expresión 'datos personales' – ya no solamente incluye información confidencial o datos relacionados con la intimidad, sino que también abarca todo género de información, tanto objetiva como subjetiva, siempre y cuando sea '*sobre*' la persona en cuestión. En esta sentencia el TJUE específica que este último requisito se cumplirá siempre que "debido a su contenido, finalidad o efectos, la información está relacionada con una persona concreta," y subraya que "las respuestas escritas proporcionadas por un aspirante en un examen profesional son datos relacionados con su persona," en aplicación del RGPD y el derecho a la intimidad del aspirante en lo relativo al tratamiento de sus datos.

Además de precisar que las respuestas dadas por el candidato son datos personales, el TJUE añade que las anotaciones realizadas por el examinador en base a dichas respuestas son también datos personales.

2. Deutsche Post AG y Hauptzollamt Koln (2017)

Mediante esta sentencia [35] el TJUE aclara la interpretación del Reglamento de ejecución 2015/2447 de la Comisión[36] en el marco del Reglamento 2016/679 RGPD.

[35] Sentencia del Tribunal de Justicia de la Unión Europea de 20 de diciembre de 2017, asunto: C-496/17, ECLI: EU:C:2019:36

[36] Reglamento de Ejecución (UE) 2015/2447, de la Comisión de 24 de noviembre de 2015, por el que se establecen normas de desarrollo de determinadas disposiciones del Reglamento UE n. 952/2013 del Parlamento Europeo y del Consejo por el que se establece el código aduanero de la Unión, 29.12.2015

Deutsche Post AG, empresa que disfruta del estatuto 'AEO' (estatuto de operador económico autorizado), interpuso el recurso en base a los escritos provenientes de la Hauptzollamt Koln (Oficina Aduanera Central) solicitando que Deutsche Post presentase datos personales de terceros.

La Oficina Aduanera precisó que si Deutsche Post AG no comunicaba dicha información (específicamente: "números de identificación fiscal, asignados para la recaudación del impuesto sobre la renta, de los miembros del consejo de supervisión del solicitante y de las personas que actúen para el mismo como directores gerentes, directores de departamento, director contable, director del departamento de aduanas y los responsables de asuntos aduaneros y demás personas que trabajen en asuntos aduaneros así como las coordenadas de las oficinas tributarias competentes para todas estas personas"), la empresa no cumpliría los requisitos de autorización establecidos en el código aduanero – en cuyo caso se revocarían las autorizaciones que disfrutaba Deutsche Post AG en ese momento.

En estas circunstancias, el Tribunal de lo Tributario de Dusseldorf presentó una cuestión prejudicial sobre la autoridad que tiene una autoridad aduanera para requerir a una empresa (solicitante del estatuto de AEO) que comunicase dicha información.

El TJUE concluyó que dicha información sí lo pueden exigir las autoridades aduaneras siempre que esos datos permitan obtener información relativa a las infracciones reiteradas o graves de la legislación aduanera, disposiciones fiscales o infracciones penales graves cometidas por dichas personas en relación con su actividad económica.

3. Interferencia en Cataluña

Por último, cabe mencionar la interferencia en Cataluña en lo relativo a las campañas de desinformación (y spam) para aumentar la inestabilidad Catalana y agrandar el problema independentista. Hay muchos que opinan que quien estaba detrás era Rusia, sin embargo

España no ha realizado ningún acto de atribución (a pesar de contar con la normativa adecuada como para fundar una decisión apropiada). Otros han sido tajantes; según el informe[37] de Ben Cardin, senador de EE.UU, y el comité de relaciones extranjeras, la interferencia rusa en el procedimiento democrático de otros países no acabó con la interferencia en las elecciones americanas del 2016 (analizado más adelante), ya que desde entonces los rusos continúan activos en 19 países europeos, entre los cuales se encuentra España. Además, en una rueda de prensa, el senador Cardin especificó que el gobierno de Rajoy no estaba preparado para lidiar con esta situación, pero que supone una "lección aprendida," y España, como el resto de países occidentales "debe aceptar que Rusia jugará en nuestras elecciones domésticas."[38] Además añadió que era necesario mantener una "red de apoyo internacional de intercambio de información y métodos,"[39] para tajar este problema. Aunque no conocemos sus motivos exactos podemos estimar que se trata de fomentar una europea débil y poco unida para así avanzar sus propios intereses.

Rusia por su lado, no ha dado ninguna importancia a estas declaraciones. En una rueda de prensa de la OTAN (Organización del Tratado del Atlántico Norte) a finales del año pasado, el ministro de Asuntos Exteriores ruso, Serguéi Lavrov, bromeó con la implicación rusa en las elecciones catalanas, diciendo que su país no tenía tiempo como para preocuparse de la situación de los agricultores sudafricanos porque "estamos demasiado ocupados entrometiéndonos en las elecciones de Cataluña."[40] Parece lo opuesto a lo que han hecho varios medios rusos; comparando la crisis en Cataluña con los conflictos de Crimea y Kurdistán. Por ejemplo, un titular del periódico Vzglyad (afín al gobierno ruso de Putin) empieza con "España con la fuerza suprime la 'primavera

[37] Ben Cardin, "Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security," Committee on Foreign Relations, US Senate, 10/01/18 (disponible en https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf ; última consulta 06/02/19)
[38] El Confidencial, "La campaña de Desinformación Rusa sigue activa en Cataluña," Revista El Confidencial, 22/01/18 (disponible en https://www.elconfidencial.com/mundo/2018-01-22/desinformacion-rusa-cataluna-ben-cardin_1509898/ ; última consulta 07/02/19)
[39] Id.
[40] RTVE, "El ministro de Exteriores ruso bromea con la implicación de Rusia en las elecciones catalanas," (disponible en http://www.rtve.es/noticias/20180928/ministro-exteriores-ruso-bromea-implicacion-rusia-elecciones-catalanas/1808860.shtml ; última consulta 07/02/19)

catalana,"[41] y cuyo artículo relata la supuesta brutalidad que sufren los españoles en Cataluña.

Hay distintas consideraciones que se tienen en cuenta a la hora de responder a las injerencias de este tipo (entre ellas, posibles efectos adversos sobre las relaciones bilaterales entre España y Rusia etc…), pero España podía haber realizado una acusación formal y fundando una respuesta en alguna de las siguientes normas:

- Artículo 197 del Código Penal Español[42] (en adelante CP) (descubrimiento y revelación de secretos)
- Artículo 248 CP (estafa, incluyendo la manipulación informática)
- Artículo 263, 264 CP (daños, daños informáticos)
- Directiva NIS, entre otras

4.ii Aplicación de la Normativa de EE.UU

1. United States v. Morris (1991)

Esta sentencia[43] es trascendental porque es la primera vez que se condena a alguien bajo la CFAA. El 'gusano Morris' fue el primer ejemplar de software malicioso del cual tenemos constancia. Un estudiante Americano, llamado Robert Tappan Morris, estudiante de primero de carrera de posgrado de Cornell, tardó 2 meses en desarrollar el malware, sin embargo, subestimó el poder del malware porque acabó infectando al 10% de los equipos conectados a la red – lo cual es único en la historia de internet[44].

