Revista Penal México 18
Doctrina
Núm. 18, enero - junio de 2021

Riesgos que genera el ciberespacio para los derechos fundamentales

Isabel Morón Pendás *Magistrado.*

***Resumen**: El imparable desarrollo de las tecnologías y las extraordinarias oportunidades que proporciona el ciberespacio tienen por contrapartida el peligro de lesión de derechos fundamentales y la aparición de nuevas formas de criminalidad.*

Palabras clave: Ciberespacio, derechos fundamentales, ley penal, protección de datos, ciberseguridad.

***Abstract**: The unstoppable development of technologies and the extraordinary opportunities provided by cyberspace are in return for the danger of fundamental rights injury and the emergence of new forms of criminality.*

***Key words**: Cyberspace, fundamental rights, criminal law, data protection, cybersecurity.*

Rec: 15 jun 2020 | **Fav:** 01 ago 2020

1. Aproximación

Decía el Profesor Ferré en 2013 que "las posibilidades tecnológicas son casi ilimitadas, o, al menos hoy, desconocemos sus límites. La creación de un espacio nuevo y virtual, inimaginable hace pocas décadas, en el que transita cualquier tipo de información, desde nuestros datos personales más sensibles hasta todo género de operaciones comerciales, supone una auténtica revolución tecnológica"[1]. Hoy es necesario añadir que el modelo mismo de sociedad y hasta las propias estructuras de los Estados se ven profundamente afectados por esta imparable revolución silenciosa .

En el Reino de España, la reciente Estrategia Nacional de Ciberseguridad 2019 (en adelante ENC 2019), aprobada por el Consejo de Seguridad Nacional, califica al ciberespacio como "espacio común global caracterizado por su apertura funcional y su dinamismo", que se presenta como escenario con innumerables oportunidades de futuro, pero que al mismo tiempo presenta serios desafíos a la seguridad[2].

Entre las oportunidades que proporciona este, no ya tan nuevo espacio, pero en imparable crecimiento y evolución, destaca la ENC 2019 la posibilidad de la conectividad universal, el libre flujo de información, servicios e ideas, y el consiguiente estímulo del emprendimiento y del progreso socioeconómico, poniendo de manifiesto que el verdadero potencial transformador de la revolución digital está por descubrir y sus implicaciones, que trascienden a lo meramente tecnológico, se adentran en la conformación misma de los modelos sociales, las relaciones sociales y la ética.

De la otra cara, la ENC 2019 califica al ciberespacio como "campo de batalla" en que la información y la privacidad de los datos son activos de alto valor que se presentan especialmente vulnerables y difíciles de proteger precisamente por la creciente conectividad y la dependencia de las redes y sistemas .

Ahora como nunca se hace realidad aquello de que la información es poder, o, en términos más actuales, que el poder es información, y la protección de la información es la protección del poder. Las posibilidades, pero también las vulnerabilidades del ciberespacio condicionan las agendas de los gobiernos que, reconociendo su condición de sector estratégico, elevan la ciberseguridad a categoría de objetivo prioritario, y aspiran a la creación de una sociedad digital basada en la confianza.

Partiendo de las apuntadas oportunidades que ofrece el ciberespacio, pueden analizarse algunos de los retos de futuro que se ponen en juego.

Muy gráficamente, Neal Kaytal escribía hace ya más de 15 años, que el ciberespacio era un lugar oscuro que fomentaba el anonimato y que pronto encararíamos la posibilidad de que "la red sea tan insegura como las calles del centro de la ciudad". Resulta interesante la analogía con las calles del centro. En muchas ciudades, la gente elude transitar de noche por las calles, ante el miedo a ser atacados. En otras, las luces o el propio diseño de las vías pone límites a la delincuencia[3]. El autor, partiendo de las ideas sembradas por Jane Jacobs[4] analiza la trascendencia de la arquitectura y de la planificación urbanística en la prevención del delito, y, trasladando esos conceptos al ámbito del ciberespacio, considera que del mismo modo que en la vida real, en la virtual, la protección puede venir dada por medidas adoptadas desde el poder público o bien desde el propio usuario[5]. De un estudio basado en entrevistas a delincuentes concluía Sally Merry que tratan de buscar, para delinquir, aquellos lugares en que no serán observados. Sus escenarios favoritos son los caminos cerrados donde la visibilidad es escasa y los testigos inexistentes. Las zonas abiertas son consideradas pobres para sus fines "porque hay demasiados ojos allí". Las localizaciones ideales son las que proporcionan muchas vías de escape, con muchos recovecos y esquinas[6].

[1] Cfr. Ferré Olivé, J.C. "*Tecnologías de información y comunicación, comercio electrónico, precios de transferencia y fraude fiscal*", en AA.VV: "Nuevas Amenazas a la seguridad nacional: Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación". Tirant Lo Blanch , 2013. p.193

[2] Cfr. Orden PCI/487/2019 de 26 de abril , por la que se publica la Estrategia Nacional de Ciberseguridad 2019 (en adelante ECN 2019) , aprobada por el Consejo de Seguridad Nacional, (BOE núm. 103, de 30 de abril de 2019) Capítulo 1 .

[3] Cfr. Katyal, N.K "Digital Architecture as Crime Control". The Yale Law Journal. Vol. 112, No. 8 (2003), p. 2263.

[4] Vid. Jacobs, J. "*The death an life or great american cities*". Ed. Random House, New York, 1961, *passim*. Esta autora investiga el porque de los distintos índices de criminalidad entre las diversas ciudades y barrios concluyendo que el objetivo es, a través del urbanismo, llenar las calles de luz y sobre todo, de observadores, que se convierten así en vigilantes de la ciudad lo cual incide directamente en la reducción de la delincuencia callejera. Ocurre lo mismo con la estructura de los edificios y otros elementos del urbanismo.

[5] Cfr, Katyal, N.K "Digital Architecture as Crime Control". The Yale Law Journal. Vol. 111, No. 5 (2002)

[6] Cfr. Merry, S. E. *Defensible Space Undefended: Social Factors in Crime Control Through Environmental Design*, Urban Affairs Quarterly, Volume: 16 (1981). p. 409.

Los partidarios del Crime Pevention Through Enviroment [7](CPTE) coinciden en lo esencial de la luz, esto es, de la iluminación de los espacios en orden a la prevención de la delincuencia. Nada es más aplicable al oscuro ciberespacio, tan plagado de zonas de sombra, callejones oscuros y esquinas a salvo de testigos, favorecedor del anonimato y caldo de cultivo idóneo para el delito. Como sostiene José R. Agustina, ha ido calando la idea de la necesidad de arbitrar cambios estructurales en el sistema, para introducir luz en las arquitecturas digitales que generan una atmósfera de anonimato que protege, promueve y alimenta nuevos modos de atentar contra las personas e instituciones, que podría tener el mismo efecto que "la introducción de la luz de gas y la electricidad"[8], en las oscuras calles en que antiguamente proliferaba el delito.

La conectividad universal y la apertura del espacio apuntan directamente a un nuevo escenario de regulación e intervención que supera las fronteras nacionales, con los complejos problemas que ello supone. Los instrumentos normativos parten de la consideración de lo esencial de la cooperación internacional y la coordinación no solo entre Estados, sino, asimismo, con el sector privado en la lucha contra la ciberdelincuencia.

La proliferación y generalización en el uso de las Tecnologías de la Información y Comunicación es ya una realidad que, "inexorablemente, sigue avanzando, inmiscuyéndose en nuestra vida cotidiana, permeándolo todo"[9]. La clave de este avance "seguramente se encuentra en la capacidad de almacenamiento y manejo velocísimo de la información, lo que ha sido posible a través de los avances de las TICS, que aportan medios cada vez más evolucionados y sofisticados para conservar, procesar y difundir todo tipo de contenidos"[10]. La potencialidad de este ingente trasiego de datos y el renovado valor de la información que circula por las redes exige la debida protección tanto de la información misma como de los derechos fundamentales de los titulares de los datos.

