Decálogo sobre a nova normativa de protección de datos

Decálogo sobre la nueva normativa de protección de datos

Decalogue on the new data protection regulations

JOSÉ JULIO FERNÁNDEZ RODRÍGUEZ
Profesor titular de Dereito Constitucional
Delegado de Protección de Datos
Universidade de Santiago de Compostela
josejul.fernandez@usc.es

Recibido: 15/11/2018 | 22/01/2019

Resumo: O artigo aborda os dez aspectos máis relevantes da nova normativa de protección de datos, sobre a base do Regulamento UE 2016/679 e a Lei orgánica 3/2018. Iso faise tanto desde un punto de vista descritivo como desde posicións máis analíticas e explicativas. Previamente realízase un enfoque situacional que subliña o papel que representa na actualidade o dereito fundamental á protección de datos no marco dunha Sociedade da Información hiperglobalizada. O enfoque, aínda que resulta preferentemente xurídico, complétase con aspectos sociolóxicos e politolóxicos.
Palabras clave: Protección de datos, Regulamento (UE) 2016/679, LO 3/2018, dereito fundamental, principios, bases de lexitimación, dereitos, responsable de tratamento, delegado de protección de datos, autoridade de protección de datos, infraccións e sancións.

Resumen: El artículo aborda los diez aspectos más relevantes de la nueva normativa de protección de datos, sobre la base del Reglamento UE 2016/679 y la Ley orgánica 3/2018. Ello se hace tanto desde un punto de vista descriptivo como desde posiciones más analíticas y explicativas. Previamente se hace un enfoque situacional que subraya el papel que representa en la actualidad el derecho fundamental a la protección de datos en el marco de una Sociedad de la Información hiperglobalizada. El enfoque, aunque resulta preferentemente jurídico, se completa con aspectos sociológicos y politológicos.
Palabras clave: Protección de datos, Reglamento (UE) 2016/679, LO 3/2018, derecho fundamental, principios, bases de legitimación, derechos, responsable de tratamiento, delegado de protección de datos, autoridad de protección de datos, infracciones y sanciones.

Abstract: The paper addresses the ten most relevant aspects of the new data protection regulations, based on the Regulation EU 2016/679 and Organic Act 3/2018. This is done both from a descriptive point of view, and from more analytical and explanatory positions. Previously, a situational approach is made that highlights the role currently played by the fundamental right to data protection within the framework of

a hyperglobalized Information Society. The approach, although it is preferably legal, is completed with sociological and political aspects.
Key words: Data protection, Regulation (EU) 2016/679, Organic Act 3/2018, fundamental rights, principles, lawfulness of processing, rights, controller, data protection officer, infringements and penalties.

1 INTRODUCIÓN

A protección de datos converteuse nun elemento esencial para o axeitado funcionamento social e político. Emerxe como unha resposta xurídica fronte ao imparable avance do mundo dixital e de todos os problemas que este pode orixinar na vida das persoas. A Sociedade da Información transita agora por un segundo momento, amplificada pola hiperglobalización e redefinida polas tecnoloxías disruptivas que se están a construír na actualidade. Nunca como ata este momento os dereitos conectados coa privacidade estiveron tan expostos.

Como sostivemos, a finalidade do dereito en sentido obxectivo, consistente en regular a vida en sociedade, exixe realizar actualizacións e reformas cando a evolución social así o determine. Só deste xeito as normas xurídicas se manterán eficaces. A materia de protección de datos é un exemplo paradigmático desta idea[1]. En efecto, os avances tecnolóxicos de hai cincuenta anos deron lugar a que os sistemas xurídicos reaccionasen e asentasen a inicial regulación específica de protección de datos. Un pouco despois foise conformando a Sociedade da Información, que grazas á dixitalización foi capaz de procesar de forma masiva e eficaz datos de todo tipo. Pero xa entrado o século XXI percibíronse cambios na dita sociedade, en especial na súa segunda década cando a extensión das redes sociais e o desenvolvemento das citadas tecnoloxías disruptivas abocan a ese segundo momento da Sociedade da Información. A xenérica automatización atópase á volta da esquina, e a intelixencia artificial queda á espera de abrir outro período[2].

A Unión Europea percibiu esta situación e nun proceso complexo xerou unha nova normativa de protección de datos por medio do Regulamento 2016/679, do 27 de abril de 2016, relativo á protección das persoas físicas no que respecta ao tratamento de datos persoais e á libre circulación destes datos e polo que se derroga a Directiva 95/46/CE (en diante RXPD, pois xa é común referirse a esta norma como Regulamento xeral de protección de datos)[3]. O 25 de maio de 2018 comezou a aplicarse este regulamento en todo o territorio da Unión. No propio RXPD fálase de que "a rápida evolución tecnolóxica e a globalización formularon novos retos para a protección dos datos persoais" (considerando 6). E no mesmo lugar recoñécese que a tecnoloxía permite usar datos "nunha escala sen precedentes", "a escala mundial". Iso obriga a reforzar o control e a seguridade xurídica (considerando 7).

E en España, en desenvolvemento deste RXPD, ditouse a Lei orgánica 3/2018, do 5 de decembro, de protección de datos e garantía de dereitos dixitais (en diante LOPDGDD). Confórmase así unha especie de tándem normativo que haberá que ter en conta á vez no ámbito da protección de datos no noso país.

O propósito deste traballo é facer un percorrido explicativo dos dez aspectos desta nova regulación que consideramos máis relevantes (serán os puntos do 2 ao 11, ambos os dous incluídos). Polo tanto, non se trata só dunha aproximación descritiva, aínda que, claro está,

achegamos datos desde esa óptica, senón de facer unha abordaxe máis analítica. A atención preferente prestámoslla ao RXPD, como norma de referencia base, aínda que en todo momento tamén atendemos á LOPDGDD. Así mesmo, puntualmente consideramos outra normativa.

2 DEREITO FUNDAMENTAL

A protección de datos configurouse como un dereito fundamental. Iso é o primeiro elemento do noso decálogo neste traballo por posuír especial significación xurídico-política e social. Intégrase así no corpus de dereitos que constitúen a base da orde política e da paz social (art. 10.1 da Constitución española). Os dereitos fundamentais son a clave de bóveda sobre a que se asenta un sistema público e se converten en elementos nucleares da democracia, que non será verdadeiramente tal se non se prevén e garanten con corrección estes dereitos. Conforman deste xeito a raíz epistemolóxica da sociedade e dos poderes públicos. Tamén a protección de datos, que se conecta por esta vía coa propia dignidade da persoa.

O dereito á protección de datos outórgalles a todas as persoas unha potestade de control dos seus datos persoais, entendidos estes como toda información que identifica ou fai identificable unha persoa. Deste modo, empodera a cidadanía no actual contorno cambiante e convulso, onde as capacidades do mundo dixital son quen de tratar datos como nunca se tería imaxinado no pasado. O Tribunal Constitucional español, na súa famosa Sentenza 292/2000, falaba do "dereito a controlar o uso dos datos", que atribúe ao seu titular un "feixe de facultades" consistentes "no poder xurídico de impor a terceiros a realización ou omisión de determinados comportamentos" (fundamento xurídico 5). Desta forma, malia a afinidade co dereito á intimidade, o dereito á protección de datos é diferente, pois teñen distinta función, obxecto e contido.

É importante resaltar esta idea da protección de datos como dereito fundamental, pois non nos atopamos ante un mero principio político ou ético, ou ante unha recomendación de bo goberno. Nin moito menos. Estamos ante un verdadeiro dereito fundamental que presenta por iso un conxunto específico de garantías, as propias dun dereito fundamental[4].