[41] Nikita Kovalenko, Ekaterina Korostichenko, "Испания силой подавляет «каталонскую весну»," Periódico Vzglyad, 20/10/17(disponible en https://vz.ru/world/2017/9/20/887874.html ; última consulta 07/02/19)
[42] Ley. Orgánica. 10/1995, de 23 de noviembre del Código Penal
[43] United States v. Morris (United States Court of Appeals, Second Circuit, 1991) (disponible en https://h2o.law.harvard.edu/collages/41678 ; última consulta 07/02/19)
[44] Aunque también es verdad que el número de personas que utilizaban internet en ese momento era menor que el actual y por aquel entonces la mayoría de sus usuarios trabajaban en el campo de la seguridad informática.

En apelación, se afirmó la sentencia del tribunal de primera instancia y el Juez Howard, en aplicación de la CFAA; 18 U.S.C. § 1030 (a)(5)(A), terminó por imponer una pena de 3 años de libertad vigilada, 400 horas de servicios prestados a la comunidad y una multa de $10.000 (en lugar de la pena de 15 – 21 meses que establecían las directrices para la imposición de condenas; Sentencing Guidelines).

A partir de esta sentencia veremos que EE.UU toma una posición poco flexible y muy distinta a los ejemplos anteriores ya que las condenas muestran que bajo la CFAA estos tipos de actos son actos criminales y no solo afectan a los ciudadanos sino al propio gobierno federal – independientemente de que el objetivo de Morris no fuese malévolo. Morris diseñó el gusano para demostrar los defectos que existían entonces en los sistemas de seguridad[45] (fin académico)- al contrario que la gran mayoría de gusanos que existen en Internet hoy en día (buscan colapsar los ordenadores y redes informáticas).

2. Power Ventures v. Facebook (2016)

Esta sentencia[46] arrojó un poco de luz sobre las prácticas empresariales de Facebook en relación con el almacenamiento de datos de sus usuarios y el 'data scraping' o 'web scraping' (extracción y almacenamiento de información de otras páginas web).

Steve Vachani, anterior CEO de Power Ventures, fue el primero que se enfrentó al gigante Facebook. Su empresa desarrollaba una plataforma central para que sus usuarios (aquellos que voluntariamente diese su consentimiento) pudiesen agregar a un único sistema los perfiles que tenían en todas sus redes sociales. En su punto álgido llegó a tener 20 millones de usuarios,[47] pero no duró mucho por culpa de los juicios con

[45] Timothy B. Lee "How a grad student trying to build the first botnet brought the internet to its knees," Washington Post, 01/11/13 (disponible en https://www.washingtonpost.com/news/the-switch/wp/2013/11/01/how-a-grad-student-trying-to-build-the-first-botnet-brought-the-internet-to-its-knees/?utm_term=.b16bd6873c4f ; última consulta 07/02/19)
[46] Facebook, Inc v. Power Ventures Inc, US Court of Appeals, 9th Circuit, 12/07/16 (disponible en https://caselaw.findlaw.com/us-9th-circuit/1741713.html ; última consulta 26/03/19)
[47] Aarti Shahani, "The Man Who Stood Up To Facebook," NPR, 13/11/16 (disponible en https://www.npr.org/sections/alltechconsidered/2016/10/13/497820170/the-man-who-stood-up-to-facebook ; última consulta 07/02/19)

Facebook. Desde entonces Power Ventures quebró, Vachani declaró bancarrota y pocos se han vuelto a enfrentar a Facebook.

Power Ventures animaba a sus usuarios a que invitasen a amigos suyos a probar su plataforma mediante la herramienta de 'eventos' en Facebook. A raíz de ello, Facebook interpuso una demanda y tachó a Vachani de 'spammer' y 'hacker' - a pesar de que los usuarios de Power Ventures daban su consentimiento para amalgamar sus cuentas en una única plataforma, y aunque únicamente eran alegaciones, causaron mucho daño a la empresa. La clave era contestar a la siguiente pregunta en el marco de la CFAA – si un grupo de individuos utilizan dos redes sociales, ¿puede una de estas empresas (que cuenta con el consentimiento previo de estos usuarios) acceder a los datos almacenados por la otra empresa (datos sobre los mismos usuarios)? Según el 9th Circuit Court, esto sí constituye una violación de la CFAA (18 U.S.C. § 1030 (a) (2) (c)); "a defendant can run afoul of the CFAA when he or she has no permission to access a computer or when such permission has been revoked explicitly," (828 F.3d 1068 de la sentencia).

3. Operación Aurora (2009) y Westinghouse (2014)

'Operación Aurora' es el nombre que la comunidad internacional le ha puesto a una serie de ciberataques a empresas de Silicon Valley (Google, Adobe Systems, Dow Chemical, entre otras) y supuestamente procedentes de China. Este caso es importante porque atrajo a muchos medios de comunicación dadas las muchas pruebas que parecía haber (malware que utiliza sistema chino, el idioma etc…), sin embargo, las autoridades EE.UU decidieron no realizar ningún acto de atribución en base a que no tenía suficientes pruebas para atribuir la operación directamente al gobierno chino.

Google fue la primera que dio la voz de alarma en enero del 2010, declarando[48] que a mediados de diciembre del año anterior había detectado un ataque altamente sofisticado procedente de China. Poco tiempo más tarde las demás compañías que habían sido

[48] Google Official Blog, "A New Approach to China," Google, 12/01/10 (disponible en https://googleblog.blogspot.com/2010/01/new-approach-to-china.html ; última consulta 06/02/19)

víctimas de éste ataque revelaron que ellas también habían sido víctimas. Esto supuso un gran cambio en la tendencia que existía hasta entonces de esconder estos escándalos (el admitir que datos personales o información confidencial ha sido robada puede tener efectos muy perjudiciales para las empresas, como por ejemplo asustar o ahuyentar a los inversores y causar una bajada de su valor de cotización etc…) – motivo por el cual fue Google la primera multinacional en divulgarlo[49].

Según la propia publicación de Google[50], el principal objetivo de estos individuos era adquirir información sobre disidentes chinos (en este caso, activistas y defensores de derechos humanos). Sin embargo, la empresa tecnológica Damballa (se dedica a investigar y detectar botnets y APTs) concluyó[51] que las técnicas utilizadas y el origen de los ciberataques de Operación Aurora provenía de novatos utilizando 'herramientas sencillas,' en dos universidades chinas. A pesar de todo lo anterior, no se realizó ninguna atribución formal.

Sin embargo, pocos años más tarde el gobierno EE.UU cambia de posición; el caso Westinghouse (2014) es emblemático por ser la primera vez que un país acusaba formalmente a otro de ciberespionaje. Esta vez consideró que contaba con pruebas suficientes como para sustentar una convicción bajo la CFAA.

