ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

77bis/2014 14 de julio de 2014

*Henning Wegener**

LA CIBERSEGURIDAD EN LA UNIÓN EUROPEA

LA CIBERSEGURIDAD EN LA UNIÓN EUROPEA

Resumen:

Los comienzos de la política de ciberseguridad en la Unión Europea se puede fijar en la comunicación conjunta del Consejo y la Comisión COM (2000) 890. Se describen las etapas y documentos –y también la normativa de las instituciones correspondientes– que han venido sucediendo con posterioridad y se hace un alto con más detalle en los dos documentos más recientes e importantes: La Estrategia de Ciberseguridad de la Unión Europea de 2013, JOIN (2013) 1 final[1], y la Directiva de Seguridad de las Redes y de la Información (NIS).
A continuación de este breve análisis y las conclusiones correspondientes se tratan, en armonía con el tema de la ciberseguridad, la política europea de protección de datos y de la información con una perspectiva transatlántica, pero también con el trasfondo de la evolución tecnológica en la conexión de datos y *big data*. Finalmente se proponen algunas recomendaciones. Como indica el título del documento, la seguridad de datos - la ciberseguridad- y la protección de datos son dos aspectos inseparables.

Abstract:

The beginning of the Cybersecurity policy in the European Union can be to the joint comunication of the Council and the Commission COM (2000) 890. The phases and documents –and also the norms of the corresponding institutions– that have been issued later are described and a stop is set to detail the two most recent and important documents: the Cibersecurity Strategy of the European Union of 2013, JOIN(2013) 1, and the Directive for Network and Information Security (NIS).

Continuing after this short analysis and the corresponding conclusions, in harmony with the subject of cybersecurity, the european policy on data and information protection is discussed under a transatlantic perspective, but also with the background of technologic evolution in data connection and big data. Finally, some recommendations are proposed. As the title of this document states, data security –cybersecurity– and data protection are inseparable.

[1] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667

*NOTA: Las ideas contenidas en los ***Documentos de Opinión*** son de responsabilidad de sus autores, sin que reflejen, necesariamente, el pensamiento del IEEE o del Ministerio de Defensa.

Palabras clave:

Ciberseguridad, protección de datos, Unión Europea, Estados Unidos.

Keywords:

Cybersecurity, data protection, European Union, United States.

INTRODUCCIÓN

Ante la creciente conciencia que se está generando en ese contexto no se necesita describir los grandes y crecientes peligros de la era digital. Sin embargo, es indispensable subrayar y reafirmar la importancia de una amplia estrategia que atienda a los grandes retos de nuestro tiempo: el control de los peligros de la era digital –incluidos los peligros del uso militar– es una condición necesaria para el funcionamiento en un sentido amplio de nuestras sociedades desarrolladas[2]. Todos sabemos que los retos de la sociedad de la información solo se pueden superar a través de una estrecha cooperación internacional y de una posible normativa y regulación universal.

La política de ciberseguridad global significa la colaboración de los países, pero también la de todos los actores digitales. El planteamiento de la comunidad Multi-Stakeholder está en boca de todos, y lo está porque es irrenunciable. El concepto tradicional de soberanía resulta insuficiente en la lucha contra el ciberconflicto. Ningún estado, ningún grupo de estados y ninguna organización internacional son autónomos respecto a la situación que caracteriza a una exigente política de ciberseguridad global y los campos de acción regionales son incluso tan esenciales como los estados individuales.

La Unión Europea tiene en este contexto una extraordinaria importancia, no solo porque agrupe a 28 países industrializados, que en la economía digital mundial juegan un papel relevante[3], sino que en ellos las tecnologías digitales son mucho más que en otro lugar, el paradigma sobre la economía y la sociedad en su conjunto. Y también proporcionalmente están más amenazados que otros países. Como los crecientes ciberataques dirigidos por bandas internacionales conectadas entre sí y que operan con un elevado nivel técnico, la ciberdelincuencia nos lleva a una realidad descarnada en países abiertos e interconectados como los de la Unión Europea, que se encuentran especialmente afectados. En Alemania, según un estudio de McAfee, su producto social bruto resulta más dañado por estos ataques

2 En la lista de las grandes amenazas del mundo del informe Global Risk 2014 del World Economic Eorum aparecen los ciberataques en el puesto número cinco de los riesgos mundiales

3 La Unión Europea sigue siendo la mayor economía del mundo

que en otros países. El daño anual alcanza el 1,65 % del Producto Interior Bruto. Que son muchos miles de millones de euros[4]. Y solo se mencionan aquí los daños económicos originados y no los peligros de potenciales conflictos de política de seguridad nacional y las consecuencias a largo plazo que se derivan del ciberespionaje.