Ao lado das garantías xurídicas, tamén funcionan outros tipos de requirimentos para protexer os dereitos fundamentais. Por unha parte, a cidadanía debe cumprir a legalidade, o que é especialmente intenso no caso dos dereitos fundamentais. E, por outra parte, os responsables públicos asumen un deber adicional de respecto e protección destes dereitos (o art. 26 da Lei 19/2013, do 9 de decembro, de transparencia, acceso á información pública e bo goberno, ao regular os principios de bo goberno, establece que os altos cargos aos que se lles aplican "promoverán o respecto aos dereitos fundamentais e ás liberdades públicas").

Na Unión Europea o dereito á protección de datos está previsto no artigo 8 da Carta de dereitos fundamentais e no artigo 16.1 do Tratado de funcionamento da Unión Europea. En España, pola súa banda, a protección de datos derivou do artigo 18.4 da Constitución grazas á interpretación doutrinal[5] e á xurisprudencia constitucional, sobre todo a través da citada Sentenza do Tribunal Constitucional 292/2000[6].

A Unión Europea confía na protección de datos para que as persoas poidan facer fronte ás novas situacións. Non en van, "o tratamento de datos persoais debe estar concibido para servir á humanidade" (considerando 4 RXPD). Pero a Unión tamén é consciente dos retos cando se afirma que "a magnitude da recollida e do intercambio de datos persoais aumentou de xeito significativo", ademais de que "a tecnoloxía permite que tanto as empresas privadas como as autoridades públicas empreguen datos persoais nunha escala sen precedentes" (considerando

6 RXPD). O dereito fundamental á protección de datos converteuse así nun elemento esencial da convivencia democrática.

A LOPDGDD tamén evidencia as novas circunstancias cando se le, no punto III do seu preámbulo, que "os fluxos transfronteirizos de datos persoais como consecuencia do funcionamento do mercado interior, os retos formulados pola rápida evolución tecnolóxica e a globalización" fixeron que os datos persoais "sexan un recurso fundamental" para a Sociedade da Información".

En fin, como diciamos antes, esta segunda fase da Sociedade da Información, hiperglobalizada e tanxida polas tecnoloxías disruptivas, avanza cara a un futuro diferente que necesita máis que nunca do dereito á protección de datos. Mesmo haberá que sofisticar as categorías e regulacións xurídicas para manter a súa operatividade e para salvagardar a vida privada no escenario que se achega.

Un último apuntamento antes de proseguir. Cómpre ter en conta que non hai dereitos fundamentais absolutos, tampouco o de protección de datos. Pódense limitar cando hai razóns que o xustifican e que están previstas no ordenamento. Esta limitación, dito agora con sinxeleza, debe facerse por un procedemento baseado no principio de proporcionalidade. Do que se trata en moitas ocasións é de equilibrar os conflitos entre dereitos para solucionar casuisticamente os problemas que vaian xurdindo e regular correctamente a sociedade. Así, por exemplo, o encontro entre protección de datos e o dereito de acceso á información pública disciplínase no artigo 15 da citada Lei 19/2013, de transparencia, acceso á información pública e bo goberno.

3 UNIFORMIDADE EUROPEA E RECEPCIÓN EN ESPAÑA

O segundo elemento do noso decálogo é a aposta da Unión Europea por unha norma como é o regulamento (o aludido RXPD[7]), o cal pretende impor unha uniformidade na materia de protección de datos en todo o territorio desa organización. Iso non se conseguira coa norma de referencia anterior, a citada e xa derrogada Directiva 95/46/CE, posiblemente pola súa propia natureza.

Debemos lembrar que a norma europea coñecida como regulamento presenta un alcance xeral, resulta obrigatorio en todos os seus elementos e aplícase directamente en cada Estado membro. Tales características non as ten a directiva[8]. Ou sexa, que o regulamento posibilita unha finalidade homoxeneizadora que non permite a directiva. Nesta orde de cousas, o propio RXPD recoñece as diferenzas no nivel de protección dos datos ao abeiro da Directiva 95/46 (considerando 9). Ademais, sostén que para garantir "un nivel coherente de protección" é necesario un regulamento que proporcione seguridade xurídica e transparencia (considerando 13).

En principio non é necesario que os Estados adopten un acto nacional de transposición dun regulamento europeo. Non obstante, iso pode ser conveniente para gañar en certeza e seguridade xurídica. É o caso do RXPD, que no suposto español reclama unha lexislación nova que depure o ordenamento interno, dado que este posúe previsións que non se acomodan a aquel.

Apunta atinadamente Jiménez Asensio que a derrogación da Directiva 96/45/CE e a súa substitución polo RXPD "non é unha operación normativa menor", senón motivada polo cambio dun contexto (tecnolóxico) en que a nosa vida se está *datificando* (é dicir, revelamos sen querer enormes cantidades de información)[9].

Dada a importancia da materia regulada, a elaboración do RXPD foi complexa e intensa[10]. Iso tradúcese nunha norma extensa, alambicada e confusa en certos lugares. Como sostivemos noutro traballo, o seu carácter sobrecargado "resulta sen ningún xénero de dúbidas unha dificultade

| A&C | ISSN: 1887-0287 | Vol. 13_n. 2_2018 (xulio – decembro 2018) |

hermenéutica"[11]. Tamén chama a atención o elevado número de remisións ao lexislador nacional: máis de cincuenta remisións ao dereito dos Estados, co que o desenvolvemento que comentabamos antes cobra outra xustificación adicional. De igual xeito, os moitos considerandos iniciais, que funcionan como unha sorte de preámbulo (173), realizan unha especie de interpretación auténtica e mesmo proporcionan información adicional e distinta da que consta nos artigos posteriores. Iso denota unha incorrecta técnica lexislativa.

O RXPD é para a Unión Europea un instrumento transcendental para a dita organización, na actualidade e no futuro. Deste modo, afírmase que "este regulamento pretende contribuír á plena realización dun espazo de liberdade, seguridade e xustiza e dunha unión económica, ao progreso económico e social, ao reforzo e á converxencia das economías dentro do mercado interior, así como ao benestar das persoas físicas" (considerando 2 RXPD). Parece depositarse nunha correcta normativa de protección de datos a evolución desta organización, tanto en termos xurídicos como sociais e económicos.

En todo caso, existen distintas materias fóra do RXPD, como veremos no subapartado 11.1 deste traballo, como os da investigación policial e xudicial en virtude da Directiva 2016/680. Esta dualidade de previsións explícase pola necesidade que en Europa se tivo de aumentar a cooperación xudicial e policial, o que levou a unha norma específica como a citada directiva.

A recepción en España do RXPD faise a través da citada LOPDGDD. Considerouse, con bo criterio, que cumpría aprobar unha nova lei orgánica que substituíse a anterior de 1999. Como se le no punto III do preámbulo da LOPDGDD, o principio de seguridade xurídica, por un lado, obriga a integrar o ordenamento europeo dun xeito claro e público, e, por outro, implica a obriga de "eliminar situacións de incerteza derivadas da existencia de normas no dereito nacional incompatibles co europeo". Isto tradúcese na necesidade de eliminar a normativa interna incompatible coa norma europea. Estas razóns fundan a necesidade da LOPDGDD. Non obstante, esta foi máis alá do tema de protección de datos ao abordar a cuestión dos dereitos dixitais. Estamos convencidos de que iso foi unha mala técnica lexislativa, pois deberon aprobarse dúas leis distintas, xa que ambos os dous contidos así o reclamaban. Outra cousa será a transposición da Directiva 2016/680, cando esta se produza.