La versatilidad del ciberespacio, sus infinitas posibilidades para el progreso en todos los ámbitos tiene como contrapartida los riesgos de su utilización con fines ilícitos, surgiendo una nueva categoría que se ha venido a llamar ciberdelincuencia, cibercriminalidad o tecnocriminalidad. Y, de igual modo, la configuración de este nuevo espacio virtual se apoya en unas infraestructuras físicas, públicas y privadas, que lo sustentan y que se encuentran expuestas igualmente a permanentes amenazas que plantean asimismo nuevos retos de seguridad.

En esta línea la ENC 2019 señala en su resumen ejecutivo " las actividades que se desarrollan en el ciberespacio son fundamentales para la sociedad actual. La tecnología e infraestructuras que forman el ciberespacio son elementos estratégicos, trasversales a todos los ámbitos de actividad, siendo la vulnerabilidad del ciberespacio una de los principales riesgos para nuestro desarrollo como nación"[11].

2. Ciberespacio, protección de datos personales y derechos fundamentales.

La información se ha convertido en elemento estratégico clave para el mundo de la empresa, incluso para las de pequeñas y medianas dimensiones. Pero también para la gestión, el gobierno, la defensa y la administración, por lo que es un activo esencial en lo público y en lo privado. No solo las empresas, también las administraciones públicas demandan más información, más datos, que, procesados, permiten generar el conocimiento necesario para mejorar su actividad, sus procesos productivos, el logro de sus objetivos. Para orientar la conducta del consumidor, del votante, del usuario del servicio público o privado es especialmente útil conocer sus hábitos, sus inclinaciones políticas, morales, sus preferencias y costumbres entre otras.

En un mundo movido por la información la obtención de datos se ha convertido en esencial y las

[7] La prevención de la delincuencia por medio del urbanismo refiere a un conjunto de estrategias iniciadas a partir de los trabajos de Elisabeth Madera , Schlomo Angel y Jane Jacobs desde el principio de los años sesenta en Estados Unidos , luego desarrolladas principalmente por el criminólogo Ray Jeffery y el arquitecto Oscar Newman, que se encaminan a emplear el diseño de las calles y edificios como modo evitar la delincuencia, en el entendido de que los delincuentes huyen de espacios vigilados y concurridos, siendo la" vigilancia natural", la derivada de la presencia de ciudadanos en las calles el mejor método de disuasión

[8] Cfr. Agustina, J. R. "Cibercriminalidad y perspectiva victimológica: un enfoque general explicativo de la cibervictimización", Cuadernos de Política Criminal, nº 114, 2014. p.147 .

[9] Cfr. Agustina, J. R. "Cibercriminalidad y perspectiva victimológica…" op. cit., p.145.

[10] Ferré Olivé, J.C. "*Tecnologías de información y comunicación, comercio electrónico, precios de transferencia y fraude fiscal*", en AA.VV: "Nuevas Amenazas a la seguridad nacional: Terrorismo , criminalidad organizada y tecnologías de la información y la comunicación". Tirant Lo Blanch, Valencia, 2013. p. 193.

[11] Op cit. Orden PCI/487/2019 de 26 de abril.

nuevas, y las ya no tan nuevas, tecnologías, permiten su tratamiento casi de forma instantánea, para el logro de cualesquiera finalidades, no siempre lícitas. La información es hoy un valor estratégico para toda organización, los datos personales son *el recurso fundamental de la sociedad de la información12*. El análisis de datos, posibilita conocer el pasado, indagar el presente y con ello obtener los instrumentos para adoptar las decisiones adecuadas para encarar el futuro. Y las nuevas tecnologías permiten recabar datos y procesarlos a velocidades inimaginables. La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de dichos datos[13].

El problema, como todo en derecho, consiste en determinar cuales son los límites a que deben quedar sujetos la que se ha dado en llamar *minería de datos*, su análisis y el tratamiento de esos datos de carácter personal para su empleo por terceros, sean sujetos públicos o privados, máxime cuando se trata de datos especialmente sensibles, susceptibles de afectar a los derechos fundamentales. Tradicionalmente la regulación de la protección de datos, en relación a su obtención, registro y tratamiento, entendida como un método de salvaguarda de los derechos de libertad e intimidad de las personas, venía adaptada a las actividades de tratamiento realizadas por las instancias públicas, si bien la nueva realidad exige atender a las llevadas a cabo por manos privadas[14].

La Constitución Española de 1978 fue de las primeras, siguiendo el modelo de la Portuguesa de 1976[15], en abordar la cuestión, llamando el artículo 18 CE a la Ley a fin de limitar el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos[16].

El Tribunal Constitucional español ha declarado que el contenido del derecho a la protección de datos consiste en "un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso". Estos poderes de disposición y control "se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular". A su vez, "ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién

[12] Cfr. Preámbulo de la Ley Orgánica 3/2018, de 5 de diciembre , de Protección de Datos Personales y Garantía de los derechos digitales, "*El carácter central de la información personal tiene aspectos positivos, porque permite nuevos y mejores servicios, productos o hallazgos científicos. Pero tiene también riesgos, pues las informaciones sobre los individuos se multiplican exponencialmente, son más accesibles, por más actores, y cada vez son más fáciles de procesar mientras que es más difícil el control de su destino y uso*".

[13] Cfr. Considerando 6 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

[14] Cfr. De Alfonso Laso, D. "Intimidad y protección de datos en el derecho penal" en AA.VV. "Delincuencia informática. Problemas de Responsabilidad". Cuadernos de Derecho Judicial IX. Madrid 2002, p. 39.

[15] El artículo 35 de la Constitución de la República de Portugal de 1978 regulaba la "*Utilización de la informática 1. Todos los ciudadanos tendrán derecho a tomar conocimiento de lo que conste en forma de registros mecanográficos acerca de ellos y de la finalidad a que se destinan las informaciones y podrán exigir la rectificación de los datos, así como su actualización. 2. No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos. 3. Se prohíbe atribuir un numero nacional único a los ciudadanos*".

[16] El artículo 18 de la Constitución española de 1978 establece "*1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. 2.El domicilio es inviolable (...) 3. Se garantiza el secreto de las comunicaciones, y en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*".

dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos (…) exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele"[17] y asimismo, que este derecho "no tiene carácter absoluto. Puede ser restringido por medio de la ley, siempre que ello responda a un fin de interés general, y los requisitos y el alcance de la restricción estén suficientemente precisados en la ley y respeten el principio de proporcionalidad"[18].

La libertad informática se concibe como derecho instrumental, pues contiene "un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos" que, además, es en sí mismo "un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama *la informática*"[19].

La libertad informática es el derecho a controlar el uso de los datos relativos a la propia persona, insertos en un programa informático (*habeas data*). Comparte con el derecho fundamental a la intimidad el objetivo de protección de la vida privada, pero difieren en su función, su objeto y contenido. La función del derecho fundamental a la intimidad es defensiva, faculta a defenderse *frente a invasiones en el ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de intromisiones de terceros, sean poderes públicos o simples particulares*[20]. La libertad informática, garantiza un poder de control sobre los datos personales, su uso y destino. Impone a los poderes públicos la prohibición de convertirse en fuentes de esa información personal y el deber de prevenir los riesgos derivados del acceso o divulgación indebidas de aquella. Y su contenido, más amplio, no se limita a datos relativos a la vida privada o íntima sino que alcanza a cuantos datos sean relevantes para -o tengan incidencia en- el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado, de forma que no se extiende solo a datos íntimos de la persona, sino incluso a los públicos, que no pueden, por el hecho de serlo, escapar a su control. La expresión "carácter personal" no limita la protección a los relativos a la vida privada o íntima de la persona, los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que, en determinadas circunstancias, constituya una amenaza para el individuo[21].

En el ámbito Europeo la protección de datos de carácter personal aparece consagrada en el Título II -"Libertades"- de la Carta de los Derechos Fundamentales de la Unión Europea, hecha en Estrasburgo el 12 de diciembre de 2007, en concreto el artículo 8 consagra el derecho a la protección de datos de carácter personal[22].