La Unión Europea es a la vez una unión de estados soberanos y una organización con instituciones y un marco normativo común[5]. La mayoría de los actos normativos que se realizan en común con el Consejo a propuesta del Parlamento y de la Comisión son vinculantes y obligatorios. Los Reglamentos y las Decisiones son en todas sus partes vinculantes para los estados miembros y las Directivas lo son en cuanto al resultado a alcanzar. Esto es un hecho único en el panorama internacional. La base institucional de la normativa europea supone no solo la aplicación inmediata en Europa sino que ejerce una notable influencia fuera del territorio europeo.

Europa sirve de ejemplo, como laboratorio institucional, en el que se prueba lo que mañana puede aplicarse en el ámbito internacional. La normativa europea es un instrumento de coordinación intra europea, pero también una puerta para la regulación internacional.

LA POLÍTICA DE CIBERSEGURIDAD

La política de ciberseguridad europea está unida tanto a un marco de regulación internacional como nacional y se interpreta y formula en un contexto de estructuras de varios niveles y estructuras multistakeholder. Esto se encuentra en la lógica de la política europea, en la que se entremezcla la política exterior e interior y apenas pueden separarse en la política de seguridad europea. El ámbito de competencias de la política exterior e

4 La media del coste de un ciberataque por empresa se ha calculado recientemente en unos 5 millones de euros

5 Las competencias de los órganos de la Unión Europea para ciberseguridad y la sociedad de información se derivan de la competencia sobre establecimiento y funciones del mercado interior. Según el artículo 16 del tratado sobre el funcionamiento de la Unión Europea tiene competencia para la regulación de los prescripciones sobre protección de datos, la garantía de los derechos fundamentales sobre la protección de datos personales art. 8 de la Carta de Derechos Fundamentales de la Unión Europea

interior se difumina. La complicada realidad institucional de los 28 países europeos fuerza a una cooperación intersectorial y a un cambio de los papeles tradicionales, también a la internacionalización de la política de justicia y de interior - todos ellos campos de experimentación ejemplares para otros intentos de regulación supranacional en la política de ciberseguridad[6].

Muy pronto la Union Europea ya empezó a desplegar una gran actividad respecto a las exigencias de la sociedad de información y la política de ciberseguridad, dirigida por comisarios y comisarías muy activos, capaces y competentes en la materia. Desde hace años la ciberseguridad figura en las prioridades de la agenda política de la Unión Europea. El verdadero comienzo de esta política se puede fijar en la Comunicación conjunta del Consejo y de la Comisión de 2000 (COM/2000/890 final).

Después de esta Comunicación del Consejo de la Comunidad Europea del año 2000 y a pesar de algunas reticencias institucionales - la competencia común respecto al llamado tercer pilar era entonces objeto de discusión, pero el Parlamento ejerció presión- en 2002 se trabaja en la Directiva marco para la lucha contra los ciberataques y la armonización del derecho penal de los estados miembros y cooperación en la persecución penal, COM(2002)173 final, que entró en vigor en octubre de 2003. Era vinculante y los estados miembros debían transponerla al derecho interno en el plazo de un año. Después de la ampliación de la Unión Europea vale también para los nuevos estados.

La directiva marco contiene una sistematización de los ciberataques y un catálogo de prohibiciones, que son parecidos a los reflejados en el Convenio de Budapest[7] sobre la Ciberdelincuencia, firmado casi al mismo tiempo, en cuya preparación la mayoría de los estado de la Unión participaron activamente, y que fue ratificado por España en el 2010.

---

6 En el ámbito internacional la Unión Europea respecto a la ciberseguridad es muy activa tanto a nivel bilateral como a nivel multilateral, por ejemplo los grupos de trabajo Estados Unidos –Unión Europea sobre ciberseguridad y ciberdelincuencia y las aportaciones en todas las organizaciones internacionales competentes

7 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_spanish.PDF

El Convenio de Budapest es, sin duda, universal y también transatlánticamente el documento más importante respeto a la ciberdelincuencia, y hasta ahora el único cibertratado que tiene por objetivo la armonización universal de la normativa del derecho penal nacional y la persecución penal de los delitos relacionados con Internet. Según interpretación de la Unión Europea, la directiva marco y el Convenio de Budapest son totalmente compatibles y, en consecuencia, 23 países de la Unión Europea ya han ratificado dicho Convenio. Debido a la identidad de objetivos de ambos instrumentos, la directiva marco ha traído consigo sin duda un cierto retardo en la ratificación del Convenio, a pesar de que los diferentes documentos y seminarios de la Unión Europea y la (todavía por analizar) Estrategia de la Ciberseguridad de la Unión Europea de 2013, han solicitado la rápida ratificación del Convenio por los cinco estados rezagados, a saber, Grecia, Irlanda, Luxemburgo, Polonia y Suecia, con el intento de fortalecer su efecto e impulso en la política universal.