Sexa como for, o RXPD e a LOPDGDD amósanse hoxe en día como un conxunto normativo sumamente interconectado, con referencias continuas entre ambos os dous textos. É de agardar que este conxunto sexa decisivo no devir social e xurídico, ademais de ser tido moi en conta polos responsables públicos e privados. O éxito da súa aplicación, se se logra, será un avance na convivencia democrática que a todos nos toca construír.

4 NOVO PARADIGMA

O terceiro punto deste decálogo é, nin máis nin menos, o cambio de paradigma no tema de protección de datos.

O anterior modelo era un sistema reactivo que descansaba no control do cumprimento e na inscrición de ficheiros nas axencias *ad hoc*. O novo modelo, en cambio, é de supervisión continua e cotiá, proactivo, que obriga os responsables e encargados de tratamento a adoptar as medidas técnicas e organizativas necesarias para garantir a protección de datos. Para iso deben analizarse os riscos que poden presentarse, antes de que se presenten, e estar xa preparados para a resposta se se produce unha fenda de seguridade. O destacado rol que deben desempeñar as

autoridades de control sitúase na mesma liña. Non se trata de meros cumprimentos formais das obrigas, senón de asumir esta cultura da responsabilidade activa, con lealdade e transparencia.

O entendemento dinámico deste sistema proactivo tradúcese en que as medidas axeitadas deben ser obxecto de revisión e actualización cando sexa necesario (art. 24 RXPD), o que testemuña que as medidas tomadas en certo momento poden anquilosarse e ser inútiles se non se someten a *aggiornamento*.

Esta mutación de modelo fai que a palabra "tratamento" sexa a correcta para reflectir a atención permanente que cómpre articular, pois fai referencia ao presente. Alude ao emprego que os usuarios fan dos datos no dito tempo presente. O reto vai estar en que as organizacións sexan quen de se imbuír da nova mentalidade o máis axiña posible porque manterse en esquemas do pasado vai lastrar a protección de datos de forma inaceptable.

5 PRINCIPIOS

No réxime de protección de datos existe un conxunto de principios que enmarcan todo tratamento. Así os denomina o RXPD, aínda que desde un punto de vista técnico-xurídico non todos sexan realmente principios. Tales previsións, que son o núcleo central do réxime xurídico de protección de datos, deben ser tidas en conta en todo caso.

Deste xeito, no artigo 5 RXPD atopamos os denominados principios de lealdade e transparencia no tratamento de datos; limitación da finalidade (ou sexa, só se recollen datos para fins determinados, explícitos e lexítimos); minimización de datos (só se tratan os datos axeitados e pertinentes en relación cos fins); exactitude dos datos (os datos deben ser exactos, e, se non, hai que actualizalos); limitación do prazo de conservación (non se deben gardar máis do tempo necesario para os fins de tratamento); integridade e confidencialidade (manter a seguridade dos datos); e responsabilidade proactiva (que exemplifica o cambio de modelo visto no apartado anterior).

A LOPDGDD aborda a cuestión no seu título II, titulado "Principios de protección de datos", onde con grande imprecisión xurídica se abordan cousas diversas, como o deber de confidencialidade (que é obviamente un deber, non un principio), consentimento de menores ou datos especiais. Pódese destacar o artigo 4.2 LOPDGDD, que establece que en certos supostos non será imputable ao responsable de tratamento a inexactitude dos datos persoais sempre que adoptase todas as medidas razoables para que se supriman ou rectifiquen. En concreto, cando os obtivese directamente do interesado, ou dun mediador ou intermediario, ou doutro responsable ao exercerse o dereito de portabilidade, ou dun rexistro público.

A lei española tamén precisa que o deber de confidencialidade é complementario dos deberes de segredo profesional e que sempre se manteñen "mesmo cando finalizase a relación do obrigado co responsable" (art. 5.3 LOPDGDD).

6 BASES DE LEXITIMACIÓN

Un elemento relevante da actual regulación europea de protección de datos é a existencia de seis supostos xerais en que será posible tratar datos persoais. Por iso, pódese falar de que tales supostos son as bases que xustifican o tratamento, ou sexa, que o lexitiman. O RXPD refírese a "licitude de tratamento".

Estes casos son un elenco pechado, de maneira que, fóra dos supostos que expresamente permiten o tratamento dos datos, este non estará autorizado, ou sexa, será ilegal (coa excepción

do réxime específico das categorías especiais de datos, ao que nos referiremos *infra*, no apartado 11.2). En virtude do artigo 6.1 do RXPD, as condicións que fan lícito o tratamento son as seguintes:

a) Consentimento: "o interesado deu o seu consentimento para o tratamento dos seus datos persoais para un ou varios fins específicos".

b) Execución dun contrato: "o tratamento é necesario para a execución dun contrato en que o interesado é parte ou para a aplicación a petición deste de medidas precontractuais".

c) Obriga legal: "o tratamento é necesario para o cumprimento dunha obriga legal aplicable ao responsable do tratamento"[12].

d) Urxencia vital: "o tratamento é necesario para protexer intereses vitais do interesado ou doutra persoa física".

e) Interese público: "o tratamento é necesario para o cumprimento dunha misión realizada en interese público ou no exercicio de poderes públicos conferidos ao responsable do tratamento".

f) Intereses lexítimos: "o tratamento é necesario para a satisfacción de intereses lexítimos perseguidos polo responsable do tratamento ou por un terceiro, sempre que sobre os ditos intereses non prevalezan os intereses ou os dereitos e liberdades fundamentais do interesado que requiran a protección de datos persoais, en particular cando o interesado sexa un neno".

A regra xeral do punto f) (interese lexítimo) non se aplica ao tratamento realizado polas autoridades públicas no exercicio das súas funcións. Para elas está destinada a base e), a de interese público. Ambos os dous conceptos, o interese lexítimo e o interese público, requiren concreción para precisar o seu verdadeiro significado, o que se irá obtendo a medida que se vaian aplicando. A LOPDGDD exixe que o cumprimento dunha misión realizada en interese público ou no exercicio de poderes públicos do responsable ten que derivar "dunha competencia atribuída" por unha norma con rango de lei" (art. 8.2 LOPDGDD).

O consentimento é obxecto de previsións adicionais, o que revela que se intentaron superar situacións anteriores disfuncionais. Agora exíxese que o consentimento para autorizar o tratamento de datos debe ser libre, específico, informado e inequívoco, e un acto afirmativo claro (considerando 32 e art. 4.11 RXPD, art. 6.1 LOPDGDD). Trátase de fuxir de situacións confusas do pasado, nas cales as persoas eran literalmente enganadas polas organizacións que solicitaban os seus datos. Acabouse a letra pequena ilexible ou as redaccións incomprensibles. Trátase de apostar pola lealdade dos que solicitan os datos respecto aos interesados. Como afirma o Grupo do Artigo 29, o consentimento só pode ser unha base xurídica axeitada "se se ofrece ao interesado control e unha capacidade real de elección con respecto a se desexa aceptar ou rexeitar as condicións ofrecidas ou rexeitalas sen sufrir prexuízo ningún"[13]. Se existe un importante desaxuste entre os intervenientes nunha recollida de datos, o consentimento pode estar viciado por non ser realmente libre.