En 2014 y a raíz del ciberataque que sufrieron varias empresas de la industria del acero americana[52] salió a la luz información sobre una unidad hasta entonces secreta del ejército Chino, denominada 'unidad 61398.' Éste grupo es operado por el gobierno chino y se dedica a sabotaje y espionaje industrial cibernético de empresas americanas para realizar los objetivos 'Made in China 2025,' y el gobierno de Obama sorprendió a la

[49] Adobe Systems, por ejemplo, publicó su artículo 15 minutos después de que Google admitiese que su infraestructura interna había sido quebrantada).
[50] Id.
[51] Damballa, "The Command Structure of the Aurora Botnet," Estudio de Damballa Inc, 02/03/10 (disponible en https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2010/Aurora_Botnet_Command_Structure.pdf ; última consulta 06/02/19)
[52] Entre ellas, Westinghouse Electric Company, SolarWorld, U.S. Steel Corporation, y Alcoa Incorporated

comunidad internacional cuando acusó formalmente[53] a cinco individuos de nacionalidad china y miembros de ésta unidad y les declaro responsables del ciberataque de la industria del acero. En la acusación se formularon 31 cargos bajo la CFAA.

Las acusaciones no tardaron en tener efecto ya que los chinos, temporalmente, cambiaron de tácticas y en lugar de depender tanto de las fuerzas armadas optaron por el hacking 'freelance'; es decir, contratando a civiles, e incluso motivó el acuerdo entre EEUU y China en 2015 según el cual ambos acordaron suspender ciberataques para robar propiedad intelectual (incluyendo secretos comerciales e información empresarial de carácter confidencial) e intentar obtener ventajas competitivas.

Sin embargo, desde entonces no hemos visto un descenso en la actividad APT de China por lo que el acuerdo solo parece haber supuesto un suspenso temporal en su actividad (o más bien un cambio temporal de objetivos) y una victoria diplomática entre Obama y Jinping, con escasos efectos prácticos. Tan solo 3 semanas después de su acuerdo, varias empresas del sector farmacéutico americano denunciaron [54] varios ciberataques provenientes de China. Esto unido a los planes de Jinping sobre convertirse en un gran poder en la era cibernética, indudablemente va a causar muchos problemas y no sólo entre EEUU y China.

4. Interferencia en las Elecciones Americanas (2016)

Si comparamos los anteriores casos con el de la interferencia rusa en las elecciones americanas, sorprende el que el propio gobierno no haya tomado ninguna iniciativa en base a la CFAA, sin embargo como veremos a veces no interesa formular una atribución formal por motivos geo-políticos.

[53] United States v. Dong , 01/ 05/2014, U.S. District Court, Western District of Pennsylvania
[54] Adam Segal, "Why China Hacks the World," Christian Science Monitor, 31/01/16 (disponible en https://www.csmonitor.com/World/Asia-Pacific/2016/0131/Why-China-hacks-the-world ; última consulta 06/02/19)

El origen de la interferencia en las elecciones americanas del 2016 lo encontramos en una llamada de teléfono realizada por el Agente Especial Adrian Hawkins (F.B.I.) al DNC ('Democratic National Committee' o 'Comité Nacional Democrático') en Septiembre de 2015. Hawkins llamó para avisar a la DNC de que al menos un ordenador de la DNC había sido accedido por un grupo de hackeadores conocido como 'the Dukes' y vinculado al gobierno ruso. Sin embargo, Yared Tamene, quien contestó la llamada no era un experto en ciberseguridad ni se puso en contacto con uno. El Sr. Tamene no tenía forma de ratificar si era realmente un agente especial (podría haberse tratado también de una broma telefónica) por lo que no lo dio mucha importancia[55]. Lo que quizá no se comenta tanto es que el edificio del DNC se encuentra a tan solo pocos minutos andando de la sede de la FBI.

El acceso inicial se produjo por unos '*spear-phishing emails'* (correos fraudulentos destinados a personas específicas y enviados con la intención de hacer que el recipiente haga 'click' en un lugar del correo, en cuyo caso se suele descargar software malicioso que proporciona a los infractores acceso al sistema) dirigidos a varios altos cargos del DNC, en especial los individuos más cercanos a Hilary Clinton. Entre ellos estaban John D. Podesta[56] (expresidente de la campaña de H. Clinton), Debbie Wasserman Schultz (presidenta de la DNC en Florida), y otros. Se publicaron cientos de correos privados de Clinton que tuvieron un gran impacto sobre las elecciones ya que revelaron sus debilidades, sus correos electrónicos privados y conversaciones privadas con altos cargos de agencias federales americanas (por ejemplo con el director del FBI, James B. Corney). Todo ello en beneficio del otro candidato: Trump.

Unido a ello, según el Informe del Comité de Inteligencia del Senado[57], la campaña publicitaria dirigida por la empresa 'Internet Research Agency' perteneciente a Yevgeny

[55] Eric Lipton, David E. Sanger, Scott Shane, "The Perfect Weapon: How Russian Cyberpower invaded the U.S." NY Times, 13/12/16 (disponible en https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html : última consulta 07/02/19)

[56] Cabe mencionar que en el caso del Sr. Podesta, Director de la campaña de H. Clinton, ni siquiera tenía activado '*two-factor authentication*.'

[57] Scott Shane, Sheera Frenkel "Russian 2016 Influence Operation Targeted African-Americans on Social Media," N.Y. Times, 17/12/18 (disponible en https://www.nytimes.com/2018/12/17/us/politics/russia-2016-influence-campaign.html ; última consulta 07/02/19)

V. Prigozhin (aliado cercano de Putin) utilizó miles de botnets para crear cuentas falsas, crear publicidad engañosa (siempre haciéndose pasar por americanos) y hacer que la balanza se inclinase en contra de H. Clinton. Al parecer, se dirigieron en su mayoría a la comunidad afroamericana, por ejemplo; creando páginas de web dedicadas exclusivamente a la brutalidad policial (de los 81 páginas de Facebook creadas, 30 de ellas iban dirigidas a la comunidad afroamericana)[58]. Era un intento de dividir a las masas americanas por motivos raciales.

La interferencia rusa en las elecciones americanas tuvo gran importancia al ser la primera vez que se hacía pública la utilización del ciberespionaje y una campaña de información para interferir en las elecciones de otro país. Aquí, la descoordinación entre las agencias americanas, falta de importancia que le dieron al ataque y la reticencia del gobierno americano por tomar medidas desde un primer momento – fueron todos factores que contribuyeron a que los hackers rusos pudiesen navegar libremente en la red interna de la DNC durante 7 meses (al cabo de este tiempo alertaron a los individuos cuyas cuentas habían sido comprometidas y contrataron a expertos para proteger sus sistemas).

Lo que no estaba tan claro era cómo iba a responder el gobierno americano a Moscú. Tampoco habían muchas opciones; a) confrontar abiertamente a los rusos (lo cual era peligroso dada la situación vulnerable en la que se encontraba EE.UU estando en medio de las elecciones), b) imponer sanciones a Putin, c) responder de la misma forma que fueron atacados, o d) ir a por el círculo cercano de oligarcas rusos de Putin (y consigo cortar su acceso a cuentas de banco secretas en Europa y Asia). Las autoridades americanas, comentando las conclusiones a las que había llegado Obama sobre cómo responder a Putin; "*The only thing worse than not using a weapon is using it ineffectively. And if he does choose to retaliate, he has insisted on maintaining what is known as 'escalation dominance,' the ability to ensure that you can end a conflict on your terms.*"[59]

[58] Id.
[59] David E. Sanger "Obama Confronts Complexity of Using a Mightly Cyberarsenal Against Russia," N.Y. Times, 17/12/19 (disponible en https://www.nytimes.com/2018/12/17/us/politics/russia-2016-influence-campaign.html ; última consulta 06/02/19)

¿Qué recursos legales se podían haber usado? De acuerdo con el CFAA, EE.UU podía haber fundado una respuesta en alguno de los siguientes artículos:

- 18 U.S.C. 1030(a)(1)
- 18 U.S.C. 1030(a)(2)
- 18 U.S.C. 1030(b)
- 18 U.S.C 1030(g)

4.iii Aplicación de la Normativa de China

La Ley de Ciberseguridad de 2016 entró en vigor en 2017 y no contamos con muchos precedentes para analizar su aplicación. Desde su promulgación se han publicado 15 casos, de los cuales la mayoría se centran en la implementación de la ley a nivel local (es decir, se centra en los negocios pequeños)[60] y los tribunales han impuesto penas, por lo general, leves - entre ellas, la imposición de un plazo de 15 días para rectificar una medida, o multas de entre 10.000 RMB a 500.000 RMB.