En el empeño de construir la protección contra los ciberataques, se han estado publicando en los años siguientes documentos conjuntos de la Unión Europea. Se puede citar la COM (2001)209 "Seguridad de las redes y de la información. Propuesta para una política europea "; en el año 2006 COM (2006) 251"Estrategia para una sociedad de información segura"; de 2009 una Decisión del Consejo 2009/C 321.01 "De un enfoque europeo común sobre la seguridad de la información y de las redes"; de 2010 COM (2010) 245 "Una agenda digital para Europa". Durante años la Unión Europea ha fijado como punto fuerte la protección de infraestructuras críticas y ha desarrollado el "Programa Europeo de protección de infraestructuras críticas (EPCIP)", COM(2006) 786, la Directiva (2008) 114/UE y la Comunicación y el Plan de Acción COM(2009) 149, y de 2011 la Comunicación "Resultados y siguientes pasos. El camino para la seguridad global de la red" COM(2011) 163. Una conferencia de ministros de la Unión Europea sobre este tema tuvo lugar en 2009 en Tallín[8]. Como regulación actual con severas condiciones para todos los participantes en el tráfico

8 https://www.mkm.ee/en/news/eu-ministerial-conference-estonia-initialized-tallinn-process-secure-critical-information

digital está en el Reglamento 611/2013 de junio de 2013[9] con una obligación de notificación de los casos de violación de datos personales dirigido a las redes de comunicaciones electrónicas públicas. En este punto, analizar cada uno de estos documentos mencionados no parece muy útil porque sus contenidos, en relación con una evolución gradual futura, ya están recogidos en otras decisiones y documentos recientes todavía por mencionar –la Estrategia de Ciberseguridad de la Unión Europea y la Directiva NIS–.

De gran significado operativo fue la creación en 2004 de la Agencia Europea para la Seguridad de las Redes y de la Información (ENISA) por el Reglamento 460/2004, cuyas competencias e importancia experimentaron en 2010 un notable incremento bajo la COM (2010) 521[10] –con efectos en 2013 (el Reglamento 580/2011 amplió su vigencia inicial hasta septiembre de 2013)–**.** Los campos de actividad de ENISA en la protección y seguimiento de la política de ciberseguridad de la UE, también en colaboración con las autoridades de seguridad de los estados miembros es notable. En la página web de ENISA se reflejan estas actividades[11]. La Unión Europea dispone con ENISA de un instrumento reconocido también internacionalmente, que solo en Estados Unidos se puede encontrar algo igual.

Al comienzo de 2013 se creó el Centro Europeo de Lucha contra la Ciberdelincuencia (EC3), que parte de la policía europea EUROPOL, como punto central para el tratamiento de los ciberataques, incluso un CERT de ámbito europeo, el CERT-EU que colabora con los CERT nacionales de los estados miembros, cuya creación les exigió la Unión Europea en su Agenda Digital.

ESTRATEGIA DE SEGURIDAD DE LA UNIÓN EUROPEA

Ahora llegamos a la "Estrategia de Ciberseguridad de la Unión Europea". La publicación de un documento estratégico que aborda de manera general el problema de la ciberseguridad

9 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:ES:PDF

10 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0521:FIN:EN:PDF

11 www.enisa.europa.eu

es hoy casi una señal de modernidad. En los últimos años unos 35 países, entre ellos varios miembros de la Unión Europea como Alemania y España, se han dotado de instrumentos como estos de análisis y coordinación. La Estrategia debe garantizar la seguridad de las tecnologías de información así como el cumplimiento de los derechos y valores fundamentales de la Unión Europea. La estrategia identifica en cada capítulo tareas para los órganos de la UE, ENISA, los estados miembros y la industria

Se han señalado cinco estrategias prioritarias:

- La resiliencia contra ciberataques
- La reducción drástica de la delincuencia en la red;
- El desarrollo de una política de ciberdefensa y de las capacidades correspondientes en el ámbito de la Política Común de Seguridad y Defensa (PCSD);
- El desarrollo de los recursos industriales y tecnológicos necesarios en materia de ciberseguridad;
- El establecimiento de una política internacional coherente del ciberespacio en la Unión Europea y la promoción de los valores europeos esenciales.