[17] Ver STC 292/2000, de 30 de noviembre (BOE núm. 4 , de 4 de enero 2001) F.J.5.

[18] Ver STC 76/2019 , de 22 de mayo (BOE núm. 151 , de 25 de junio de 2019) F.J.5.

[19] Ver STC 254/1993, de 20 de julio (BOE núm. 197, de 18 de agosto de 1993) F.J. 6. Idénticos razonamientos se reiteran posteriormente en otras como las SSTC 254/1993, F.J. 6, que otorga amparo a un particular frente a la denegación de información solicitada a la administración acerca de los ficheros automatizados en que figurasen datos de carácter personal que le concernían ; 143/1994, F.J. 7; 11/1998, F.J. 4, que declara contraria a la libertad sindical la utilización por la empresa del dato de afiliación de los trabajadores a un determinado sindicato, dato recabado a los solos efectos del descuento de la cuota sindical al confeccionar la nómina para su entrega la sindicato , con la finalidad no consentida de detraer sus haberes con ocasión de la huelga promovida por aquel Sindicato ; 94/1998 F.J. 6 en asunto similar al anterior ; 202/1999, F.J. 2, que otorga amparo frente al almacenamiento sin cobertura legal, en una base de datos " de absentismo con baja médica" de datos referidos a las enfermedades que determinaron las bajas laborales de los empleados de una entidad crediticia sin consentimiento expreso de los afectados, al no concurrir tampoco un interés general en la existencia del fichero como podría ser la preservación de la salud de los trabajadores, sino el mero control del absentismo laboral ; 292/2000 F.J. 5, que anula parcialmente varios preceptos de la anterior LO 15/1999 de Protección de Datos de Carácter Personal PD en cuanto a algunas las excepciones que permitían la cesión de datos de carácter personal entre las administraciones públicas ; 76/2019, F.J. 5 en relación a la declaración de inconstitucionalidad del precepto introducido por la LO 3/2018 en la LOREG en cuanto permitía sin respetar las debidas garantías la utilización de datos para crear perfiles de opiniones políticas).

[20] STC 144/1999 de 22 de julio, (BOE núm. 204, de 22 de agosto de 1999) F.J 8.

[21] STC 292/2000 op. cit. FF.JJ. 5 a 7.

[22] Dice el mencionado artículo "*1.* Toda persona *tiene derecho a la protección de los datos de carácter personal que le conciernan. 2.* Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene

La Unión Europea ha mostrado una especial preocupación en la protección de datos de carácter personal pretendiendo crear un "marco sólido y coherente para la protección de datos en la UE respaldado por una ejecución estricta" y ello "dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior"[23]. Es por ello que se ha pretendido crear un sistema completo de tutela a través de múltiples instrumentos, de los que han de destacarse el Reglamento General de Protección de Datos, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante RGPD); la *Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, del 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos, y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo*; la Directiva sobre el Comercio Interior, Directiva 2000/31/CE del Parlamento Europeo y del Consejo, del 8 de junio de 2000, relativa a determinados aspectos jurídicos de la sociedad de la información, en particular el comercio electrónico en el mercado interior; o el Reglamento (CE) 45/2001, del Parlamento Europeo y del Consejo, del 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y organismos comunitarios y a la libre circulación de esos datos.

Todo este entramado normativo, y singularmente, la obligación derivada de la entrada en vigor el 25 de mayo de 2018 del RGPD ha tenido reflejo en el ordenamiento jurídico español en la reciente Ley Orgánica 3/2008, del 5 de diciembre, de Protección de Datos Personales y Garantía de los derechos digitales. El objeto de la Ley Orgánica es doble: adaptar nuestro ordenamiento al Reglamento Europeo en materia de tratamiento de datos y garantizar los derechos y libertades predicables al entorno de internet. En materia de garantía de los derechos digitales se regulan: la neutralidad de la red y el acceso universal, los derechos a la seguridad y educación digital, los derechos al olvido, a la portabilidad y al testamento digital. Ocupa un lugar relevante el reconocimiento del derecho a la desconexión digital en el marco del derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral y la protección de los menores en internet. Finalmente, resulta destacable la garantía de la libertad de expresión y el derecho a la aclaración de informaciones en medios de comunicación digitales.

Se regulan las posibles habilitaciones legales para el tratamiento de datos fundadas en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el RGPD. Se adapta el principio de transparencia y se recoge la denominada "información por capas" ya aceptada en ámbitos como el de la videovigilancia o la instalación de dispositivos de almacenamiento masivo de datos (tales como las *"cookies"*), facilitando al afectado la información básica, si bien, indicando una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información. Se regulan junto a los derechos tradicionales acceso, rectificación, cancelación, oposición, los introducidos por el RGPD: derecho a la limitación del tratamiento y derecho a la portabilidad. Se contemplan disposiciones específicas sobre tratamientos concretos, incorporando una serie de supuestos no exhaustivos, de tratamientos lícitos que en ningún caso e nervan el deber de los responsables de adoptar las medidas de responsabilidad previstos en la propia Ley Orgánica y el RGPD, en primer lugar, aquellos respecto de los que el legislador establece una presunción *iuris tantum* de prevalencia del interés legítimo del responsable cuando se lleven a cabo con una serie de requisitos, y otros, tales como la videovigilancia, los ficheros de exclusión publicitaria o los sistemas de denuncias internas en que la licitud del tratamiento proviene de la existencia de un interés público, en los términos del RGPD, y por último se hace referencia a los presupuestos de licitud de otros tratamientos, como los relacionados con la función estadística o con fines de archivo de interés

derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.*3.* El respeto de estas normas estará sujeto al control de una autoridad independiente."

[23] Cfr. Considerando 7 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

general y los relativos a infracciones y sanciones administrativas.

Se refleja la evolución del modelo basado en el control del cumplimiento a otro fundado en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos personales para, a partir de dicha valoración, adoptar las medidas que procedan. La figura del delegado de protección de datos adquiere una destacada importancia en la resolución amistosa de reclamaciones no atendidas por el responsable o encargado del tratamiento. Siguiendo al RGPD puede tener un carácter obligatorio o voluntario, estar o no integrado en la organización del responsable o encargado y ser tanto una persona física o jurídica. Gozan de inamovilidad salvo dolo o negligencia grave. Su designación ha de comunicarse a la autoridad de protección de datos competente. La Agencia Española de Protección de Datos (AEPD) mantendrá una relación pública y actualizada de los delegados de protección de datos. Se regula el régimen de la Agencia Española de Protección de Datos (AEPD), como autoridad administrativa independiente, con facultades de investigación y auditoria y con la facultad de regulación por medio de circulares que fijan los criterios de su actuación. El procedimiento para el caso de posible vulneración de la normativa de protección de datos, siguiendo las pautas del RGPD, contempla una fase de admisión a trámite por la AEPD, la posibilidad de abrir una investigación previa al acuerdo de inicio del procedimiento sancionador y la posibilidad de adoptar medidas cautelares de bloqueo de los datos y atención inmediata del derecho recamado, entre otras. Se clasifican las infracciones consistentes en incumplimientos de la normativa en muy graves, graves y leves según el grado de incumplimiento, relegando los meros incumplimientos formales a falta leve y remitiendo al RGPD la concreción de las conductas. Se contemplan elevadas sanciones pecuniarias que pueden alcanzar los 20 000 000 de euros, o para empresas hasta 4 % del volumen de negocio total anual global del ejercicio anterior, optándose por la de mayor cuantía, así como un amplio elenco de criterios de graduación.

Es de destacar que se fija el "régimen sancionador aplicable a determinadas categorías de responsables o encargados del tratamiento", cuando se trate de autoridades y organismos públicos, se opta por la sanción de apercibimiento junto a las medidas que resulten procedentes par el cese de la conducta o la corrección de los efectos de la infracción, sin perjuicio de proponer la iniciación de actuaciones disciplinarias, en su caso.