De entre esos 15 casos, cabe hacer mención al caso de las redes sociales (chinas) de 2017, a continuación, por ser la primera investigación formal realizada bajo la Ley de Ciberseguridad. Las plataformas grandes americanas, como por ejemplo Facebook, Whatsapp, Twitter, Google, Instagram etc... están prohibidas en China (motivos de censura) y en lugar de las plataformas americanas, China cuenta con sus propias versiones, como por ejemplo: WeChat, Weibo, Baidu, Douyin etc...

La nueva normativa de ciberseguridad ha introducido requisitos más rigurosos - a comparación con la regulación de otros países - y reflejan la tendencia y estrategias que ha ido emprendiendo China para evolucionar desde su mundialmente conocido 'Made in China 2025' a 'inventado en China.' La regulación anterior forma parte de su ideal de

[60] Sobretodo redes sociales (entre ellas Baidu Tieba), plataformas de compra online (por ejemplo Taobao, 58.com), y empresas tecnológicas (Alibaba Cloud)

dejar de ser uno de los líderes a nivel mundial en fabricación de productos de baja calidad (de ahí 'Made in China') para convertirse en el país número 1 en fabricación a nivel mundial[61] antes del año 2049. Ello implica reducir su gran dependencia en tecnología extranjera en aras a alcanzar independencia en el mundo digital. Muestra de ello lo encontramos en el discurso del Presidente Xi Jinping en Junio 2014 en la Conferencia Nacional de Ciencias y Tecnología[62] ; "*Only if core technologies are in our hands can we truly hold the initiative in competition and development*," y añadió que ésta era la única manera de proteger su economía nacional, defensa, y otras áreas en el campo de defensa. En este sentido, prohibió que el gobierno chino utilizase iPads, MacBooks, y productos de Microsoft y Symantec (empresas americanas) para fomentar así la dependencia sobre compañías chinas[63] - de ahí que no sea sorprendente el contenido del artículo 37 comentado anteriormente.

El problema con fomentar la industria tecnológica China es que ha ido de la mano de un aumento descontrolado en actividad ilícita en el ciberespacio (al menos en base a los estándares europeos) y hemos visto un aumento preocupante en la cantidad de ciberataques con origen en China, analizado más en adelante.

Según algunos comentaristas[64], el ambiente 'hacker' en China no se compone de grupos secretos y estructurados sino más bien de patriotas desorganizados que son contratados por las autoridades chinas para desempeñar labores concretas. La mayoría de las veces el propio gobierno ignora estas actividades ilícitas porque solapan con los intereses del gobierno de Xi Jinping, de ahí que se diga que hay una regla implícita según la cual los hackers freelance son libres para atacar a quienes quieran, siempre y cuando el objetivo sea empresas extranjeras y que el gobierno chino únicamente tomará medidas cuando el

[61] Peter Pham, "What Will China's Future Look Like ?" Forbes Magazine, 07/03/18 (disponible en https://www.forbes.com/sites/peterpham/2018/03/07/what-will-chinas-future-look-like/#6af036867488 ; última consulta 07/02/19)
[62] Tom Warren, "China bans iPads and MacBooks from government use in clampdown on US companies." The Verge Magazine, 06/08/14, (disponible en https://www.theverge.com/2014/8/6/5974313/chinese-government-bans-apple-ipads-and-macbooks ; última consulta 05/02/19)
[63] Id.
[64] Mara Hvistendahl, "China's Hacker Army," Foreign Policy Magazine, 14/03/10, (disponible en https://foreignpolicy.com/2010/03/03/chinas-hacker-army/ ; última consulta 06/02/19)

objetivo sea las empresas nacionales[65] - pero esto parece haber cambiado con el caso WeChat, Weibo y Baidu analizado a continuación.

WeChat, Weibo, y Baidu (2017)

A mediados del 2017, las autoridades anunciaron[66] el comienzo de investigaciones sobre 3 redes sociales, WeChat, Weibo y Baidu, por presuntas violaciones de la Ley de Ciberseguridad. Acusaron a las empresas de difundir información prohibida (temores de que se estaban utilizando para difundir rumores falsos, obscenidades y contenidos violentos) y de no cumplir con sus deberes de gestión (protección de información de sus usuarios). De acuerdo con el gobierno, suponía la difusión de este material un peligro para "la seguridad nacional, la seguridad pública y el orden social."[67]

Las autoridades anunciaron en septiembre de 2017 la imposición de la máxima multa contenida en la Ley de Ciberseguridad - según el artículo 68 son 500.000 RMB (o entre 10.000 RMB y 100.000 RMB en caso de ser un particular) – pero no publicaron la decisión.

Este caso marca un cambio importante en la postura del gobierno en lo relativo a la aplicación de la normativa de ciberseguridad (Ley de Ciberseguridad) ya que hasta este momento, estas empresas habían logrado 'escapar' hasta cierto punto estos tipos de controles gracias a su origen chino - por lo que ya tenían incorporados la censura en sus sistemas. Desde entonces solo ha ido a más, ese mismo año las autoridades clausuraron

---

[65] Id.
[66] Market Watch, Chinese probe Targets Weibo, WeChat, Baidu site over threat to public security," 11/08/17 (https://www.marketwatch.com/story/social-media-sites-run-by-baidu-others-under-probe-for-possibly-breaking-china-cybersecurity-law-2017-08-11; última consulta 26/03/19)
[67] Europapress, "China investiga a sus dos principales redes sociales, WeChat y Weibo," Petar Kudjundzic, 11/08/17 (disponible en: https://www.europapress.es/internacional/noticia-china-investiga-dos-principales-redes-sociales-wechat-weibo-20170811154741.html ; última consulta 27/03/19)

aproximadamente 60 páginas web que hablaban de famosos, por entender que dañaba "los valores socialistas básicos."[68]

Este caso tuvo repercusiones para las empresas investigadas por la interrupción en su funcionamiento (por ejemplo, Weibo tuvo que cerrar obligatoriamente su plataforma de forma parcial, lo que ocasionó una pérdida de aproximadamente US $1.300 millones para Weibo y su empresa matriz, Sina Corp.). Además, la investigación tuvo repercusiones negativas en la bolsa de Hong Kong ya que las 3 empresas investigadas sufrieron pérdidas de al menos 5% en bolsa. En este sentido, la nueva normativa constituye también una preocupación para los inversores porque desde su promulgación ha ocasionado pérdidas millonarias para las empresas[69]. La 'soberanía cibernética' claramente es una prioridad para el gobierno de Xi Jinping.