De los cinco puntos clave solo uno se refiere claramente al problema de la seguridad militar y la creación de capacidades militares y de servicios de información, a pesar de la preocupante y creciente amenaza que resulta de una imparable y desordenada carrera armamentística en el espacio digital y la proliferación de cibercomandos y ciberestrategias ofensivas. Las otras cuatro prioridades se encuentran en la línea de la ciberpolítica de la Unión Europea, pero con nuevos índices operativos y tareas, con una visiblemente más fuerte inclusión del sector privado, en cuyas manos se encuentran la mayoría de infraestructuras críticas.

De la participación del sector privado se trata también en la propuesta de la Directiva sobre Seguridad de la Información y Redes (NIS) COM (2013) 48[12], que el Parlamento adoptó en

12 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0048:FIN:ES:PDF

febrero de 2014, con algunos cambios a la propuesta de la Comisión, pero que todavía necesita el consentimiento del Consejo; se cuenta con terminar a finales de 2014, seguramente todavía con algunas modificaciones más. Mucho en la propuesta de la Directiva, como la extensión de la obligación de notificación, está todavía por discutir, pero la estructura básica esta aceptada. La Directiva unifica numerosas políticas de seguridad, por ejemplo lo referente al papel de los CERTs, recuerda a los operadores de infraestructuras críticas la obligación de contribuir a la protección de infraestructuras digitales y obliga a las empresas a preocuparse de que sus productos y servicios cumplan con los actuales estándares de seguridad. Sobre todo establece un sistema de notificación para bancos, empresas energéticas, empresas de Internet, redes sociales, empresas de infraestructura de transportes y otros sectores, con la obligación de informar a un centro de alerta nacional de los ciberataques significativos. Estos centros compartirán información con los centros de países miembros de la Unión Europea y cuando proceda también informarán a los afectados particulares o públicos. Esta regulación va más allá que el Reglamento 611/2013 sobre medidas aplicables en la notificación de violación de datos personales, porque ahora lo convierte en obligación de comunicar, lo que hasta ahora era voluntario. En la preparación se consultó también con los Estados Unidos en lo referente a la americana Disclosure Guidance. Una vulneración de la obligación de informar puede conllevar notables sanciones. La Directiva permitirá sin duda un mejor análisis de los peligros colectivos e incitará a las empresas a actuar para fortalecer su ciberprotección y la protección de su seguridad.

Entre otras medidas actuales de la Unión Europea hay que citar Connecting Europe, comenzada en 2013 con 15 millones de euros de presupuesto para la lucha contra los botnets y los programas dañinos, que une la capacidad de los NIS de los estado miembros, la European Public-Private Partnership for Resilience (EP3R) y Trust in Digital Life (TDL) y numerosos informes, seminarios, análisis y ejercicios sobre ciberseguridad (incluso el ejercicio conjunto Unión Europea/ Estados Unidos "Cyber Atlantic 2011") de ENISA. Digno de mención es también la European Cloud Computing Strategy (COM(2012) 529[13] que no solo regula la seguridad y la fiabilidad de los centros de datos europeos -con consecuencias

13 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF

prácticas para el usuario europeo, sino también asegura la total garantía de las condiciones europeas de la protección de datos en estos centros y los correspondientes derechos fundamentales.

Resumiendo, se puede decir que la política de ciberseguridad de la Unión Europea y las medidas y actos normativos correspondientes a las prioridades políticas funcionan. En la armonización y unificación de las normas, competencia y procedimientos administrativos y en la coordinación europea de los gobiernos y la comunidad Multistakholder se han logrado grandes mejoras. Las innumerables estructuras internas en los estados miembros se integran y mejoran notablemente y lo que es más importante, se reduce la vulnerabilidad del conjunto de la Unión Europea.

LA PERSPECTIVA TRANSATLÁNTICA

El punto fuerte de la política de la Unión Europea se encuentra en la construcción de la resilencia y en la lucha contra la ciberdelincuencia –la palabra clave es ciberdefensa– , la prevención y la minoración de daños a través de la colaboración y de una gestión pública y privada eficaz. Los puntos fuertes de la Estrategia de Ciberseguridad de la UE lo muestran muy claro. Una comparación con la política de los Estados Unidos no se puede proponer aquí en detalle, pero de una mirada superficial es claro que el concepto de Estados Unidos parece totalmente diferente. En primer plano aparece la disuasión digital y la construcción de una capacidad de ataque, que se plasma en la dotación técnica del US Cyber Command y sus medios financieros pero también en las numerosas ciberoperaciones de las autoridades competentes. La agenda de seguridad nacional es prioritaria; la política de ciberseguridad de Estados Unidos está marcada esencialmente por la idea de que la seguridad nacional está amenazada por los ciberataques y que esta amenaza se trata con mentalidad y medios militares. La disuasión y la amenaza con reacciones masivas son hoy, al menos en una interpretación corriente, el elemento central de la política de ciberseguridad de los Estados Unidos[14]. Nos reencontraremos con esta tendencia al sobrepeso de consideraciones de