Se para o cumprimento dun mesmo fin ou mesmos fins é necesario levar a cabo diversas actividades, o consentimento debe darse para todas esas actividades de tratamento (considerando 32 RXPD). E, por suposto, cando o tratamento teña varios fins, debe darse o consentimento para todos eles (*ibidem*, e igualmente art. 6.2 LOPDGDD). Ou sexa, o consentimento é individualizado ao requirirse para todas as finalidades que se persigan co tratamento.

Así mesmo, "cando o tratamento se basee no consentimento do interesado, o responsable deberá ser capaz de demostrar que aquel consentiu o tratamento dos seus datos persoais" (art. 7.1 e considerando 42 RXPD). Isto obriga os responsables a protocolizar o arquivo dos

consentimentos, aparentemente *sine die*, para lograr cumprir no futuro con esa exixencia de proba de consentimento.

En todo caso, o carácter verdadeiramente informado do consentimento atopa unha destacada dificultade na complexa comprensión dalgúns procesos tecnolóxicos de tratamento. A isto refírese López Calvo ao aludir á adhesión a redes sociais, con cláusulas de privacidade extensas e confusas[14]. A axuda das autoridades de control nesta tesitura móstrase como necesaria, para botar luz nesta escuridade e aconsellar os interesados.

Co novo RXPD hai que entender que xa se exclúe o consentimento tácito[15], que antes era aceptado. En efecto, este regulamento europeo trata de fuxir de situacións escuras e defende nos seus considerandos o consentimento como acto afirmativo "claro" (o mencionado considerando 32 RXPD). Acéptase calquera declaración ou conduta "que indique claramente neste contexto que o interesado acepta a proposta de tratamento dos seus datos persoais". Polo tanto, "o silencio, os recadros xa marcados ou a inacción non deben constituír consentimento".

O consentimento dos menores de idade presenta unhas previsións específicas. É de sobra coñecido como o uso da tecnoloxía dixital polos menores pode presentar riscos para a súa socialización e formación. Certamente, a interacción entre menores e tecnoloxía dixital é problemática, o que se reflicte nos múltiples riscos que se xeran para a súa correcta socialización e formación[16]. Os menores, polas súas características, requiren unha protección adicional no emprego dos seus datos. Como sinala o considerando 38 do RXPD, os nenos "poden ser menos conscientes dos riscos, consecuencias, garantías e dereitos concernentes ao tratamento de datos persoais". O perigo advírtese sobre todo na utilización de datos de menores "con fins de mercadotecnia ou elaboración de perfís de personalidade ou de usuario, e da obtención de datos persoais relativos a nenos cando se utilicen servizos ofrecidos directamente a un neno".

Neste sentido, o artigo 8 do RXPD titúlase "condicións aplicables ao consentimento do neno en relación cos servizos da sociedade da información". Cando estamos no suposto xeral do consentimento para o tratamento de datos (o do citado art. 6.1.a RXPD), "no caso de oferta directa a nenos de servizos da sociedade da información, o tratamento dos datos persoais dun neno considerarase lícito cando teña como mínimo 16 anos". É dicir, se o menor ten 16 anos ou máis pode consentir el por si mesmo. Pode e debe consentir, pois un terceiro, como os pais, non pode substituír ese consentimento. En cambio, "se o neno é menor de 16 anos, tal tratamento unicamente se considerará lícito se o consentimento o deu ou autorizou o titular da patria potestade ou tutela sobre o neno, e só na medida en que se deu ou autorizou". Non obstante, estas previsións están en parte subordinadas á marxe de apreciación nacional, xa que os Estados membros "poderán establecer por lei unha idade inferior a tales fins, sempre que esta non sexa inferior a 13 anos". Amparándose nesta marxe de apreciación nacional que autoriza o regulamento, a LOPDGDD establece a barreira en 14 anos (art. 7.1 LOPDGDD), aínda que quedan a salvo os supostos en que unha lei exixa a asistencia dos titulares da patria potestade para a celebración dun negocio xurídico. Deste xeito, "os titulares da patria potestade poderán exercitar en nome e representación dos menores de catorce anos os dereitos" que veremos no apartado seguinte (art. 12.6 LOPDGDD).

A importancia do tema do consentimento dos menores reclama unha dilixencia adicional para os responsables de tratamento. Ademais, poderase aplicar o dereito de supresión de datos persoais se o interesado, sendo xa adulto, deu o seu consentimento sendo neno e non era plenamente consciente dos riscos que implica o tratamento, en especial en Internet (considerando 65 RXPD).

7 DEREITOS

O dereito fundamental á protección de datos contén dentro de si un grupo de dereitos ou subdereitos que, como tales, lles atribúen outras tantas facultades aos interesados. Pode parecer curiosa esta situación (un dereito que contén dereitos), pero tamén se produce noutros ámbitos (como o dereito á tutela xudicial, que presenta varios dereitos no seu interior).

Estes dereitos concretan o control que os interesados deben ter sobre os seus datos, cun feixe de facultades que, desde o principio de autonomía da vontade, fan posible adoptar diversas decisións para non perder o dito control. Como dicimos, os dereitos exércense se así o decide o seu titular, e como indica a LOPDGDD "directamente ou por medio de representante legal ou voluntario" (art. 12.1 LOPDGDD). Para facilitar estas accións "o responsable de tratamento estará obrigado a informar o afectado sobre os medios á súa disposición para exercer os dereitos que lle corresponden" (art. 12.2 LOPDGDD).

Na configuración tradicional da protección de datos, estes dereitos eran catro, que respondían ao acrónimo ARCO. Tratábase dos dereitos de acceso, rectificación, cancelación e oposición. Co RXPD os dereitos amplíanse. A nova listaxe é a seguinte: dereitos de información, acceso, rectificación, supresión, limitación de tratamento, portabilidade, oposición, e non decisión única, ademais doutros dereitos como os de presentar unha reclamación ante a autoridade de control, ou a tutela xudicial contra unha decisión dunha autoridade de control, ou tamén a tutela xudicial fronte a un responsable ou encargado de tratamento.

A LOPDGDD alude aos "dereitos das persoas" no seu título III, onde se concretan distintas cuestións do seu exercicio. Tamén o artigo 32 LOPDGDD incide no tema de dereitos, ao especificar que cando sexa pertinente a rectificación ou supresión de datos se procederá ao seu bloqueo. De relevancia práctica é a específica previsión da información por capas: a información básica é á que primeiro accederá a persoa interesada, onde se indicará "un enderezo electrónico e outro medio que permita acceder de forma sinxela e inmediata á restante información" (art. 11.1 LOPDGDD).

Todo este conxunto de dereitos fortalece a posición da cidadanía neste tema, que poderá acudir potestativamente a eles para artellar, como dixemos, distintas facultades. Todas estas facultades están garantidas co sistema deseñado para iso e que agora se ve fortalecido pola dureza das sancións, ao que nos referimos máis abaixo.

8 ESTRUTURA INSTITUCIONAL

A correcta articulación da protección de datos exixe certa rede institucional específica. Ímonos referir agora a esta, e non ás estruturas orgánicas que serven para a garantía dos dereitos en xeral (e que xa citamos na nota 4 deste artigo).

Desta forma, o RXPD aposta por determinada estrutura, con distintos suxeitos, aos que dota de relevantes funcións para a boa marcha da protección e xestión do tratamento de datos persoais. Trátase dunha situación en gran parte novidosa con relación ao réxime anterior, que obriga as distintas entidades e organizacións a reformular a súa estrutura para responder ás actuais exixencias.