3. La ciberseguridad como elemento de seguridad nacional.

En 2011 el Gobierno de España publica el primer documento llamado *Estrategia Española de Seguridad. Una Responsabilidad de todos*[24] *(en adelante EES 2011)*, en un contexto de crisis económica global, en que hay que afrontar la presencia de "amenazas y riesgos transversales, interconectados y transnacionales" que reclaman respuestas coordinadas no solo en el plano interno, implicando al conjunto de la sociedad, sino también a nivel internacional.

A estos efectos "amenaza es toda circunstancia o agente que ponga en peligro la seguridad o estabilidad de España" y "riesgo es la contingencia o probabilidad de que una amenaza se materialice produciendo un daño".

El conocimiento de los intereses vitales y estratégicos[25] y el análisis de las amenazas y riesgos que recaen sobre ellos, junto con las capacidades de respuesta, constituyen las bases sobre las que se formulan las directrices y líneas estratégicas necesarias para fortalecer la seguridad y bienestar.

En el análisis de los presupuestos que permitan el diseño de una adecuada estrategia de seguridad nacional, en 2011 ya se identifican las ciberamenazas junto a los riesgos tradicionales[26]. Tomando en consideración que gran parte de la actividad, tanto pública como privada, se desarrolla hoy a través de este nuevo espacio, se adquiere conciencia de la importancia de lograr un ciberespacio seguro, y de los

[24] *La Estrategia Española de Seguridad. Una Responsabilidad de todos*. Gobierno de España, *2011. Se* puede consultar en http://www.realinstitutoelcano.org/wps/wcm/connect/c06cac0047612e998806cb6dc6329423/EstrategiaEspanolaDeSeguridad.pdf?MOD=AJPERES&CACHEID=c06cac0047612e998806cb6dc6329423

[25] La EES 2011 identifica los intereses vitales como los que afectan a los derechos fundamentales y a los elementos constitutivos del Estado, mientras que los estratégicos son aquellos que afectan a la consecución de un entorno pacífico y seguro.

[26] Enumera como tales la EES conflictos armados, terrorismo, crimen organizado, inseguridad económica y financiera, vulnerabilidad energética, proliferación de armas de destrucción masiva, flujos migratorios incontrolados, emergencias y catástrofes

graves daños que pueden generar los ciberataques, en lo público y en lo privado, pudiendo llegar incluso a paralizar la actividad de un país, y, aun asumiendo que la mayoría de atentados se realizan con fines comerciales, "también estamos expuestos a agresiones por parte de grupos criminales, terroristas u otros, incluso de Estados".

La importancia de los sistemas informáticos y las redes de información y comunicación para ciudadanos y gobiernos hace de la seguridad del ciberespacio un eje fundamental de nuestra sociedad y sistema económico. "La estabilidad y prosperidad económica del país dependerá en buena medida de la seguridad de nuestro ciberespacio". La seguridad puede sufrir por causas técnicas, fenómenos naturales o por ataques ilícitos. Los ciberataques son una amenaza creciente por su potencial para afectar incluso a las infraestructuras críticas que puede proceder del terrorismo, crimen organizado, Estados o individuos aislados. De hecho, si inicialmente los ataques procedían, por lo general, de individuos aislados que empleaban una infraestructura mínima, hoy se habla ya de una "enorme industria criminal" en torno a la informática[27]. Además, se trata de enfrentar nuevos retos como el ciberespionaje, provenga de agentes criminales o de otros Estados. Pero la mayor parte de ataques se realizan con fines económicos. La captación de información y datos personales a través de la Red, frecuentemente para comerciar con ellos, preocupa más incluso que por su coste en términos económicos, por el efecto desestabilizador para la economía que puede acarrear la pérdida de confianza en los sistemas electrónicos de pago. Pero además se toma conciencia del valor de la ciberseguridad desde la perspectiva competitiva para atraer la confianza de las inversiones.

La estrategia identificaba dos tipos de factores que favorecen las ciberamenazas, legales y tecnológicos. Entre los primeros, la ausencia de una legislación común o de seguridad global que permita combatirlas de modo efectivo, entre los segundas el olvido de la seguridad en los momentos iniciales, ya que la red se creó para ser útil y sencilla, sin pensar en la seguridad. La inclusión en ella de las infraestructuras, suministros y servicios críticos, aumenta los niveles de riesgos sobre estos. El anonimato y la complejidad para rastrear los ataques, dificultan su neutralización. Se hace vital la cooperación tanto internacional como interna público-privada, y la concienciación de todos, sector público, privado y ciudadanos en los riesgos de seguridad.

La política de seguridad se sustenta en el documento de 2011 en seis conceptos básicos: Enfoque integral, coordinación público-privada, eficiencia en el uso de los recursos, anticipación y prevención de las amenazas y riesgos, resistencia y recuperación de sistemas e instrumentos e interdependencia responsable con nuestros socios y aliados. En el plano de la ciberseguridad se marcaban como líneas estratégicas de acción, entre otras, el fortalecimiento de la legislación sin merma de la privacidad, el fomento de la cooperación nacional e internacional, del sector público y privado, la concienciación de todos, administraciones, empresas y ciudadanos sobre los riesgos, la elaboración de mapas de riesgos, catálogos de expertos, recursos y buenas prácticas, y el aumento de la inversión en tecnologías de seguridad y en formación especializada. La estrategia de 2011, consciente de la importancia creciente de la seguridad del ciberespacio en la Seguridad Nacional, concluye precisamente con la previsión de la elaboración de la primera Estrategia específica sobre Ciberseguridad, que vería la luz en 2013.

La Estrategia de Ciberseguridad Nacional aprobada por el Consejo de Seguridad Nacional el 5 de diciembre de 2013 (en adelante ECN 2013), alerta de los riesgos derivados de la dependencia actual del ciberespacio con el incesante flujo de información que este propicia y de la proliferación de las acciones delictivas en el nuevo espacio, alentadas por la rentabilidad de su explotación en términos económicos e incluso políticos, la facilidad de ejecución y el bajo coste de los elementos empleados para los ataques, el reducido riesgo para los autores por el anonimato que otorga el escenario, la facilidad de ocultación y la posibilidad de atacar desde cualquier punto del planeta, así como por el alto impacto de las consecuencias de los ataques. Considera el carácter trasnacional de la

[27] Cfr. González Cussac, J.L. " *Tecnocrimen*", en AA.VV: "Nuevas Amenazas a la seguridad nacional: Terrorismo , criminalidad organizada y tecnologías de la información y la comunicación". Tirant Lo Blanch , 2013 pág. 216 " *(...)las posibilidades de beneficio económico para estos cualificados especialistas capaces de aprovechar ilícitamente las brechas de seguridad en sistemas y programas informáticos de terceros, solo pueden ofrecerlas ahora las redes de delincuencia organizada. Precisamente la evolución de este maridaje es sumamente signiicativa, desde los comienzos con los fraudes en el comercio electrónico y en la banca electrónica, hasta el mismo nacimiento de grupos especializados en la comisión de ciberdelitos, como por ejemplo, el malware".*

ciberseguridad y atribuye carácter esencial a la cooperación con la Unión Europea y otros organismos de ámbito internacional o regional.

Define el ciberespacio como "dominio global y dinámico compuesto por las infraestructuras de tecnología de la información –incluida internet–, las redes y los sistemas de información y de telecomunicaciones" reconociendo que, si bien proporciona nuevas oportunidades, también comporta nuevos retos, riesgos y amenazas "conocer sus amenazas, gestionar los riesgos y articular una adecuada capacidad de prevención, defensa, detección, análisis, investigación, recuperación y respuesta constituyen elementos esenciales de la Política de Ciberseguridad Nacional".

Afronta la ciberseguridad como motor del progreso económico, pues un entorno más seguro es esencial para atraer la inversión, generar empleo e incrementar la competitividad. Pretende establecer un modelo integrado basado en la implicación coordinación y armonización de todos los actores y recursos del Estado, la cooperación público-privada y la participación ciudadana. Esta necesidad de implicar a los propios ciudadanos en la gestión de los riesgos que para la seguridad nacional derivan del nuevo escenario es consecuencia del reconocimiento de la incapacidad misma de los Estados de hacerle frente por sí solos28. Y marca las directrices y líneas generales de actuación para enfrentar el desafío de la vulnerabilidad del ciberespacio.