4.iv Aplicación de la Normativa de Rusia

En el periodo transcurrido entre 2007 y 2016, la Ley de Datos Personales casi no se invocaba, pero esto cambió de forma repentina con el caso de LinkedIn en 2016 en el cual la sentencia de un tribunal de distrito de agosto de 2016 resultó en la prohibición de LinkedIn en territorio ruso.

1. LinkedIn (2016)

Mediante sentencia de 4 de agosto de 2016, el tribunal condenó a LinkedIn (compañía estadounidense adquirida por Microsoft en el 2016), en base a su incumplimiento con la normativa de protección de datos, Ley de Datos Personales, que obliga a las empresas a almacenar información en Rusia y utilizar bases de datos ubicadas en Rusia.

[68] Ticbeat, "La máquina de la censura china apunta ahora hacia WeChat, Baidu, y Weibo," 11/08/17(disponible en https://www.ticbeat.com/seguridad/la-maquina-de-la-censura-china-apunta-ahora-hacia-wechat-baidu-y-weibo/ ; última consulta 27/03/19)
[69] Id. at 63.

Esta decisión (avalada por dos sentencias judiciales: un tribunal de primera instancia y otro de segunda instancia) es importante porque es la primera gran plataforma/ red social que bloquea el gobierno ruso en base a la normativa de ciberseguridad y protección de datos y establece un precedente importante que afectará como operarán las empresas, extranjeras y nacionales, en Rusia.

A día de hoy LinkedIn sigue estando prohibido en Rusia. A diferencia de la prohibición de otros servicios de mensaje instantáneo (como por ejemplo Blackberry Messenger), el caso de LinkedIn fue muy documentado por los medios de comunicación debido a su utilización generalizada - por aquel entonces contaba con aproximadamente 6 millones de usuarios en Rusia. Casi inmediatamente después de la prohibición de LinkedIn, un empresario ruso llamado Serguéi Kravtsov, propietario de la empresa OMMG Technology, creó y lanzó (la misma semana que las autoridades anunciaron la prohibición de LinkedIn) una aplicación análoga a LinkedIn, llamada Link You[70] aunque muchos expertos opinan[71] que no tendrá el mismo éxito que LinkedIn.

Desde su prohibición muchos han criticado al gobierno encuadrándolo en la lucha contra la censura pero el Kremlin ha negado estas acusaciones. Según Dmitri Peskov[72], portavoz de la presidencia, el organismo encargado de aplicar la sentencia, el organismo regulador de telecomunicaciones, únicamente están acatando estrictamente la ley y las autoridades ya avisaron varias veces a empresas del sector, entre ellas Facebook y Twitter (sin imponer ninguna sanción hasta el caso de LinkedIn).

[70] RBTH, "Tras la prohibición, aparece un análogo de LinkedIn en Rusia," Russia Beyond, Izvestia, 24/11/16 (disponible en https://es.rbth.com/cultura/technologias/2016/11/24/tras-la-prohibicion-aparece-un-analogo-a-de-linkedin-en-rusia_650663 ; última consulta 27/03/19)
[71] Id.
[72] Diario El Comercio, "Rusia bloquea la red social LinkedIn," Agencia AFP, 17/11/16 (disponible en https://www.elcomercio.com/guaifai/linkedin-redessociales-bloqueo-rusia-datos.html. ; última consulta 23/03/19)

2. *Telegram (2018)*

En el caso de Telegram[73] (empresa que proporciona servicios de mensajes instantáneos), la plataforma más popular en Rusia, las autoridades rusas reclamaron la falta de conformidad de Telegram con la Ley de Datos Personales ya que ésta obliga a que las empresas proporcionen claves específicas al gobierno ruso (para así descifrar mensajes de los usuarios de estos servicios y leer la correspondencia), a lo que Telegram se negó (fundamentando esta alegación en que sería imposible acatar esta norma por la encriptación end-to-end que utilizan).

Su fundador, Pavel Durov alegó que dicha imposición violaba el derecho a la privacidad o secreto de la correspondencia y que por lo tanto era inconstitucional. El Sr. Durov ha hecho varias proclamaciones sobre ello, por ejemplo en su cuenta de Twitter el Sr. Pavel escribió "La privacidad no está a la venta y los derechos humanos no deberán verse comprometidos por el miedo y la codicia,"[74] y "Threats to block Telegram unless it gives up private data of its users won't bear fruit. Telegram will stand for freedom and privacy.[75]" Además añadió que aunque solamente afecta a un porcentaje de usuarios relativamente bajo (a nivel mundial Telegram tiene 100 millones de usuarios, de los cuales hay 14 millones en Rusia), este tema era "especialmente importante," para él[76].

Por su lado, la FSB argumentaba que la información solicitada (correspondencia entre los usuarios de Telegram) no constituía 'secreto de correspondencia.'

Al cabo de un periodo de 30 minutos; tiempo que duró el Tribunal del Distrito Taganski en estudiar las pruebas en contra de Telegram (y en ausencia de representantes para Telegram), el tribunal dictó sentencia y ordenó el bloqueo inmediato de Telegram a

[73] BBC, "El Intento Frustrado de Rusia para bloquear Telegram que dejó inactivas 18 millones de IPs de Google y Amazon", 18/04/18 (disponible en https://www.bbc.com/mundo/noticias-43810964 ; última consulta 25/03/19)
[74] Id.
[75] El Mundo,"Rusia logra el bloqueo de Telegram," 13/04/18 (disponible en https://www.elmundo.es/tecnologia/2018/04/13/5ad06ef7e2704e90058b4590.html ; última consulta 26/03/19)
[76] Id at 58.

menos que proporcionase a las autoridades (Servicio Federal de Seguridad) las claves. Sin embargo, no acabó ahí el problema ya que desde entonces Telegram ha estado utilizando distintas direcciones IP para eludir el bloqueo. Desde que se dictó sentencia las autoridades rusas solamente han conseguido bloquear aproximadamente el 30% de las redes de Telegram[77].

Sin embargo, no es la primera vez que Telegram se enfrenta a la Ley de Datos Personales, ya que a finales del 2017 fue multado 800.000 rublos[78] (aproximadamente US$ 14.000) por incumplimiento de ésta ley, ésta vez en el marco de la imposición de medidas para luchar contra el terrorismo. También en el 2014, su fundador, el Sr. Durov decidió marcharse de Rusia por las 'presiones' que sufría por parte de las autoridades rusas para que revelara información sobre los usuarios, miembros de la oposición, de la aplicación VKontakte - otra plataforma desarrollada por el Sr. Durov.

5. Hackback

Como hemos visto en los ejemplos analizados antes, a veces la respuesta de las autoridades para hacer frente a las amenazas cibernéticas es insuficiente (bien sea por falta de jurisdicción o competencia, presiones políticas, insuficiencia normativa etc…) o es demasiado lenta (trámites burocráticos y procedimientos judiciales prolongados). Por tanto cabe preguntar si debemos instituir y regular alternativas (más rápidas y/o eficientes) que puedan emprender las empresas para hacer frente a estas amenazas. Doctrinalmente esto se conoce como el ‘hackback’ o ‘defensa activa’ (término que en la ciberseguridad hace referencia al ‘ofensiva’) y hay muchas empresas y analistas que abogan por ello, pero como veremos, no es la respuesta adecuada ante estas nuevas amenazas.