14 Para la interpretación de estos documentos y de esta doctrina se pide precaución. Están formulados

política de seguridad nacional cuando tratemos el problema de la protección de datos y del límite de la intervención estatal respecto a datos personales y empresariales. Por otro lado vemos en la política de los Estados Unidos también una dosis de ambivalencia cuando se trata de su *International Strategy for Cyberspace de 2011*[15], donde se pronuncia con insistencia por la colaboración, incluso la colaboración internacional y las soluciones amistosas[16]. Esto corresponde con la actitud bastante conciliadora y dispuesta a compromisos que los Estados Unidos ha tenido en los últimos tiempos en los foros internacionales (en la Asamblea General de Naciones Unidas, en las discusiones sobre medidas de formación de confianza, en el asunto de la gobernanza de Internet, ...). Por otra parte, la política de ciberseguridad de la Unión Europea, sometida a una cierta creciente preponderancia de seguridad nacional, ha recibido valoraciones críticas en ciertos entornos, es decir, que bajo la sensación de nuevas ciberamenazas se interpreta a favor de las medidas de ciberseguridad y en perjuicio de los derechos de libertad individual y de los requerimientos del estado de derecho.

TRATAMIENTO JURÍDICO DE LOS CIBERINCIDENTES

El acceso no consentido, la injerencia a los soportes digitales –teléfonos, ordenadores, y otros aparatos– y la copia, la grabación, modificación y la transmisión (el concepto genérico es "tratamiento") de los datos ahí almacenados es un ciberdelito. Aquí se tocan la ciberdelincuencia y la protección de datos. Debemos analizar en el marco de nuestro tema la política europea de protección de datos en relación con los datos almacenados digitalmente,

---

en el sentido que cada ciberoperación debe armonizarse con el derecho internacional bélico en su moderna caracterización .

15 http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

16 En la Estrategia se dice: "It is a call to the private sector, civil society, and end-users to reinforce (these) efforts through partnership, awareness, and action. Most importantly, it is an invitation to other states and peoples to join us in realizing this vision of prosperity, security, and openness in our networked world. These ideals are central to preserving the cyberspace we know, and to creating, together, the future we seek"

sobre todo considerando la actual discusión transatlántica La política de protección de datos de la Unión Europea protege los datos personales, es decir, la persona física. Los datos comerciales y empresariales no están incluidos en ella.

El espionaje industrial, es decir, obtener generalmente datos no personales, sino datos empresariales no está sancionado por el derecho internacional, pero sí por el derecho civil y penal. Es perseguible penalmente en los países de la Unión Europea según los artículo de 2 a 6 del Convenio de Budapest y su transposición al derecho nacional, sin embargo la imputación de un ataque de injerencia es complicado, como siempre ocurre en el espacio digital. Sin embargo, también son susceptibles de demanda civil por daños y perjuicios. Resulta perseguible penalmente, también cuando el ataque se realiza fuera del territorio nacional de aquel en el que se producen los daños. Esto está en consonancia con el principio esencial del proceso penal, que el lugar del hecho es el lugar donde tiene lugar el efecto dañino. El principio territorial se establece en el artículo 22 del Convenio de Budapest y se puede interpretar que el lugar de las consecuencias del daño es primordial, aunque el sujeto activo ataque desde fuera del territorio. Esto ha sido aclarado por la regla de interpretación nº 232 del Informe Aclaratorio del Convenio. Como los ciberdaños a menudo no están limitados geográficamente, nos pone en el umbral de un derecho penal universal para los delitos digitales

La fiscalía, al menos en aquellos países en los que la presunta comisión de un delito es perseguible de oficio, obliga a abrir un proceso penal aunque se trate de desconocidos, si se sospecha un probable ataque de espionaje de un tercer país, una práctica que, lamentablemente, no ha sido observada lo suficiente pero sería políticamente muy deseable**.** Naturalmente debe detenerse al delincuente, antes de juzgarlo, pero una denuncia tiene un efecto de publicidad, que puede ser de por sí ya intimidatorio. En Berlín la fiscalía interpuso una denuncia contra desconocidos, que posiblemente en Alemania, y desde un sitio cercano, habían estado pinchando el teléfono de la canciller Merkel durante bastante tiempo. Se puede suponer que la intrusión en los aparatos digitales de un político no es solo por los datos personales del afectado sino sobre todo por la adquisición de datos sobre hechos y análisis políticos, y asi sustancialmente de espionaje.