Se consagran como principios rectores de la ciberseguridad: el liderazgo nacional y la coordinación de esfuerzos, la responsabilidad compartida, la proporcionalidad, racionalidad y eficacia y la cooperación internacional.

Entre los objetivos de la política de Ciberseguridad se destaca el objetivo global de lograr un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa y detección, análisis, investigación, recuperación y respuesta a los ciberataques. Se fijan además seis objetivos específicos por ámbitos "1) para las administraciones públicas, garantizar que sus sistemas de información y telecomunicación utilizadas por estas, posean el adecuado nivel de seguridad y resiliencia; 2) para las empresas y las infraestructuras críticas, impulsar la seguridad y la resiliencia de las redes y los sistemas de información usados por el sector empresarial en general y los operadores de infraestructuras críticas en particular; 3) en el ámbito judicial y policial, potenciar las capacidades de prevención, detección, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio; 4) en materia de sensibilización, concienciar a los ciudadanos, profesionales, empresas y administraciones públicas españolas de los riesgos derivados del ciberespacio; 5) en capacitación, alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de la ciberseguridad; y 6) en lo que se refiere a la colaboración internacional, contribuir en la mejora de la ciberseguridad, apoyando el desarrollo de una política de ciberseguridad coordinada en la Unión Europea y en las organizaciones internacionales, así como colaborar en la capacitación de Estados que lo necesiten a través de la política de cooperación al desarrollo." Y desarrolla la estructura orgánica de la ciberseguridad dentro del esquema orgánico de la Seguridad Nacional.

En el acuerdo del mismo día, 5 de diciembre de 2013, el Consejo de Seguridad Nacional crea el Consejo Nacional de Ciberseguridad, como órgano de apoyo del Consejo de Seguridad Nacional encargado de la coordinación de los organismos con competencias en la materia a nivel nacional y del desarrollo del Plan Nacional de Ciberseguridad y los planes derivados.

La Ley 36/2015 de Seguridad Nacional del 28 de septiembre[29], califica la ciberseguridad de "ámbito de especial interés de la seguridad nacional" y en la Estrategia de Seguridad Nacional aprobada en 2017

[28] Fernández Hernández, A. " ciberamenzas a la Seguridad Nacional "en AA.VV "Nuevas Amenazas a la seguridad nacional: Terrorismo , criminalidad organizada y tecnologías de la información y la comunicación". Tirant Lo Blanch, Valencia, 2013, p. 162.

[29] El artículo 10 de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional (BOE núm. 233, de 29 de septiembre de 2015) dispone " se consideran ámbitos de especial interés de la Seguridad Nacional aquellos que requieren una atención específica por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y garantizar el suministro de los servicios y recursos esenciales. A los efectos de esa ley, serán, entre otros, la ciberseguridad, la seguridad económica y financiera, la seguridad marítima, la seguridad del espacio aéreo y ultraterrestre, la seguridad energética, la seguridad sanitaria y la preservación del medio ambiente ". Y el artículo 11 contiene las obligaciones de las administraciones públicas en aquellos ámbitos de especial interés que pasan por establecer mecanismos de coordinación, intercambio de información en especial en lo que refiere a los sistemas de vigilancia y alerta ante posibles riesgos y amenazas.

[30], adquiere un espacio central en cuanto "el proceso de revolución tecnológica está llamado a transformar las sociedades y los modos de vida(…) el desarrollo tecnológico está asociado a una mayor exposición a nuevas amenazas, especialmente las asociadas al ciberespacio. La hiperconectividad actual agudiza algunas de las vulnerabilidades del sistema de seguridad y exige una mejor protección de las redes y sistemas, así como de la privacidad y los derechos digitales del ciudadano(…)". La ley caracteriza el desarrollo tecnológico como "instrumento de activación económica, crecimiento y progreso" pero reconoce que la tecnología "ha premiado al interconectividad en detrimento de la seguridad" y que "actos como el robo, uso y difusión de la información, acciones hostiles que incluyen actividades de desinformación e interferencias en procesos electorales representan hoy un desafío de grandes dimensiones". Advierte de las implicaciones que para la seguridad tendrán la inteligencia artificial, la ingeniería genética, el internet de las cosas y la robotización .

Recientemente el Consejo de Seguridad Nacional ha aprobado la Estrategia Nacional de Ciberseguridad 2019[31], que desarrolla las previsiones de la estrategia de Seguridad Nacional de 2017 en este ámbito específico.

La estrategia vigente caracteriza el ciberespacio como "espacio común global" y parte de los desafíos que para la seguridad plantea la ausencia de soberanía, la débil jurisdicción, facilidad de acceso y dificultad de atribución de las acciones. La digitalización acelerada, la inteligencia artificial, la robótica, el *big data*, el *bockchain* y el internet de las cosas son una realidad cuyo potencial transformador excede de lo tecnológico y afecta a los modelos sociales, las relaciones personales y la ética.

Pero el ciberespacio, junto a su naturaleza virtual tiene una base física, los elementos que conforman las redes y sistemas de información y comunicación de los que dependen las infraestructuras críticas y los servicios esenciales, su vulnerabilidad es la de las propias infraestructuras y servicios esenciales, un ataque a las bases físicas puede tener resultados impredecibles.

Por otro lado, se reputa esencial a la seguridad nacional el preservar los valores y principios constitucionales y democráticos, los derechos fundamentales de las personas en el ciberespacio, en especial su privacidad, la protección de los datos personales, la libertad de expresión y el acceso a una información veraz y de calidad. Todos ellos reclaman un enfoque multidisciplinario bajo los principios de unidad y coordinación. En esta línea, González Cussac identificaba como una de las tendencias claras a la hora de abordar un nuevo concepto de seguridad nacional "que resulte eficaz como criterio central de gestión de las nuevas amenazas y necesidades estratégicas" y al tiempo sea compatible con el Estado democrático y de Derecho, este enfoque multidisciplinario, como equivalente a exención de peligros en los ámbitos militar, político, económico, social y medioambiental y, por tanto, "entendida como seguridad colectiva, compartida y global"[32].

El sector privado, al ser uno de los principales titulares de los activos digitales se convierte en actor principal en materia de ciberseguridad, y se debe implicar en el objetivo de crear un entorno digital seguro y fiable. Es por ello que se ha de potenciar la inversión en ciberseguridad de las empresas, en el entendido, además, de que en el diseño de los elementos se ha hecho primar más el criterio comercial que la seguridad y se trata ahora de revertir dicha situación.

Se pretende pasar de un modelo preventivo y defensivo a otro de mayor capacidad disuasoria lo que eleva a fundamental la acción del Estado dirigida a obtener y potenciar capacidades de ciberdefensa.

Las ciberamenazas entendidas como "disrupciones o manipulaciones maliciosas que afectan a elementos tecnológicos" son transversales, desconocen las barreras geográficas, y pueden afectar a todos los ámbitos de la Seguridad Nacional. El anonimato que proporciona el sistema dificulta aún más su persecución. Pero, sobre todo, son cada vez más variadas, tanto en la intensidad como en la forma de presentarse o en sus motivaciones, y están en constante evolución. De ahí que la ciberinteligencia adquiera un papel clave a la hora de identificar y anticipar riesgos y amenazas en orden a combatirlos con las respuestas rápidas y eficaces que reclama un escenario tan extraordinariamente dinámico. Y el propio desarrollo tecnológico se

[30] Cfr. Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la estrategia de Seguridad Nacional 2017 (BOE núm. 309, de 21 de diciembre de 2017).

[31] Ver Orden PCI/487/2019.