[77] Id.
[78] Id.

5.i Ventajas del Hackback

Para enfocar el estudio, nos debemos preguntar si nos interesa que en algunas circunstancias personas/empresas del sector privado puedan acceder a los sistemas informáticos de otro (y quizá sin su conocimiento). Por ejemplo, ¿qué debe hacer Empresa A (empresa domiciliada en España) si averigua que Empresa B (domiciliada en Francia) está accediendo a la red de la Empresa A y extrayendo archivos que contienen información confidencial? Obviamente debe emprender la vía legal para solucionar el problema, pero cabe preguntarnos si merece la pena regular el hackback por ser más eficiente.

Las ventajas del hackback se detallan a continuación:

1) Como los 'threat actors' están accediendo actualmente a la red de la empresa, con el hackback podríamos responder de forma más rápida.
    - Si Empresa A dejase el asunto en manos de las autoridades policiales pertinentes - la respuesta/contraataque tendría lugar más tarde y quizá sería demasiado tarde (o imposible) poder localizar a los infractores (Empresa B)
2) Cuánto antes se resuelva este problema, antes podrá resumir la empresa su actividad normal.
    - Empresa A se encuentra en una situación delicada ya que en el presente le están robando archivos que contienen información trascendental para el funcionamiento normal y desempeño de sus funciones.
3) Mediante el hackback la empresa puede defender sus propios intereses.
    - ¿Debería quedarse Empresa A 'sin hacer nada' - sabiendo que los infractores están actualmente robando archivos que contienen información confidencial o esencial para el desempeño de su actividad?
4) ¿Estado de necesidad? Se podría argumentar estado de necesidad (en ocasiones el estado de necesidad se utiliza para crear espectáculo en los juicios pero en la práctica no se utiliza mucho porque es una postura difícil de defender).

A pesar de estas ventajas, la política del hackback tiene mayores y más importantes inconvenientes que se detallan a continuación.

5.ii Inconvenientes del Hackback

1) El hackback implica utilizar métodos afines a los que se utilizaron para perpetrar el ataque inicial.
    - (Continuamos con el ejemplo anterior) Empresa A tendría que contar previamente con los recursos suficientes y personal adecuado como para contraatacar.
2) Muchas veces es difícil medir los efectos del contraataque de forma que es casi seguro que le respuesta de la víctima no sea proporcional a la primera infracción. Tendríamos que valorar qué tipos de respuestas se consideran proporcionales al ataque inicial.
    - Empresa B ha accedido a la red interna de la Empresa A y está exfiltrando archivos, ¿estaría en su derecho Empresa A acceder al servidor de Empresa B y borrar todos los archivos robados?
3) En un principio, en estas operaciones no conocemos donde se sitúan los threat actors (pueden encontrarse a pocos metros de nosotros, en otra ciudad, en la otra punta del mundo o en un país con un líder inestable como por ejemplo Corea del Norte).
4) No sabemos cuál va a ser la respuesta a un hackback.
    - En el ejemplo solamente es posible conocer la identidad o la localización del delincuente una vez que Empresa A haya accedido a los sistemas de Empresa B (hasta entonces no se sabe quien ha iniciado el ataque ni en qué país se encuentra).
    - Existe la posibilidad de que el país en el cual se encuentre Empresa B (en este ejemplo Francia) contraataque dado la conducta de hackback de Empresa A. Éste contraataque podría originar una guerra cibernética entre los dos países o iniciar represalias sobre la infraestructura esencial de uno de ellos. Puede originar un círculo vicioso.

- ¿Qué pasaría si en lugar de ser ‘Empresa B, una empresa domiciliada en Francia,’ fuese el gobierno de Corea del Norte ?

5) ¿Qué pasa si nos equivocamos y hackeamos otro?
   - Existe la posibilidad de que en lugar de contraatacar a Empresa B en Francia, Empresa A realice el hackback contra Empresa C que se encuentra en otro país. En este caso, ¿cómo se corrige esta situación?
6) Puede ser investigado por las autoridades y conllevar la imposición de penas tanto nacionales como extranjeras. También, si los threat actors son extranjeros, existe la posibilidad que el hackback viole leyes extranjeras.
   - Al igual que la conducta de Empresa B conlleva la imposición de una pena en España, es altamente probable que el contraataque realizado por Empresa A esté penado por legislación francesa.

III. Conclusiones

1. Marco Legal

Partiendo de la base de que el software perfecto no existe[79] (es decir, que cualquier programa puede tener vulnerabilidades y errores) y que la mayoría de países de Europa occidental siguen sufriendo APTs como los desarrollados en este trabajo (siguen en aumento), llegamos a la conclusión de que es necesario reforzar la normativa existente para realizar cambios y proteger a tanto particulares como a empresas de las amenazas cibernéticas.

Más importante aún es que las leyes existentes sigan en paralelo el desarrollo de la nuevas tecnologías en el área de ciberseguridad, porque como hemos visto, de lo contrario se pierde mucho tiempo valioso en analizar las distintas repercusiones que puede tener el tomar una vía legislativa en comparación con otra, mientras que los 'threat actors' desaparecen (quedando impunes), y dejando a muchos desprotegidos (víctimas de los ciberataques y stakeholders). También, de esta forma eliminamos la posible institución del hackback o defensa activa como alternativa a la vía legal convencional, dados los varios inconvenientes que conlleva este tipo de respuesta.

Asimismo, es recomendable reforzar la cooperación entre países (también entre países y el sector privado) y homogeneizar la regulación para disminuir este tipo de amenazas ya que claramente se trata de una amenaza transfronteriza, constituye un peligro preocupante (por incidir sobre la paz internacional) y afectar a los derechos fundamentales de los individuos. Más allá del Convenio de Budapest, puede ser que haga falta un tratado internacional en materia de ciberseguridad y protección de datos, que defina de manera más clara los instrumentos legales y mecanismos de cooperación a utilizar. El Convenio de Budapest representa un logro en cuanto primer intento hacía la homogeneización normativa en materia de ciberseguridad y protección de datos, pero es insuficiente por la falta de obligatoriedad (únicamente constituye un estándar que pueden utilizar los países),

[79] Tampoco existe el incentivo para desarrollarlo

no proporciona una solución a qué ocurre si es un gobierno quien está detrás de la ciberamenaza y no tiene en cuenta que todos los Estados son iguales.

2. Financiación

Para continuar luchando contra los ciberataques es necesario ampliar la inversión a nivel global en seguridad cibernética. Esto debe de ser prioritario para los gobiernos – aunque como hemos visto, para algunos como por ejemplo China ya es una prioridad - y también para el sector privado; las empresas deberán acatar la nueva legislación promulgada e invertir ellas mismas en técnicas de seguridad y personal adecuado para protegerse en el ámbito de la ciberseguridad y protección de datos.

3. Aumentar Resistencia

Para aumentar la resistencia a los ciberataques es necesario tanto aumentar la inversión destinada a su prevención como aumentar la inversión para las situaciones en las cuales ya se ha producido un ciberataque – y así recuperarse lo antes posible. Dados los avances en el IoT, las amenazas y posibles fuentes de amenazas son tan variadas que es imposible prevenir todos los ciberataques.