CUESTIONES ASOCIADAS A LA PROTECCIÓN DE DATOS

La protección de datos personales y la esfera privada de las personas ha resultado realmente relevante con la evolución de los aparatos digitales de almacenamiento de datos y ha generado una necesidad de regulación. En la Unión Europea todavía sirve la Directiva de Protección de Datos 95/46 CEE[17] con estándares mínimos que los estados miembros, algunos con dificultades, han traspuesto al derecho interno[18]. La directiva se aplica a personas físicas y también el tratamiento de datos personales por un proveedor no domiciliado en la Unión Europea. La condición más importante para la obtención de datos es el consentimiento del interesado, pero también la protección de interés de importancia vital, la existencia de un contrato y, dentro de cierto margen, de un interés público. El suministro de datos a personas o empresas en terceros países prevé una constatación de la Comisión Europea que garantice este nivel de protección. La consecución de este estándar lo adoptaron Estados Unidos y la Unión Europea en el marco del tratado de protección de datos Safe Harbor. Bajo este tratado, las empresas americanas registradas y certificadas, que garanticen el cumplimiento de una lista de principios, consiguen el acceso a datos personales y empresariales europeos. Safe Harbor debe garantizar que los empresarios de ambos lados del Atlántico apliquen el mismo estándar legal. Este tratado refleja el convencimiento europeo, que en un mundo globalizado un alto nivel de protección para datos privados, en el sentido de seguridad de datos y de protección de datos, es una ventaja para la competitividad.

---

[17] http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_es.pdf ; http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part2_es.pdf

18 Esto fue completado por la Directiva de Protección de Datos para la comunicación electrónica,2002/58 CEE. En otros foros internacionales como la OCDE encontramos las Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (www.oecd.org/sti/economy/2013-oecd-privacy-guidelines.pdf), que tiene por objetivo la armonización universal de las normas más importantes y el Convenio Europeo de protección de datos del Consejo de Europa (http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm) que es vinculante como derecho internacional para 46 países. En los estados miembros de la Unión Europea existen también normas nacionales, así en Alemania, la ley federal de protección de datos de 1997 que traspuso también la Directiva 95/46 CEE

El Acuerdo Safe Harbor (como el acuerdo SWIFT sobre datos bancarios) está en dificultades. Según informaciones, dado que grandes empresas americanas no cumplen las obligaciones establecidas (por ejemplo la codificación de datos), de manera que los servicios secretos pueden acceder a los datos bancarios, y bajo el efecto que ha provocado el conocimiento de las escuchas/ingerencias masivas de los servicios secretos americanos en Europa, ha llevado al Parlamento europeo, con una gran mayoría, a exigir la suspensión del acuerdo Safe-Harbor. Este acuerdo ya no satisface las exigencias de la Unión Europea sobre la protección de datos. La Comisión y los estados miembros y, en particular, la industria exigen mejoras, aún más, una nueva negociación, de lo contrario el acuerdo se suspendería con graves consecuencias. No obstante, la parte americana se muestra reticente.

El cambio político y técnico de la situación desde la publicación en 1995 de la Directiva de protección de datos ha motivado a la Comisión a realizar una nueva versión. La Comisión ha enviado a los miembros del Consejo y al Parlamento un borrador de Reglamento Fundamental de protección de datos COM 2012 /11 final[19] con el efecto de ser directamente aplicable, y no como una Directiva. Este borrador debe tener en cuenta las exigencias de la protección de datos en una nueva sociedad digital, que se caracteriza por las nuevas redes sociales, una conectividad universal y una cada vez mayor penetración de la sociedad en los soportes digitales y exige la elaboración de un cuerpo jurídico europeo que sea homogéneo. El Reglamento Fundamental toma las normas de anteriores directivas, las precisa y las hace más exigentes. Se reconoce el derecho al borrado de datos (el derecho al olvido). Las normas del procedimiento son más detalladas. En el caso de una vulneración del derecho de la protección de datos se prevén multas de hasta millones de euros. El borrador es una codificación monumental con una extensión de al menos 150 páginas. El Consejo de Ministros de la Unión Europea hasta ahora no ha podido ponerse de acuerdo sobre el contenido exacto de la reforma. La negociación en el Consejo se puede extender hasta finales de 2014.