[32] Cfr. González Cussac, J.L. "Tecnocrimen…" op. cit. págs. 207 y 208

presenta como una herramienta extraordinariamente eficaz en este campo. Las tecnologías de la información y la comunicación agilizan significativamente la búsqueda, recopilación y tratamiento de datos para lograr la información que permita una adecuada evaluación de los riesgos y amenazas en orden a anticiparlos y prevenirlos o combatirlos adecuadamente. La nube está propiciando una nueva revolución industrial soportada en las nuevas "fábricas de datos" (centros de datos, *data centers*) y de aplicaciones web (*web apps*). Esta nueva revolución producirá un gran cambio social, tecnológico y económico[33] pero también tiene consecuencias en el campo de los derechos y libertades. Así ha sido puesto de manifiesto por Ramírez Barbosa al analizar el conocido caso Odebrecht[34].

Pero aquí aparece de nuevo la eterna pugna entre seguridad y libertades[35], el clásico problema de los límites, revitalizado en un escenario de alarma por las consecuencias del nuevo terrorismo extendido a nivel global, que ha propiciado la armonización de las legislaciones estatales especialmente interesadas en combatir no solo sus acciones sino también los grupos mismos a través de la estrangulación de sus fuentes de captación de adeptos y su financiación[36]. Tan loables fines ciertamente exigen sacrificios pero es necesario poner barreras de modo que se produzca la mínima injerencia en los derechos fundamentales[37]. En esta línea, no puede olvidarse el empleo por los Estados de las utilidades que ofrecen las nuevas tecnologías con fines de investigación que alcanza cotas, que en muchas ocasiones tienen difícil encaje en un Estado de Derecho. Con acierto señala Cuerda Arnau que "los sistemas tradicionales de observación y seguimiento son "reliquias del pasado"[38] sustituidas por nuevas técnicas de vigilancia cuyo ejemplo paradigmático es el "control estratégico de las telecomunicaciones", la recogida aleatoria de información y su procesamiento empleando filtros de búsqueda con palabras clave. Destaca que *Echelon*[39] es considerada la mayor red de espionaje de la historia, con capacidad de captar toda clase de comunicaciones en prácticamente todo el mundo, y someterlas a análisis mediante filtros que emplean determinadas palabras clave en función del interés de la investigación concreta[40]. Si el sistema *Echelon* generó la aprobación por el Pleno del Parlamento Europeo de la Resolución del 5 de septiembre de 2001, que concluyó con la recomendación de que se adopten medidas para que los Estados miembros de la Unión Europea se comprometan a prohibir el espionaje industrial y a no participar en él directa o indirectamente, las revelaciones que, desde junio de 2013, derivaron de los documentos filtrados por el excontratista de la Agencia Nacional de Seguridad de los Estados Unidos, Edward Snowden, sobre los programas de Inteligencia de la Agencia[41] determinaron

[33] Cfr. Joyanes Aguilar, L. "*Introducción. Estado del arte de la ciberseguridad*" , en "*Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*"; Instituto Español de Estudios Estratégicos. Ministerio de Defensa, Cuadernos de Estrategia nº 149, Madrid, 2010, pág. 23

[34] Cfr. Ramírez Barbosa, P.A. "La ley contra las prácticas corruptas en el extranjero. La FCPA de Estados Unidos: "compliance", extraterritorialidad y responsabilidad de la persona jurídica. Reflexiones acerca del caso Odebrecht", en AAVV "Desafíos del Derecho Penal en la sociedad del Siglo XXI", Bogotá, 2018, p. 38 y sig.

[35] Como sostiene Silva Sánchez la antinomia entre libertad y seguridad ha sido el detonante de la crisis del derecho penal contemporáneo. Vid Silva Sánchez, J.M. "Aproximación al derecho penal contemporáneo", Barcelona 1992. P 13 y ss.

[36] Sobre esta cuestión vid. Ferré Olivé, J.C. "Instrumentos internacionales en la lucha contra la financiación del terrorismo" en AA.VV. " financiación del Terrorismo" Valencia 2018. p 57 y ss.

[37] Ver Lamarca Pérez, C. " *Terrorismo trasnacional*", en AA.VV. "*Política criminal ante el reto de la delincuencia trasnacional*" Tirant Lo Blanch, Valencia, 2016 , p.460 " En todo caso , las acciones terroristas lo que han venido propiciando no es solo un reforzamiento de las medidas jurídicas para combatirlas sino la aparición de una auténtica legislación de emergencia permanente cuya vis expansiva y excepcionalidad han convertido a la legislación antiterrorista en uno de los mejores bancos de prueba que se puede utilizar para conocer el estado de salud de que goza un Estado democrático pues es precisamente en esta materia donde el sistema política, incluso el más democrático, muestra de modo patente una tendencia claramente autoritaria, que lesiona de manera muy grave la eficacia de las garantías individuales"

[38] Cuerda Arnau, M.L. "*Intervenciones prospectivas y secreto de las comunicaciones. Cuestiones pendientes*" en AA.VV: "*Nuevas Amenazas a la seguridad nacional: Terrorismo , criminalidad organizada y tecnologías de la información y la comunicación*". Tirant Lo Blanch, Valencia, 2013. p 107

[39] En realidad el nombre Echelon solo designa la sección de espionaje de señales destinada a la interceptación de comunicaciones vía satélite , que es parte del sistema más amplio del Sistema de espionaje de Señales de los Estados Unidos (USSS)

[40] Sobre los métodos prospectivos de vigilancia mediante el empleo de las nuevas tecnologías vid. ampliamente Cuerda Arnau, M.L. "*Intervenciones prospectivas y secreto de las comunicaciones. Cuestiones pendientes*" en AA.VV: "*Nuevas Amenazas a la seguridad nacional: Terrorismo , criminalidad organizada y tecnologías de la información y la comunicación*". Tirant Lo Blanch , 2013. p. 103 y ss Vid. también en la misma obra colectiva Górriz Royo, E.M. " Investigaciones prospectivas y secreto de las comunicaciones: respuestas jurídicas", p.243 y ss.

[41] Según la Resolución del Parlamento Europeo de 12 de marzo de 2014, , se trata de programas que permiten la vigilancia masiva de ciudadanos mediante el acceso directo a los servidores centrales de las empresas estadounidenses líderes en internet (programa PRISM) , el análisis de contenido y metadatos (programa Xkeys-

la resolución del Parlamento Europeo del 12 de marzo de 2014, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los Estados Unidos, los órganos de vigilancia en diversos Estados Miembros y su impacto en los Derechos Fundamentales de los ciudadanos de la Unión Europea y en la cooperación trasatlántica en materia de justicia y asuntos de interior (P7_TA(2014)0230)[42], en que refiere al impacto de la vigilancia masiva, para señalar que las medidas de seguridad incluidas las de la lucha contraterrorista han de sujetarse a las obligaciones en materia de derechos fundamentales incluidas las relacionadas con la intimidad y protección de datos. Destaca asimismo la Resolución, que en un memorando del 7 de enero de 2014, la propia Agencia de Seguridad de los Estados Unidos puso de manifiesto la ineficacia de la vigilancia masiva de datos para la prevención de actos terroristas, que los servicios de inteligencia de las sociedades democráticas están sujetos a una rendición de cuentas democrática y al control judicial y han de usar los poderes y capacidades que se ponen a su disposición dentro de los límites legales impuestos por los derechos fundamentales, la democracia y el Estado de Derecho, y condena la recopilación de datos generalizada, extensa y sistemática que se ha llevado a cabo. Finalmente, presenta una serie de Recomendaciones como un plan de prioridades y un "Habeas corpus digital europeo –proteger los derechos fundamentales en una era digital–" con ocho acciones concretas estableciendo también un plan de seguimiento.

La incidencia de las nuevas tecnologías también se deja sentir en el campo de la respuesta penal con la preocupante introducción de la inteligencia artificial y el uso de algoritmos en orden a condicionar las labores de determinación de las penas, la aplicación de medidas de seguridad y la procedencia de la libertad condicional que se viene imponiendo en el sistema de justicia de los Estados Unidos y se pretende exportar a otros sistemas jurídicos[43].