En este sentido, puede ser necesario dotar a (algunas) autoridades de mayor poder/ facultades de investigación, vigilancia y mecanismos de supervisión para poder perseguir estos delitos. Por otro lado, el aumentar estas facultades puede no ser apropiado para todos los países, de hecho sería arriesgado en el caso de países autoritarios que ya utilizan estos tipos de herramientas en contra de sus propios ciudadanos, por tanto sería necesario que estas medidas contasen con suficientes garantías de transparencia y objetividad para así no ser objeto de abuso.

Por último, los hackers claramente se aprovechan de la ingenuidad de los usuarios de internet a la hora de ejecutar sus objetivos por lo que una de las formas de reducir o dificultar su trabajo es concienciar a los particulares/ empresas sobre los peligros (por

ejemplo no abrir archivos maliciosos o desconocidos por la posibilidad de que escondan malware). De esta forma se dificultaría de cierto modo el que se pueda construir un botnet. También es muy recomendable el descargar las nuevas actualizaciones del software cuanto antes sea posible (aunque siendo realistas son pocos quienes se descargan inmediatamente una actualización cada vez que se publica) y utilizar programas antivirus.

Bibliografía

A. Legislación

- Comisión Europea, "Estrategia de Ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro," Consejo de la Unión Europea, 07/02/13 (disponible en http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=es ; última consulta 08/02/19)
- Directiva 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (19/07/16)
- Directiva 95/46/EC del Parlamento Europeo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (23/11/1995)
- Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (04/05/2016)
- Cybersecurity Law of the People's Republic of China, passed November 6, 2016, effective June 1, 2017, (http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm), traducida: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ , última consulta 25/03/19)
- National People's Congress Standing Committee Decision concerning Strengthening Network Information Protections, China Copyright and Media, 28/12/12 (disponible en https://chinacopyrightandmedia.wordpress.com/2012/12/28/national-peoples-congress-standing-committee-decision-concerning-strengthening-network-information-protection/ ; última consulta 25/03/19)

- Ley sobre Seguridad de la Infraestructura de Información Crítica para Rusia, N. 187-FZ, 26/07/17
- Ley de Datos Personales, N. 152-FZ, 27/07/06
- Ley Federal sobre Información, Tecnología de la Información y Protección de la Información, N. 149-FZ, 27/07/06
- Convenio sobre Cibercriminalidad, hecho en Budapest, de 23 de noviembre de 2001
- Reglamento de Ejecución (UE) 2015/2447, de la Comisión de 24 de noviembre de 2015, por el que se establecen normas de desarrollo de determinadas disposiciones del Reglamento UE n. 952/2013 del Parlamento Europeo y del Consejo por el que se establece el código aduanero de la Unión, 29.12.2015
- Ley. Orgánica. 10/1995, de 23 de noviembre del Código Penal

B. <u>Jurisprudencia</u>

- United States of America v. Dmitry Dokuchaev, Igor Suschin, Alexsey Belan and Karim Baratov, US District Court, Northern District of California, San Francisco Division, 2017 Indictment
- Nowak v. Data Protection Commissioner, Sentencia del Tribunal de Justicia de la Unión Europea de 20 de diciembre de 2017, asunto: C-434/16, ECLI: EU:C:2017:994
- Deutsche Post AG y Hauptzollamt Koln, Sentencia del Tribunal de Justicia de la Unión Europea de 20 de diciembre de 2017, asunto: C-496/17, ECLI: EU:C:2019:36
- United States v. Morris (United States Court of Appeals, Second Circuit, 1991) (disponible en https://h2o.law.harvard.edu/collages/41678 ; última consulta 07/02/19)
- Facebook, Inc v. Power Ventures Inc, US Court of Appeals, 9th Circuit, 12/07/16 (disponible en https://caselaw.findlaw.com/us-9th-circuit/1741713.html ; última consulta 26/03/19)
- Casos Operación Aurora (2009) y Westinghouse (2014)

- United States v. Dong , 01/ 05/2014, U.S. District Court, Western District of Pennsylvania
- Caso WeChat, Weibo, y Baidu (2017)
- Caso LinkedIn (2016)
- Caso Telegram (2018)

C. Obras Doctrinales

- Informe de Hootsuite y We are Social, "Digital 2019: Global Digital Overview," DataReportal, 31/01/19 (disponible en https://datareportal.com/reports/digital-2019-global-digital-overview ; última consulta 06/02/18)
- Informe de Hootsuite y We are Social, "Digital 2019: Spain," DataReportal, 31/01/19, (disponible en https://datareportal.com/reports/digital-2019-spain?rq=spain, última consulta 05/02/19)
- RAND Europe, "A Focus on Cybersecurity." Informe de RAND Corporation, (disponible en https://www.rand.org/content/dam/rand/pubs/corporate_pubs/CP800/CP871-1/RAND_CP871-1.pdf ; última consulta 04/02/19)
- RAND Corporation Research Series, National Security Research Division "Markets for Cybercrime Tools and Stolen Data," RAND Study, 2014 (disponible en https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf , última consulta 06/02/19)
- MarketWatch, "How the number of data breaches is soaring – in one chart," Victor Reklaitis, 25/05/18 (disponible en: https://www.marketwatch.com/story/how-the-number-of-data-breaches-is-soaring-in-one-chart-2018-02-26 ; última consulta 02/04/19)
- Informe IOCTA, Internet Organised Crime Assessment, 2018, Europol, EC3 European Cybercrime Centre

- Redacción, “GDPR: La nueva regulación de protección de datos impulsará el mercado único digital,” Revista electrónica TechWeekly, 20/ 04/18, (disponible en http://www.techweek.es/seguridad/analisis/1018894004801/gdpr-regulacion-proteccion-datos-ue-impulsa-mercado-unico-digital.1.html ; última consulta 06/02/19)
- José Manuel Rodríguez, Beatriz Page, “Cómo te afecta la nueva ley de protección de datos,” Revista electrónica LaVanguardia, 24/05/18 (disponible en https://www.lavanguardia.com/tecnologia/20180524/443785604531/rpgd-proteccion-datos-privacidad-multas-ciudadano.html ; última consulta 06/02/19)
- Ben Popken, “Google sells the future, powered by your personal data,” NBCNews, 10/05/18 (disponible en https://www.nbcnews.com/tech/tech-news/google-sells-future-powered-your-personal-data-n870501 ; última consulta 06/02/19)
- Gemma Galdon Clavell , “Qué hacen con nuestros datos en internet?”, El País, 11/06/15https://elpais.com/tecnologia/2015/06/12/actualidad/1434103095_932305.html ; última consulta 06/02/19)
- El Cronista, "Nueva ley de ciberseguridad china implica más censura," 02/06/17 (disponible en https://www.cronista.com/financialtimes/Nueva-ley-de-ciberseguridad-china-implica-mas-censura-20170602-0059.html ; última consulta 27/03/19)
- European Parliament, Directorate-General For Internal Policies, Policy Department, Citizens’ Rights and Constitutional Affairs, The Data Protection Regime in China (2015) (disponible en: http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA%282015%29536472_EN.pdf ; última consulta 23/03/19)
- Perfil, "La Gran Burbuja: redes sociales en China," Facundo F. Barrio, 14/07/18(disponible en https://www.perfil.com/noticias/elobservador/la-gran-burbuja-redes-sociales-en-china.phtml ; última consulta 27/03/19)
- The Law Reviews Magazine, The Privacy, Data Protection and Cybersecurity Law Review – Edition 5 (disponible en https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-5/1175638/russia ; última consulta 24/03/19)