8.1 Responsable e encargado de tratamento

En primeiro lugar, temos o responsable de tratamento de datos, que é quen determina "os fins e medios do tratamento" (art. 4.7 RXPD). Pode ser unha persoa física ou xurídica, ou un organismo ou servizo. Esta figura é a que asume as principais obrigas na materia, entre as

que destacamos a adopción das medidas técnicas e organizativas para garantir a legalidade do tratamento (art. 24.1 RXPD e art. 28.1 LOPDGDD) e un nivel de seguridade axeitado ao risco (art. 32.1 RXPD).

O encargado de tratamento será quen trate datos persoais "por conta do responsable" anterior (art. 4.8 REDP). Tamén pode ser unha persoa física ou xurídica, ou un organismo ou servizo. Para regular a relación entre ambos os dous, prevese un contrato cun contido detallado no artigo 28.3 RXPD.

O novo modelo de protección de datos de responsabilidade activa exixe que o responsable e o encargado valoren o risco que podería xerar un tratamento e así poder adoptar as medidas pertinentes ante esa situación concreta. Sobre iso volveremos no punto 9 deste traballo.

8.2 Delegado de protección de datos

O delegado de protección de datos é o asesor e fiscalizador na materia de certas organizacións e entidades que tratan datos, en concreto as que se citan no artigo 37.1 RXPD e no 34.1 LOPDGDD (como todas as autoridades públicas, salvo os tribunais). O nomeamento deste delegado correspóndelle ao responsable ou ao encargado de tratamento, o que deberá comunicarse á autoridade de control. A súa posición é de independencia, e non poderá recibir instrucións (art. 38.3 RXPD). Ademais, debe participar en todas as cuestións de protección de datos da organización (art. 38.1 RXPD) e igualmente inspeccionar os procedementos e emitir recomendacións (art. 36.1 LOPDGDD). O delegado é o "interlocutor do responsable ou encargado do tratamento" ante a autoridade de control (art. 36.1 LOPDGDD).

A LOPDGDD, no seu artigo 37, reforza a posición do delegado ao atribuírlle a competencia de recibir e resolver reclamacións de posibles afectados, o que o achega, curiosamente, á natureza dun *ombudsman*. Desta forma, o afectado pode dirixirse ao delegado de protección de datos da entidade contra a que reclame antes de acudir á autoridade de control. O delegado ten dous meses para comunicarlle ao afectado a súa decisión. Así mesmo, a autoridade de control pode remitirlle unha reclamación ao delegado para que responda voluntariamente no prazo dun mes.

Trátase dunha figura inspirada na institución do *compliance* do ámbito mercantil, aínda que adquiriu un crecente protagonismo, quizais excesivo, pois os focos deben caer sobre responsable e encargado, os verdadeiros obrigados para que o sistema actual funcione. En España a súa posición, no caso de órganos públicos, debe cohonestarse coas previsións do Esquema Nacional de Seguridade no ámbito da Administración electrónica, aprobado polo Real decreto 3/2010, do 8 de xaneiro (onde se prevé un responsable de seguridade, ademais dun responsable da información e un responsable de servizos –art. 10–).

8.3 Autoridade de control

Cada Estado debe establecer unha ou varias autoridades públicas independentes para supervisar a aplicación do RXPD (art. 51.1 REDP). A súa finalidade é tanto protexer os dereitos e liberdades das persoas físicas no tratamento de datos como facilitar a libre circulación destes no territorio da Unión Europea. Están dotadas de funcións (art. 57 RXPD) e poderes (art. 58 RXPD) relevantes, entre os que se atopan os poderes correctivos, que inclúen sancións e ordes. A norma europea destaca esa posición de independencia no artigo 52, no cal se fala de "total independencia", de membros "alleos a toda influencia externa" que "non solicitarán nin admitirán ningunha instrución", e de que cada Estado garantirá que cada autoridade de control dispoña "en todo momento dos recursos humanos, técnicos e financeiros, así como dos locais e as infraestruturas necesarios".

En España a autoridade de control nacional é a Axencia Española de Protección de Datos, prevista na LOPDGDD nos artigos 44 e seguintes. Como autoridade administrativa independente, está suxeita á Lei 40/2015, do 1 de outubro, de réxime xurídico do sector público. O deber de colaboración con esta axencia que pesa sobre as administracións públicas e os particulares está recollido no artigo 52 LOPDGDD, precepto que alude a datos, informes, antecedentes e xustificantes necesarios para levar a cabo a actividade e investigación da axencia. Este deber parece imprescindible para levar a bo termo as competencias da axencia.

Ademais, no ámbito autonómico temos órganos deste tipo en Cataluña (Autoridade Catalá de Protección de Datos) e País Vasco (Axencia Vasca de Protección de Datos), e en parte en Andalucía, aínda pendente de desenvolver algunha das súas competencias (Consello de Transparencia e Protección de Datos). A LOPDGDD ampara a existencia destas entidades autonómicas (arts. 57 e ss.), que deberán cooperar coa axencia estatal e intercambiar mutuamente a información necesaria para o cumprimento das súas funcións.

8.4 Comité Europeo de Protección de Datos

O último elo na rede institucional é o Comité Europeo de Protección de Datos (arts. 68 e ss. RXPD), un organismo da Unión Europea que supervisa a aplicación do RXPD e asesora á Comisión europea no tema, ademais de, entre outras cousas, emitir directrices, recomendacións e boas prácticas. Así mesmo, elabora un informe anual que fai público e transmite ao Parlamento Europeo, ao Consello e á Comisión.

No Comité intégranse os directores das autoridades de control dos Estados membros e o Supervisor Europeo de Protección de Datos. Substitúe o coñecido como Grupo de Traballo do Artigo 29 (que funcionaba baseándose na Directiva 95/46/CE, derrogada polo RXPD).

9 XESTIÓN DE ÍNDOLE PREVENTIVA

O modelo actual de protección de datos, como vimos no apartado 4, é proactivo. Iso obriga o responsable a realizar unha serie de labores que poderían cualificarse de preventivos. Do que se trata é de anticiparse aos problemas que poidan xurdir e ás fendas de seguridade. Mellor evitalas que responder despois de que se produzan. O modelo anterior, de control do cumprimento, implicaba actuacións unha vez que o problema xa tivera lugar, para reparalo. Por iso, o paradigma actual, se funciona correctamente, é moito máis plausible.

Neste sentido, citamos tres actuacións que cremos que reflicten ben a idea que queremos transmitir. A primeira é a elaboración do rexistro de actividades de tratamento coas especificacións que se exixen (art. 30 RXPD e art. 31 LOPDGDD). Do que se trata sobre todo é de especificar "as actividades de tratamento levadas a cabo", ou sexa, de que o rexistro sexa un fiel reflexo da realidade do tratamento de datos na organización respectiva. As entidades públicas citadas no artigo 77.1 LOPDGDD deben facer público un inventario das súas actividades de tratamento (art. 31.2 LOPDGDD), o que xa se incorporou como unha obriga de transparencia activa no artigo 6 bis da Lei 19/2013, do 9 de decembro, de transparencia, acceso á información pública e bo goberno (en virtude da disposición derradeira undécima da LOPDGDD). Esta publicación é unha boa noticia para avanzar no principio de transparencia. Ademais, téñase en conta que non levar rexistro de actividades de tratamento é unha infracción grave (art. 73.n LOPDGDD); e que, se o rexistro non incorpora toda a información exixida, estamos ante unha infracción leve (art. 74.l LOPDGDD).