Las mismas condiciones que hacen del ciberespacio un motor del progreso, son utilizadas con fines maliciosos, alentadas por la protección que proporciona el anonimato. Internet y las redes sociales pueden ser utilizados perversamente como medios de influencia y poder, el espionaje pasa a ser ciberespionaje facilitado enormemente con el cambio de escenario, y surgen las llamadas Amenazas Persistentes Avanzadas (APTS), que en general funcionan a modo de espías instalados en los sistemas para apoderarse de información durante un cierto periodo y pueden afectar tanto a empresas como al sector público, incluso a gobiernos, las *amenazas híbridas* , entendidas como acciones coordinadas y sincronizadas dirigidas a atacar las vulnerabilidades sistémicas de los Estados democráticos y las instituciones, mediante ciberataques, manipulación de información o elementos de presión económica.

La cibercriminalidad se concibe en la recientemente aprobada Estrategia Nacional de Ciberseguridad como problema de seguridad ciudadana, y comprende todas las "actividades ilícitas cometidas en el ciberespacio que tienen por objeto los elementos, sistemas informáticos o cualesquiera otros bienes jurídicos, siempre que en su planificación, desarrollo y ejecución resulte determinante la utilización de herramientas tecnológicas" incluyendo ciberterrorismo, ciberdelito o hacktivismo. Destaca Subijana Zunzunegui que los ilícitos cometidos en el ciberespacio tienen cuatro características específicas: "se cometen fácilmente; requieren escasos recursos en relación al perjuicio que causan; pueden cometerse en una jurisdicción sin estar físicamente presente en el territorio sometido a la misma; y se benefician de lagunas de punibilidad que pueden existir en determinados Estados, los cuales han sido denominados paraísos cibernéticos, debido a su nula voluntad política de tipificar y sancionar estas conductas".[44] Los grupos terroristas aprovechan vulnerabilidades del ciberespacio para

core) la elusión del cifrado en línea (BULLRUN) el acceso a redes informática y telefónicas y a datos de localización, y algunos programas de la Agencia de inteligencia británica GCHQ , como la actividad preliminar de vigilancia (programa Tempora) , el programa de descifrado (Edgehill) , los ataques selectivos con intermediarios contra sistemas de información)(programas Quantumtheory y Foxacid) y la recopilación y retención de 200 millones de mensajes de texto al día (programa Dishfire).

[42] El texto íntegro se puede consultar en la página del Parlamento Europeo http://www.europarl.europa.eu/sides/getDoc.do?reference=P7-TA-2014-0120

[43] Sobre esta cuestión vid. ampliamente Romeo Casabona, C.M. "*Riesgo, procedimientos actuariales basados en inteligencia artificial y medidas de seguridad*". Revista Penal 42, julio 2018. p.166 y ss. Vid. también Miró Llinares, F. *"Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots*". Revista de derecho penal y criminología, 20 , 2018. p. 87 y ss. y De la Cuesta Aguado, P. "*La ambigüedad no es programable: racionalización normativa y control interno en inteligencia artificial*". Revista Aranzadi de Derecho y proceso penal, 44, 2016, p 165 y ss.

[44] Subijana Zunzunegui, J.I., "*El ciberterrorismo: una perspectiva legal y judicial*" Eguzkilore, Número 22. San Sebastián, 2008, p. 171

sus ataques, actividades de radicalización, financiación, adiestramiento o propaganda. La ciberdelincuencia opera con esquemas del crimen organizado, amparada por el anonimato que proporciona el nuevo espacio y el empleo de criptomonedas para el comercio de bienes y servicios ilícitos, la extorsión el fraude y la falsificación de medios de pago, está a la orden del día. De igual modo, el blanqueo de capitales y el fraude fiscal son fuente de ingresos para el crimen organizado que se vale de las nuevas tecnologías para favorecer su actividad. El hacktivismo aprovecha el sistema para realizar ataques con motivaciones ideológicas de gran impacto mediático.

Especial atención merecen por su efecto desestabilizador las campañas de desinformación mediante la difusión de noticias falsas aprovechando el efecto multiplicador de las redes sociales, como medio de ataque a Estados, organizaciones internacionales, personajes públicos e incluso procesos electorales. Y asimismo, dado el creciente valor de la información digital, el uso de los datos personales que circulan en la red para múltiples finalidades incluido el comercio de datos, pone en riesgo la privacidad, la confidencialidad de los datos y la libertad informática de las personas.

Apunta en su introducción la ENC 2019[45] que se ha de tener en cuenta la concepción del ciberespacio como vector de comunicación estratégica, que puede ser utilizado, como ya reconocía la ESN 2017, para influir en la opinión pública y en la forma de pensar de las personas a través de la manipulación de la información, de las campañas de desinformación o las acciones de carácter híbrido.

El objetivo de la ciberseguridad es hoy, en términos de la Estrategia de Seguridad Nacional de 2017 "garantizar un uso seguro y responsable de las redes y los sistemas de información y comunicaciones a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques potenciando y adoptando medidas específicas para contribuir a la promoción de un ciberespacio seguro y fiable" y ello pasa por fomentar la cultura de la ciberseguridad implicando a toda la sociedad, por impulsar la industria de ciberseguridad promoviendo la investigación, el

[45] Sin duda recuerda incidentes como los protagonizados por la Compañía *Cambridge Analytica* y su intervención en las últimas campañas electorales de Estados Unidos, Argentina y en el Referéndum para la salida de Reino Unido de la Unión Europea, mediante la explotación de datos personales obtenidos de millones de usuarios de Facebook. Recientemente en julio 2019 la Comisión Federal de Comercio de Estados Unidos ha sancionado a Facebook con una multa de 5.000 millones de dólares por compartir datos de millones de usuarios con la Compañía Cambridge Analytica. El Tribunal Constitucional español declaró en la ya citada STC 76/2019, de 22 de mayo contrario a la Constitución y nulo el apartado 1 del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del régimen electoral general, incorporado a esta por la disposición final tercera, apartado dos, de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, que disponía "Utilización de medios tecnológicos y datos personales en las actividades electorales. *1.La recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas.* Parte el TC de asumir que el precepto constituye una injerencia en el derecho fundamental a la protección de datos personales garantizado por el artículo 18.4 CE. El Reglamento (UE) 2016/679 General de Protección de Datos no excluye que los Estados puedan autorizar la recopilación de datos personales sobre las opiniones políticas en el marco de actividades electorales, si bien esa autorización está expresamente condicionada al establecimiento de "garantías adecuadas", disponiendo su considerando 56: "Si, en el marco de actividades electorales, el funcionamiento del sistema democrático exige en un Estado miembro que los partidos políticos recopilen datos personales sobre las opiniones políticas de las personas, puede autorizarse el tratamiento de estos datos por razones de interés público, siempre que se ofrezcan garantías adecuadas" . Concluye el TC , estimando el recurso promovido por el Defensor del Pueblo , que se han producido tres vulneraciones del art 18.4 CE en relación con el 53.1 CE en cuanto la ley no ha identificado la finalidad de la injerencia para cuya realización se habilita a los partidos políticos, ni ha delimitado los presupuestos ni las condiciones de esa injerencia, ni ha establecido las garantías adecuadas que para la debida protección del derecho fundamental a la protección de datos personales reclama la doctrina constitucional, por lo que se refiere a la recopilación de datos personales relativos a las opiniones políticas por los partidos políticos en el marco de sus actividades electorales. Las tres vulneraciones " autónomas e independientes entre sí, todas ellas vinculadas a la insuficiencia de la ley y que solo el legislador puede remediar, y redundando las tres en la infracción del mandato de preservación del contenido esencial del derecho fundamental que impone el artículo 53.1 CE, en la medida en que, por una parte, la insuficiente adecuación del precepto cuestionado a los requerimientos de certeza crea, para todos aquellos a los que recopilación de datos personales pudiera aplicarse, un peligro, en el que reside precisamente dicha vulneración y, por otra parte, la indeterminación de la finalidad del tratamiento y la inexistencia de «garantías adecuadas» o las «mínimas exigibles a la Ley» constituyen en sí mismas injerencias en el derecho fundamental de gravedad similar a la que causaría una intromisión directa en su contenido nuclear". Y asimismo razona que "Las garantías adecuadas deben velar por que el tratamiento de datos se realice en condiciones que aseguren la transparencia, la supervisión y la tutela judicial efectiva, y deben procurar que los datos no se recojan de forma desproporcionada y no se utilicen para fines distintos de los que justificaron su obtención. La naturaleza y el alcance de las garantías constitucionalmente exigibles en cada caso dependerán de tres factores: el tipo de tratamiento de datos que se pretende llevar a cabo; la naturaleza de los datos; y la probabilidad y la gravedad de los riesgos de abuso y de utilización ilícita que, a su vez, están vinculadas al tipo de tratamiento y a la categoría de datos de que se trate."

desarrollo y la innovación, así como la cooperación internacional.