- Council of Europe, Parties/ Observers to the Budapest Convention and Observer Organisations to the T-CY (disponible en https://www.coe.int/en/web/cybercrime/parties-observers ; última consulta 27/03/19)
- WeLiveSecurity, "Convenio de Budapest: beneficios e implicaciones para la seguridad informática," Cecilia Pastorino, 06/12/17 (disponible en https://www.welivesecurity.com/la-es/2017/12/06/convenio-budapest-beneficios-implicaciones-seguridad-informatica/ ; última consulta 27/03/19)
- New York Times,"Somos los nuevos enemigos del Estado: el espionage a activistas y periodistas en México," Azam Ahmed y Nicole Perlroth, 19/06/17 (disponible en: https://www.nytimes.com/es/2017/06/19/mexico-pegasus-nso-group-espionaje/ ; última consulta 27/03/19)
- Ben Cardin, "Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security," Committee on Foreign Relations, US Senate, 10/01/18 (disponible en https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf ; última consulta 06/02/19)
- El Confidencial, "La campaña de Desinformación Rusa sigue activa en Cataluña," Revista El Confidencial, 22/01/18 (disponible en https://www.elconfidencial.com/mundo/2018-01-22/desinformacion-rusa-cataluna-ben-cardin_1509898/ ; última consulta 07/02/19)
- RTVE, "El ministro de Exteriores ruso bromea con la implicación de Rusia en las elecciones catalanas," (disponible en http://www.rtve.es/noticias/20180928/ministro-exteriores-ruso-bromea-implicacion-rusia-elecciones-catalanas/1808860.shtml ; última consulta 07/02/19)
- Nikita Kovalenko, Ekaterina Korostichenko, "Испания силой подавляет «каталонскую весну»," Periódico Vzglyad, 20/10/17(disponible en https://vz.ru/world/2017/9/20/887874.html ; última consulta 07/02/19)
- Timothy B. Lee "How a grad student trying to build the first botnet brought the internet to its knees," Washington Post, 01/11/13 (disponible en https://www.washingtonpost.com/news/the-switch/wp/2013/11/01/how-a-grad-

student-trying-to-build-the-first-botnet-brought-the-internet-to-its-knees/?utm_term=.b16bd6873c4f ; última consulta 07/02/19)

- Aarti Shahani, "The Man Who Stood Up To Facebook," NPR, 13/11/16 (disponible en https://www.npr.org/sections/alltechconsidered/2016/10/13/497820170/the-man-who-stood-up-to-facebook ; última consulta 07/02/19)
- Google Official Blog, "A New Approach to China," Google, 12/01/10 (disponible en https://googleblog.blogspot.com/2010/01/new-approach-to-china.html ; última consulta 06/02/19)
- Damballa, "The Command Structure of the Aurora Botnet," Estudio de Damballa Inc, 02/03/10 (disponible en https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2010/Aurora_Botnet_Command_Structure.pdf ; última consulta 06/02/19)
- Adam Segal, "Why China Hacks the World," Christian Science Monitor, 31/01/16 (disponible en https://www.csmonitor.com/World/Asia-Pacific/2016/0131/Why-China-hacks-the-world ; última consulta 06/02/19)
- Eric Lipton, David E. Sanger, Scott Shane, "The Perfect Weapon: How Russian Cyberpower invaded the U.S." NY Times, 13/12/16 (disponible en https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html : última consulta 07/02/19)
- Scott Shane, Sheera Frenkel "Russian 2016 Influence Operation Targeted African-Americans on Social Media," N.Y. Times, 17/12/18 (disponible en https://www.nytimes.com/2018/12/17/us/politics/russia-2016-influence-campaign.html ; última consulta 07/02/19)
- David E. Sanger "Obama Confronts Complexity of Using a Mightly Cyberarsenal Against Russia," N.Y. Times, 17/12/19 (disponible en https://www.nytimes.com/2018/12/17/us/politics/russia-2016-influence-campaign.html ; última consulta 06/02/19)
- Peter Pham, "What Will China's Future Look Like ?" Forbes Magazine, 07/03/18 (disponible en https://www.forbes.com/sites/peterpham/2018/03/07/what-will-chinas-future-look-like/#6af036867488 ; última consulta 07/02/19)

- Tom Warren, “China bans iPads and MacBooks from government use in clampdown on US companies.” The Verge Magazine, 06/08/14, (disponible en https://www.theverge.com/2014/8/6/5974313/chinese-government-bans-apple-ipads-and-macbooks ; última consulta 05/02/19)
- Mara Hvistendahl, “China’s Hacker Army,” Foreign Policy Magazine, 14/03/10, (disponible en https://foreignpolicy.com/2010/03/03/chinas-hacker-army/ ; última consulta 06/02/19)
- Market Watch, Chinese probe Targets Weibo, WeChat, Baidu site over threat to public security,” 11/08/17 (https://www.marketwatch.com/story/social-media-sites-run-by-baidu-others-under-probe-for-possibly-breaking-china-cybersecurity-law-2017-08-11; última consulta 26/03/19)
- Europapress, "China investiga a sus dos principales redes sociales, WeChat y Weibo," Petar Kudjundzic, 11/08/17 (disponible en: https://www.europapress.es/internacional/noticia-china-investiga-dos-principales-redes-sociales-wechat-weibo-20170811154741.html; última consulta 27/03/19)
- Ticbeat, "La máquina de la censura china apunta ahora hacia WeChat, Baidu, y Weibo," 11/08/17(disponible en https://www.ticbeat.com/seguridad/la-maquina-de-la-censura-china-apunta-ahora-hacia-wechat-baidu-y-weibo/ ; última consulta 27/03/19)
- RBTH, "Tras la prohibición, aparece un análogo de LinkedIn en Rusia," Russia Beyond, Izvestia, 24/11/16 (disponible en https://es.rbth.com/cultura/technologias/2016/11/24/tras-la-prohibicion-aparece-un-analogo-a-de-linkedin-en-rusia_650663 ; última consulta 27/03/19)
- Diario El Comercio, "Rusia bloquea la red social LinkedIn," Agencia AFP, 17/11/16 (disponible en https://www.elcomercio.com/guaifai/linkedin-redessociales-bloqueo-rusia-datos.html. ; última consulta 23/03/19**)**
- BBC, "El Intento Frustrado de Rusia para bloquear Telegram que dejó inactivas 18 millones de IPs de Google y Amazon", 18/04/18 (disponible en https://www.bbc.com/mundo/noticias-43810964 ; última consulta 25/03/19)

- El Mundo, "Rusia logra el bloqueo de Telegram," 13/04/18 (disponible en https://www.elmundo.es/tecnologia/2018/04/13/5ad06ef7e2704e90058b4590.html ; última consulta 26/03/19)