A segunda actuación que exemplifica a xestión preventiva é a realización dunha análise de riscos para determinar as medidas concretas que se deberán articular para evitalos (considerando 83 RXPD: "avaliar os riscos inherentes ao tratamento e aplicar medidas para mitigalos, como o cifrado,"). Como dixemos *supra*, no subapartado 8.1, este labor permitiralle ao responsable e encargado do tratamento aplicar as medidas técnicas e organizativas axeitadas (os xa citados art. 32.1 RXPD e art. 28.1 LOPDGDD). Neste sentido, cómpre ter en conta os "maiores riscos" que poderían producirse nunha serie de supostos que fixa o artigo 28.2 LOPDGDD (como a aparición de situacións de discriminación, usurpación de identidade, fraude, perdas financeiras, dano para a reputación, vulneración do segredo profesional ou reversión non autorizada da pseudonimización; afectación a grupos en situación de especial vulnerabilidade; tratamentos masivos; ou transferencias de datos a terceiros Estados que non contan cun nivel adecuado de protección). Outra vez hai que ter presente, no ámbito do sector público, que o xa citado Esquema Nacional de Seguridade tamén considera, pola súa parte, unha análise e xestión dos riscos (art. 13 do Real decreto 3/2010).

E a terceira obriga de tipo preventivo que recollemos son as denominadas avaliacións de impacto nas operacións de tratamento de datos (art. 35 RXPD). Estas deberán realizarse cando un tratamento entrañe un alto risco para os dereitos e liberdades. En concreto, proceden cando se vai efectuar unha "avaliación sistemática e exhaustiva de aspectos persoais de persoas físicas que se basee nun tratamento automatizado", un tratamento a grande escala de categorías especiais de datos, ou unha "observación sistemática a grande escala dunha zona de acceso público". Para realizar esta avaliación, o responsable solicitará asesoramento do delegado de protección de datos. Se se efectúa o tratamento de datos persoais sen terse realizado a avaliación de impacto nos supostos en que esta é exixible, cometerase unha infracción grave (art. 73.t LOPDGDD).

Estas xestións preventivas, polo tanto, evidencian a concreción do novo paradigma no tratamento de datos e o cambio da lóxica organizacional.

10 INFRACCIÓNS E SANCIÓNS

O dereito, en sentido obxectivo, ten como un dos seus elementos característicos a coactividade, isto é, a posibilidade de ser imposto pola forza. Se as normas xurídicas non se cumpren voluntariamente, o sistema público ten mecanismos de imposición. Esta idea é de suma relevancia no campo dos dereitos fundamentais, pois de pouco serve o seu recoñecemento teórico se despois non se establecen medios e fórmulas para garantir a súa aplicación. As garantías dos dereitos son unha exixencia da técnica xurídica e tamén da propia calidade da democracia. É máis, os instrumentos de garantía téñense que actualizar cando corresponda para que as novas situacións non afecten negativamente á aplicación dos dereitos.

O dereito á protección de datos ten, como mencionamos *supra*, as garantías dos dereitos fundamentais en xeral. Pero, ademais, o RXPD e a LOPDGDD aluden a unhas infraccións e sancións concretas ante as vulneracións da protección de datos. Isto supón un endurecemento do sistema de sancións dado o elevadas que poden resultar agora as multas. Así, fálase no seu nivel máximo de multas administrativas de 20 millóns de euros ou do 4 % do volume de negocio total anual dunha empresa, "optándose pola de maior contía" (art. 83.5 RXPD).

A LOPDGDD aborda o procedemento a seguir ante unha vulneración de protección de datos (arts. 63 e ss.) e o réxime sancionador, tanto no que atinxe a suxeitos responsables como a infraccións e sancións (arts. 70 e ss.). Descríbense as condutas típicas e gradúanse as infraccións

entre moi graves, graves e leves, gradación que se fai para determinar os prazos de prescrición. De igual xeito, fíxase a interrupción da dita prescrición (art. 75 LOPDGDD).

Neste sentido, é de salientar que os responsables de órganos públicos non serán sancionados economicamente, senón que se castigarán a través de apercibimentos, actuacións disciplinarias ou amoestacións, aínda que todo iso con publicidade e con aviso ao Defensor do Pobo ou aos defensores autonómicos (art. 77 LOPDGDD). Polo tanto, nestes supostos substitúense as multas pola publicitación do infractor, o que en determinados casos pode ser unha técnica de prevención de infraccións moi eficaz. Malia iso, hai quen considera que este réxime especial é un privilexio do sector público, co que non estamos de acordo.

11 UNHA REGULACIÓN COMPLEXA

Un dos trazos que se poderían considerar característicos da protección de datos é o da súa heteroxeneidade e complexidade. É o último elemento do noso decálogo. As causas desta complexidade centrámolas en tres: a habitual existencia de excepcións ás previsións xerais, a previsión de ámbitos excluídos e de regulacións específicas, e o que podemos cualificar como sectores regulados de xeito máis flexible.

11.1 Materias excluídas e regulacións específicas

En primeiro lugar, hai que ter presente o ámbito de aplicación material da normativa. Neste sentido, o RXPD, no seu artigo 2.2, indica que non se aplica a actividades non comprendidas no dereito da Unión, á política exterior e de seguridade común da Unión, e ás actividades exclusivamente persoais ou domésticas.

Non obstante, nunha mostra de mala sistemática, noutros lugares o RXPD tamén aborda cuestións referidas ao seu ámbito a aplicación. Así, o RXPD non se aplica aos datos persoais das persoas falecidas segundo interpretan os seus considerandos (considerandos 27, 158 e 160); nin ás persoas xurídicas (considerando 14, aínda que isto tamén se pode interpretar polo propio enunciado do RXPD); no tratamento de datos nas institucións, órganos e organismos da Unión Europea aplícase a normativa específica dese ámbito, que debe adaptarse ao novo réxime (art. 98 RXPD)[17]; tampouco se aplica o RXPD en tratamentos obxecto da citada Directiva (UE) 2016/680 (considerando 19 RXPD)[18]; con relación ás comunicacións electrónicas, aplícase prioritariamente a Directiva 2002/58/CE, e o RXPD de forma supletoria sen impor obrigas adicionais (art. 95 RXPD e considerando 173)[19]; e respecto ao comercio electrónico tamén se aplica prioritariamente a Directiva 2000/31/CE[20] (considerando 21 RXPD).

Pola súa banda, a LOPDGDD non é de aplicación aos tres supostos anteriores do citado artigo 2.2 RXPD e, ademais, aos tratamentos de persoas falecidas[21] (o que xa interpretaban os considerandos vistos do RXPD) e aos tratamentos sometidos á normativa de materias clasificadas (art. 2.2 LOPDGDD). A lei española, con relación ás actividades non comprendidas no dereito da Unión, alude a que eses tratamentos se rexerán pola súa lexislación específica, como é o caso do réxime electoral xeral ou o Rexistro Civil (art. 2.3 LOPDGDD). Sorprende que se poñan exemplos na redacción dun artigo dunha lei, pero aí están.

Realmente, nestes elencos citados nos parágrafos anteriores hai dous tipos de supostos. Un, o das materias ás cales non se aplica a protección de datos, que poderiamos cualificar como ámbitos excluídos. Trátase, por exemplo, das actividades persoais ou domésticas e dos tratamentos de persoas falecidas. E os outros supostos son os que se rexen polas súas disposicións específicas, como o caso das institucións europeas ou as actividades non comprendidas no dereito da UE.