Las actividades de los servicios secretos norteamericanos, sobre todo de la Agencia de Seguridad Nacional (NSA)l, en Europa supone según la Directiva de 1995, y también del

[19] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF

Reglamento Fundamental cuando entre de una vez en vigor, una masiva violación del derecho de la Unión Europea y de los estados miembros, tanto que ni en casos específicos se dieron los requisitos jurídicos procesales de colaboración de las autoridades de seguridad europeas para una masiva recogida de datos por razones de seguridad. De esto no hay duda. Y tampoco hay duda que las actividades de los norteamericanos con su locura de captación de datos excede de lo racional y las exigencias de seguridad de una intervención.

En contra de la provocación y la irritación que han causado estas actividades de escucha de los servicios de información norteamericana y su masiva extensión a las comunicaciones en Europa, me gustaría ofrecer una valoración desdramatizada de los hechos[20].

En primer lugar hay que reconocer que los avances tecnológicos permiten introducirse en las redes digitales y en los soportes informáticos y la recogida de datos y su tratamiento a través de potentes máquinas de búsqueda en una dimensión que hace tan solo unos años era totalmente inimaginable. Utilizar esta oportunidad tecnológica para la política de seguridad nacional de un país - sobre todo los Estados Unidos- por principio no se puede condenar. Las nuevas técnicas –la palabra clave es Big Data– cambiarán también Europa. Las nuevas técnicas se utilizan y se utilizarán, si son útiles.

Se puede ver, no solo en los Estados Unidos sino también en los servicios de información de los países europeos -, a menudo en estrecha colaboración -, que se utilizan y se han utilizado estas técnicas y nos hemos beneficiado de los conocimientos americanos en la lucha contra el terrorismo, el crimen organizado, el tráfico de drogas y el lavado de dinero. Esto es válido especialmente para Gran Bretaña que no solo utiliza las prácticas y conocimientos americanos del programa PRISM, sin las normales garantías y sin la necesidad de una sospecha previa, sino también en gran medida de su propia recolección de datos, sobre todo la recopilación de datos en las redes sociales y en su programa TEMPORA, que intercepta todos los cables de fibra óptica que pasan por el Reino Unido.

---

20 Véase también Nigel Inkster *The Snowden Revelations: Myths and Misapprehensions* SURVIVAL,February-March 2014, pag.51; Joachim Krause *Diskutieren statt moralisieren,* Internationale Politik, Januar-Februar 2014, pág .108

También la Comisión de la Unión Europea se preocupa de que Gran Bretaña no cumpla la prescripciones legales de la Unión Europea, por ejemplo, los controles judiciales necesarios. Pero también otros servicios de información extranjeros en la Unión Europea no se quedan atrás al menos en sus actividades de investigación en el extranjero.

Se minusvalora en la discusión europea también la importancia de la política de seguridad de las actividades de escucha, donde se puede discutir la relación entre la infiltración en las redes de datos totalmente y su consecuencia penal. Pero nadie aconseja prescindir totalmente de la captación de datos. Y muchos de los datos y conocimientos conseguidos por Estados Unidos y también de los datos compartidos por los aliados europeos en el exterior e interior sobre peligros inminentes son y ha sido provechosos para Europa

Hay que ser prudente con el argumento de que las autorizaciones y los controles en Estados Unidos, incluyendo el tribunal secreto FISA con sus audiencias cerradas al público, sean tan permisivos que permitan todo al ejecutivo. Es un hecho que los Estados Unidos en las últimas décadas han construido una arquitectura de seguridad militar e industrial y el gobierno ha dejado manos más libres a los servicios de seguridad. Pero también si las prioridades de la política de seguridad en Estados Unidos son notablemente más altas que en Europa, y se pueden obtener autorizaciones en general más fácilmente, y también si las empresas de IT, servidores telefónicos y otra empresas en Estados Unidos son mucho más dóciles que las europeas de cara a la presión de cumplir las obligaciones de cesión y grabación de datos, los Estados Unidos tienen dispositivos de control y normas muy responsables y eficaces.

Finalmente, no todos los datos se utilizan o se publican, Según las cifras de la NSA de 2013 la cantidad de datos que circulan al día por internet son de 1,828 Petabytes. De los cuales la NSA solo puede captar 1,2 % y de ellos solo una fracción se da a conocer, esto sería solo el 0,0004 % del total de la circulación de datos, y solo en ellos se coloca el filtro de búsqueda de las autoridades. Debemos tener sentido de las dimensiones.