Los principios rectores de la Seguridad Nacional; unidad de acción, anticipación, eficiencia y resiliencia, se trasladan al ciberespacio. En este campo resulta esencial la unidad de respuesta ante posibles incidentes para asegurar una acción coordinada, rápida, que limite al máximo los tiempos de respuesta y eficaz; ha de primar la prevención sobre la reacción. En tiempos de crisis económica resulta fundamental optimizar los recursos implicados. El fomento de la resiliencia especialmente en lo que afecta a los sistemas e infraestructuras críticas es clave para la Seguridad Nacional. Merece en este punto destacar iniciativas como las de Estonia que desde 2014 iniciaba los trabajos preparatorios de las "embajadas de datos", esto es centros de datos situados en infraestructuras nacionales en Estados aliados, con réplicas de los sistemas TIC y las bases de datos críticas para asegurar la continuidad del funcionamiento del país en caso de contingencias como invasión, ciberataque o catástrofe natural[46].

El objetivo general de crear un uso seguro y fiable del ciberespacio protegiendo los derechos y libertades y promoviendo el progreso económico se desarrolla en la estrategia de 2019 en cinco objetivos específicos: seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales; uso seguro del ciberespacio frente a su uso ilícito o malicioso; protección del ecosistema empresarial y social y de los ciudadanos; cultura y compromiso con al ciberseguridad y potenciación de las capacidades humanas y tecnológicas; y seguridad del ciberespacio en el espacio internacional. Para la consecución de tales objetivos se trazan una serie de líneas de acción y medidas concretas que pasan por el refuerzo de las capacidades ante las amenazas, mediante la mejora de la capacidad de detección y análisis, la potenciación de la cooperación de los sectores público y privado, incluso de organismos internacionales competentes, la intensificación de la inteligencia y el ágil intercambio de información en orden a lograr una alerta temprana que permita acciones preventivas o en su caso, respuestas tempranas, introduciendo útiles sistemas de evaluación, e intensificando la inteligencia y el AL CIBERCRIMINALIDAD as nciales emprana que permita acciones preventivas o en su caso , respuestas tempranas , introduceindo sisrápido intercambio de información con fines de prevención.

[46] Sobre esta cuestión se puede consultar el artículo "Estonia y las embajadas de datos " de Fojón Chamorro.E , publicado en "Ciberseguridad y Ciberdefensa" el 5 de julio de 2017 *Blog.real-institutoelcano.org/estonia-y-las-embajadas-de-datos*

4. Conclusión

Asistimos a un momento de transformación permanente en todos los aspectos de la vida de la mano del imparable desarrollo tecnológico que, obviamente, tiene repercusiones en el ámbito del derecho que se presentan como desafíos que no pueden abordarse desde las perspectivas ni con los instrumentos tradicionales, y exigen, más que nunca, un esfuerzo coordinado a nivel mundial que implique a todos los Estados y a todas las sociedades en orden a lograr que este nuevo espacio en que inevitablemente nos desarrollamos sea un lugar seguro y fiable, sin renunciar a las conquistas que supone el Estado de Derecho.

5. Bibliografía

Agustina, J.R. "Cibercriminalidad y perspectiva victimológica: un enfoque general explicativo de la cibervictimización", Cuadernos de Política Criminal, nº 114, 2014.

Cuerda Arnau, M.L. "Intervenciones prospectivas y secreto de las comunicaciones. Cuestiones pendientes" en AAVV "Nuevas Amenazas a la seguridad nacional: Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación". Tirant Lo Blanch, Valencia, 2013. p 103 y ss.

De Alfonso Laso, D. "Intimidad y protección de datos en el derecho penal "en AAVV "Delincuencia informática. Problemas de Responsabilidad". Cuadernos de Derecho Judicial IX. Madrid 2002.

De la Cuesta Aguado, P. "La ambigüedad no es programable: racionalización normativa y control interno en inteligencia artificial". Revista Aranzadi de derecho y proceso penal, 44, 2016.

Ferré Olivé, J.C. "Tecnologías de información y comunicación, comercio electrónico, precios de transferencia y fraude fiscal", en AAVV, "Nuevas Amenazas a la seguridad nacional: Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación". Tirant Lo Blanch, 2013.

Ferré Olivé, J.C. "Instrumentos internacionales en la lucha contra la financiación del terrorismo" en AA.VV. "Financiación del Terrorismo", Valencia, 2018.

González Cussac, J.L. "Tecnocrimen", en AAVV "Nuevas Amenazas a la seguridad nacional: Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación". Tirant Lo Blanch, Valencia, 2013.

González Cussac, J.L., "Estrategias legales frente a las ciberamenzas", en "Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio"; Instituto Español de Estudios Estratégicos. Ministerio de Defensa, Cuadernos de Estrategia nº 149, Madrid, 2010.

Jacobs, Jane "The death an life or great american cities". Ed. Random House, New York, 1961.

Joyanes Aguilar, L. "Introducción. Estado del arte de la ciberseguridad", en "Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio"; Instituto Español de Estudios Estratégicos. Ministerio de Defensa, Cuadernos de Estrategia nº 149, Madrid, 2010.

Katyal, N.K. "Digital Architecture as Crime Control". The Yale Law Journal. Vol. 111, nº 5, 2002.

Katyal, N.K. "Digital Architecture as Crime Control". The Yale Law Journal. Vol. 112, nº 8, 2003.

Lamarca Pérez, C. "Terrorismo trasnacional", en AA.VV. "Política criminal ante el reto de la delincuencia trasnacional", Tirant Lo Blanch, Valencia, 2016.

Merry, Sally E. "Defensible Space Undefended: Social Factors in Crime Control Through Environmental Design". Urban Affairs Quarterly, Vol. 16, 1981.

Miró Llinares, F. "Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots". Revista de derecho penal y criminología, nº 20, 2018.

Navarro Cardoso, F. "Corrupción, transparencia y derecho penal. Especial referencia al derecho de acceso a la información". Cuadernos de Política Criminal, Número 114, 2014.

Ramírez Barbosa, P.A. "La ley contra las prácticas corruptas en el extranjero. La FCPA de Estados Unidos: "compliance", extraterritorialidad y responsabilidad de la persona jurídica. Reflexiones acerca del caso Odebrecht", en AAVV "Desafíos del Derecho Penal en la sociedad del Siglo XXI", Bogotá, 2018.

Romeo Casabona, C.M. "Riesgo, procedimientos actuariales basados en inteligencia artificial y medidas de seguridad". Revista Penal 42, julio 2018.

Silva Sánchez, J.M. "Aproximación al derecho penal con temporáneo", Barcelona 1992.

Pons Gamón, V. "Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad". Revista Latinoamericana de Estudios de Seguridad, nº 20, Quito, 2017.

Subijana Zunzunegui, J.I. "El ciberterrorismo: una perspectiva legal y judicial "Eguzkilore, nº 22. San Sebastián, 2008.

Vidaurri Aréchiga, M. "Delitos Informáticos. Los retos del derecho penal". En AAVV "Ciberdelitos". Tirant lo Blanch, México, 2019.