Neste segundo tipo temos supostos en que se aplica a norma específica e non o RXPD (como en investigación policial) e outros en que o RXPD entra como norma de aplicación supletoria (como en comercio electrónico ou en comunicacións electrónicas).

Un suposto con características propias é o ámbito xudicial. Aínda que o regulamento europeo se aplica ás actividades dos tribunais, as autoridades de control non son competentes para supervisar as operacións de tratamento "efectuadas polos tribunais no exercicio da súa función xudicial" (considerando 20 e art. 55.3 RXPD). O control de tales tratamentos depende dos órganos aos que se lles atribúa esa competencia dentro do sistema xudicial (no caso español o Consello Xeral do Poder Xudicial, como así o establece o artigo 236 *nonies* da Lei orgánica 6/1985, do 1 de xullo, do poder xudicial).

11.2 Excepcións

Neste subapartado estámonos a referir a situacións en que existe unha regulación xeral que se acompaña dunha previsión que se aparta dela. Loxicamente, agora non podemos facer un repaso por todas estas excepcións ás disposicións xerais que están previstas na normativa de protección de datos. Aludimos tan só a tres exemplos que cremos que ilustran perfectamente a cuestión.

O primeiro exemplo xa o vimos antes: o consentimento de menores, que pode entenderse como unha excepción ás previsións xerais da categoría do consentimento. Remitimos ao apartado 6 deste traballo.

Nas transferencias de datos persoais a países terceiros ou organizacións internacionais, regúlanse excepcións para situacións específicas (art. 49 RXPD). Desta forma, en ausencia dunha decisión de adecuación ou de garantías axeitadas, poderase realizar unha transferencia de datos persoais se é de aplicación algunha das sete excepcións que enumera tal precepto (como consentimento explícito, execución dun contrato ou razóns de interese públicos).

De igual forma, o tratamento dos chamados datos especiais tamén pode considerarse unha excepción á regulación xeral dos datos (non especiais, polo tanto). Os datos especiais, que son a evolución do que antes en castelán se chamaban datos especialmente protexidos, refírense a catro tipos de datos (art. 9.1 RXPD): os de orixe étnica ou racial; as opinións políticas, as convicción relixiosas ou filosóficas, ou a afiliación sindical; o tratamento de datos xenéticos, datos biométricos dirixidos a identificar de xeito unívoco unha persoa física, e datos relativos á saúde; e datos sobre a vida sexual ou a orientación sexual dunha persoa física. Como indica a norma europea, os datos especiais son "particularmente sensibles en relación cos dereitos e liberdades fundamentais, xa que o contexto do seu tratamento podería entrañar importantes riscos" para estes dereitos e liberdades (considerando 51 RXPD).

Así as cousas, o artigo 9.1 do RXPD establece a prohibición xenérica de tratar os datos especiais, aínda que iso presenta dez excepcións (art. 9.2 REDP). Dunha forma sintética, estas excepcións son o consentimento explícito do interesado[22]; o cumprimento de obrigas do responsable no ámbito laboral; a protección de intereses vitais do interesado; tratamento dunha entidade política ou relixiosa respecto aos seus membros; datos que "o interesado fixo manifestamente públicos"; tratamento necesario para as actuacións xudiciais; razóns dun "interese público esencial"; fins de medicina preventiva ou laboral; saúde pública ou garantía da calidade da asistencia sanitaria; e fins de arquivo en interese público, fins de investigación científica ou histórica ou fins estatísticos.

O consentimento que se exixe neste caso dos datos especiais, como acabamos de dicir, é "explícito"[23], o que supón un paso máis con relación ao consentimento inequívoco que comentamos

nas regras xerais no apartado 6 deste traballo. Polo tanto, ante tratamento de datos non especiais hai que interpretar que cabe un consentimento implícito (pois o explícito só se cita para os datos especiais), que en todo caso será inequívoco, específico e claro, como reclama o propio concepto de consentimento que en todo caso manexa o RXPD (ou sexa, non tácito).

11.3 Ámbitos flexibilizados

Nomeamos así esta subepígrafe para aludir a un conxunto de sectores que presentan previsións máis flexibles. Poderían ser tamén excepcións á regulación xeral, que acabamos de ver, pero para gañar forza explicativa considerámolos á marxe.

O RXPD dedícalle o capítulo IX ao que titula como "Disposicións relativas a situacións específicas de tratamento". Isto refírese a certos tratamentos concretos que por iso necesitan unha previsión *ad hoc*. Nese lugar contémplanse tres supostos en que as previsións son menos ríxidas: a conciliación da protección de datos coa liberdade de expresión e información (art. 85 RXPD); o tratamento para fins de arquivo en interese público, fins de investigación científica ou histórica ou fins estatísticos (art. 89 RXPD); e a protección de datos nas igrexas e asociacións relixiosas (art. 91 RXPD)[24].

12 CONCLUSIÓNS

Tras o decálogo exposto, cremos que queda reflectida a importancia que posúe na actualidade a protección de datos, como garantía fronte ao avance irresistible da Sociedade da Información, e a propia complexidade dese sector do ordenamento, con regulacións detalladas, exclusións e previsións específicas en varios ámbitos, quizais excesivas e sobrecargadas.

A nova normativa concretou máis aspectos, cambiou o modelo e endureceu algunhas previsións (como nos requisitos do consentimento e nas posibles sancións). Búscase con todo iso superar problemas do pasado e protexer de forma efectiva a cidadanía fronte ás grandes corporacións e entidades. As ideas de lealdade e transparencia retratan ben a nova situación que se persegue, con obrigas concretas para responsables e encargados de tratamento nese sentido, e con accións proactivas que deberían evitar problemas futuros ou, se estes se producen, asegurar unha resposta axeitada.

De todos os xeitos, temos certas reservas sobre o éxito real da normativa que regula a protección de datos. Unha infinidade de escándalos que afectan á privacidade das persoas ocupan as primeiras planas dos medios cada certo tempo nos últimos anos. Estes casos rebelan como se comercia cos datos, a súa importancia económica e política, os continuos enganos a que se ve sometida a cidadanía ou a falta de escrúpulos dalgúns dirixentes de grandes empresas. O exemplo de *Cambridge Analytics* vale por todos. E despois están os casos que non saen nos medios, as actuacións secretas de ciberguerra e de intelixencia, que tamén en distintos momentos pivotan arredor de datos persoais.

A ciberseguridade irase progresivamente complicando, co que o escenario para o dereito fundamental da protección de datos se fará máis agresivo. As tecnoloxías disruptivas dificultarán o control dos nosos datos e posiblemente reclamarán unha actualización da normativa que repasamos neste traballo para regular de que xeito robots, máquinas, algoritmos ou a aínda imprevisible computación cuántica poderán, ou non, tratar os nosos datos, un ben precioso da dignidade que cualifica o ser humano. A fortaleza da nosa sociedade e da nosa democracia está en xogo, polo que a forma de aplicar e de evolucionar o réxime de protección de datos será determinante na concreción da nova dinámica social.

13 BIBLIOGRAFÍA

Fernández Rodríguez, J.J. 2004. *Lo público y lo privado en Internet. Intimidad y libertad de expresión en la Red*. México D.F.: Universidad Nacional Autónoma de México. Dispoñible en https://biblio.juridicas.unam.mx/bjv/detalle-libro/1167-lo-publico-y-lo-privado-en-internet-intimidad-y-libertad-de-expresion-en-la-red

Fernández Rodríguez, J.J. 2018. «Aproximación general a la reforma normativa: el reglamento europeo. Principios generales», en C. Campos Acuña (dir.), *Aplicación práctica y adaptación de la protección de datos en el ámbito local*. Madrid: Wolters Kluwer.