Al fin y al cabo la manera de comportarse americana es también objeto hoy de una fuerte crítica en la política interna. Los Estados Unidos no son un bloque monolítico, sino una democracia viva con valores aprendidos e incorporados. No hay que excluir que en el ajuste

de la visión americana y europea encontraremos una situación en la que podamos congeniar. En enero de 2014 el presidente de Estados Unidos anuncio unas medidas de reducción de daños (recolección de datos solo para fines de política de seguridad, los datos de telecomunicación de los americanos deberán ser grabados en el futuro solo por el proveedor, acceso para la NSA solo por orden judicial, etc...)

A pesar de mi redimensión del enfado con la NSA, hay que concluir que:

- La sensibilidad por el balance entre seguridad y libertad y por la protección de datos se define de manera muy diferente a ambos lados del atlántico. Los Estados Unidos no poseen una normativa de protección de datos comparable a la europea. Sus experiencias con el terrorismo desde 2001 han marcado la conciencia y la política. La escala de valores y las prioridades se separan y esta brecha transatlántica básicamente no se puede salvar, sino, en el mejor de los casos, reducirla. Sin embargo, Europa no se puede apartar de su alto standard de protección, sino que debe exigir mayor respeto a su ordenamiento jurídico.

- Las practicas americanas son ilícitas según el derecho internacional (Convenio de Budapest), europeo y nacional y pueden ser perseguidas penalmente en algunos de los países afectados, porque la consecuencia de interceptación digital se produce en ello. Este recurso jurídico esta sin embargo bajo la salvedad de la oportunidad política y se encuentra con la objeción de la soberanía, si una autoridad extranjera está directamente implicada (y no un servidor privado de IT), como pudo ser en la mayoría de los casos

- Las justificaciones de política de seguridad del proceder que ofrecen los americanos, son desde el punto de vista europeo jurídicamente irrelevantes, se deben observar los procedimientos de legítima vigilancia de la política de seguridad en cada uno de los países espiados

- La pérdida de confianza en la relación transatlántica es especialmente grave, pero desde el lado americano no se han dado cuenta suficientemente de su dimensión. Se

añade la pérdida de la confianza de los ciudadanos en la integridad de las redes digitales y su capacidad y en garantizar su privacidad

CONCLUSIONES

Si tuviera que terminar con algunas recomendaciones, quisiera limitarlas a unas pocas pero esenciales. En la política de ciberseguridad de la Unión Europea se ha hecho lo esencial. La Estrategia de Ciberseguridad de 2013 contiene una serie de propuestas y tareas que se deben emprender ya. Es importante que la Directiva para la Seguridad de la Información y las Redes (NIS) se publique ya definitivamente.

En el campo de la protección de datos es también necesario que el legislador europeo publique cuanto antes sea posible su Reglamento fundamental sobre protección de datos. Esta base jurídica común es también necesaria para las futuras e indispensables negociaciones con los Estados Unidos.

En esto se tiene que tratar de reconstruir la confianza perdida, posibilitar y encontrar un alto entendimiento sobre un equilibrio sostenible entre libertad y seguridad, más transparencia respecto a las explicaciones políticas de los socios transatlánticos y hacerlo sobre una base jurídica, haciendo compatible la actividad de los servicios extranjeros con los procedimientos europeos sobre las medidas exigibles en la vigilancia. Se debe hacer una nueva negociación del pacto Safe Harbor. Algunas prácticas desagradables como las escuchas ilegales a políticos de países amigos entre sí deben cesar de común acuerdo: una promesa de palabra de los jefes de estado y de gobierno de que en el futuro limpiarán de escuchas de sus comunicaciones , no es suficiente. Se necesita un pacto de no espionaje entre la Unión Europea y los Estados Unidos, de renuncia al espionaje o al menos un memorándum de entendimiento en este sentido, que pueda favorecer una colaboración más estrecha entre los servicios secretos de ambas partes.

A medio plazo Europa tiene que ocuparse de un marco internacional de reglas, que asegure de manera vinculante y consensuada el equilibrio entre los legítimos interés de seguridad de los participantes y la garantía de la libertad y la protección de datos

Los países europeos, también ellos mismos, tienen que hacer muchas tareas, también dentro de su propia casa. Entre estas figuran una construcción de la resiliencia técnica del sistema y de las redes, una mejorada autoprotección de la comunidad multistakeholder y una conciencia de seguridad más fuerte de todos los participantes, también una economía de datos más alta, mejores prácticas de back-ups de datos, etc…

Los estados de la Unión Europea deben garantizar que sus propios servicios de información respeten escrupulosamente la normativa europea y nacional y por tanto que su comportamiento sea transparente, y no exigir a los americanos más de lo que los mismos europeos hacen. Y entre estas cosas está la prohibición de espiarse mutuamente.

[i]

*Henning Wegener**
Embajador
Federación Mundial de Científicos