Grupo de Traballo do Artigo 29. 2017. *Directrices sobre el consentimiento en el sentido del Reglamento UE 2016/679*. Dispoñible en

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

Jiménez Asensio, R. 2018. «Epílogo», en C. Campos Acuña (dir.), *Aplicación práctica y adaptación de la protección de datos en el ámbito local*. Madrid: Wolters Kluwer.

Lázaro González, I.E.; Mora Prato, N., e Sarzano Volart, C. (coords.) 2012. *Menores y nuevas tecnologías*. Madrid: Tecnos.

López Aguilar, J.F. 2015. «Data Protection Package y Parlamento Europeo», en A. Rallo Lombarte e R. García Mahamut (eds.), *Hacia un nuevo Derecho Europeo de protección de datos*. Valencia: Tirant lo Blanch.

López Álvarez, L.F. 2016. *Protección de datos personales: adaptaciones necesarias al nuevo reglamento europeo*. Madrid: Lefebvre.

López Calvo, J. 2017. *Comentarios al reglamento europeo de protección de datos*. Madrid: Sepin.

Lucas Murillo, P. 1990. *El derecho a la autodeterminación informativa*. Madrid: Tecnos.

PricewaterhouseCoopers LLP. 2018. *Will robots really steal our jobs? An international analysis of the potential long term impact of automation*, dispoñible en

https://www.pwc.com/hu/hu/kiadvanyok/assets/pdf/impact_of_automation_on_jobs.pdf

NOTAS

1 Fernández Rodríguez, 2018: 33.

2 Entre outros, pode verse o informe de PricewaterhouseCoopers LLP, 2018. Nós xa abordamos e albiscamos esta problemática hai anos (Fernández Rodríguez, 2004) partindo da afectación da liberdade de expresión e do dereito á intimidade.

3 No apartado 11 deste traballo aludimos a outras normas da Unión Europea que se engaden a este RXPD na regulación de nivel secundario europeo na materia.

4 De xeito breve podemos clasificar as garantías dos dereitos en normativas (reserva de lei, respecto ao contido esencial, eficacia inmediata, rixidez constitucional), xurisdicionais (amparo "ordinario", amparo constitucional) e institucionais (Ministerio Fiscal, Defensor do Pobo, defensorías autonómicas).

5 Lucas Murillo, 1990.

6 A primeira lei orgánica española específica foi a 5/1992, do 29 de outubro, de regulación do tratamento automatizado de datos de carácter persoal, que foi substituída pola Lei orgánica 15/1999, do 13 de decembro, de protección de datos de carácter persoal. A LOPDGDD derroga esta lei de 1999 (aínda que permanecen de momento en vigor os artigos 22, 23 e 24 da Lei orgánica 15/1999, en virtude da disposición adicional décima e disposición transitoria cuarta da LOPDGDD).

7 O precedente directo deste RXPD foi a Comunicación da Comisión, do 4 de novembro de 2010, titulada "Un enfoque global da protección dos datos persoais na Unión Europea".

8 A directiva obriga os Estados destinatarios en canto ao resultado. É dicir, sobre estes Estados pesa tal obriga de resultado, pero eles elixen a forma e os medios para alcanzar o dito resultado. Por iso se di que o lexislador nacional debe adoptar un acto de transposición no dereito interno que adapte a lexislación nacional aos obxectivos da directiva. Neste proceso, os Estados teñen certa discrecionalidade, que lles serve para ter en conta as particularidades nacionais.

9 Jiménez Asensio, 2018: 628.

10 López Aguilar, 2015.

11 Fernández Rodríguez, 2018: 54.

12 O artigo 8.1 LOPDGDD prevé que esta obriga legal debe estar prevista nunha norma de dereito da Unión Europea ou nunha "norma con rango de lei".

13 Grupo de Traballo do Artigo 29, 2017: 3.

14 López Calvo, 2017: 131 e ss.

15 Non obstante, defendeuse que este consentimento si cabe, pois considérase compatible cunha conduta clara e afirmativa (*v. gr.*, López Calvo, 2017: 124 –aínda que na p. 129 parece soster outra cousa–). Nós non opinamos así, como tampouco os lexisladores nacionais que están a desenvolver o RXPD: desta forma, en España, no punto V do preámbulo da LOPDGDD dise literalmente que este consentimento da norma europea exclúe "o que se coñecía como consentimento tácito".

16 Unha visión destes problemas, pero tamén das oportunidades, pode verse en Lázaro González *et al.*, 2012.

17 A principal referencia é o Regulamento (UE) 2018/1725 do Parlamento Europeo e do Consello, do 23 de outubro de 2018, relativo á protección das persoas físicas no que respecta ao tratamento de datos persoais polas institucións, órganos e organismos da Unión, e á libre circulación deses datos, e polo que se derrogan o Regulamento (CE) n.º 45/2001 e a Decisión n.º 1247/2002/CE. Este regulamento xa está adaptado ao novo marco.

18 Recordemos que esta Directiva (UE) 2016/680 se refire á protección das persoas físicas no que respecta ao tratamento de datos persoais por parte das autoridades competentes para fins de prevención, investigación, detección ou axuizamento de infraccións penais ou de execución de sancións penais, e á libre circulación dos ditos datos. A través dela derrógase a Decisión marco 2008/977/XAI do Consello. A transposición desta directiva en España está pendente. Tal directiva non só establece normas para protexer as persoas físicas no seu obxecto material, senón que tamén garante a libre circulación de datos persoais na Unión no ámbito da cooperación xudicial en materia penal e no da cooperación policial.

19 Unha previsión similar atópase na disposición adicional undécima da LOPDGDD.

20 Directiva 2000/31/CE, do Parlamento Europeo e do Consello, do 8 de xuño de 2000, relativa a determinados aspectos xurídicos dos servizos da sociedade da información, en particular o comercio electrónico no mercado interior.

21 O artigo 3 LOPDGDD contén previsións específicas sobre os datos de persoas falecidas, relativas ao acceso dos herdeiros ou representantes.

22 O artigo 9.1 LOPDGDD preceptúa con relación a este caso que "o só consentimento do afectado non bastará para levantar a prohibición do tratamento de datos cuxa finalidade principal sexa identificar a súa ideoloxía, afiliación sindical, relixión, orientación sexual, crenzas ou orixe racial ou étnica".

23 Como afirma o Grupo do Traballo do Artigo 29, "o consentimento explícito requírese en determinadas situacións en que existe un grave risco en relación coa protección dos datos e nas cales se considera axeitado que exista un elevado nivel de control" sobre os datos persoais" (Grupo de Traballo do Artigo 29, 2017: 20).

24 En cambio, outras previsións nese lugar do RXPD son máis exixentes con relación á normativa xenérica (polo tanto, non son ámbitos de tratamento flexibilizados): acceso a documentos oficiais, tratamento do número nacional de identificación, tratamento no ámbito laboral, e obrigas de segredo para reforzar os poderes das autoridades de control. Pola súa banda, a LOPDGDD tamén alude a algo similar no seu título IV "Disposicións aplicables a tratamentos concretos", aínda que os casos que cita son como os desta nota, máis exixentes.