Anuario Jurídico y Económico Escurialense, **LVII (2024) 125-156 / ISSN: 1133-3677**

El impacto del caso concreto en la conformación del régimen regulatorio de protección de datos personales

The influence of specific cases on the development of the regulatory framework for personal data protection

Dr. Bernardo ARROYO ABAD
Real Centro Universitario
"Escorial- María Cristina"
San Lorenzo del Escorial

Resumen: Las empresas tecnológicas han sido objeto en los últimos años de un debate acalorado tanto en el ámbito jurídico, como fuera de él, en torno a la responsabilidad en el uso indebido de datos personales de usuarios, constituyendo el caso Cambridge Analítica, un punto de inflexión, al afectar los datos personales de millones de usuarios. Este caso y los que le sucedieron, han aumentado la conciencia pública sobre la importancia de proteger los datos personales y han impulsado la renovación del marco regulatorio en el que se desenvuelven estas compañías a nivel mundial, en términos de mayor exigencia, control y garantía, sin soslayar las particularidades que presentan los sistemas jurídicos de países que responden a parámetros históricos, sociales, económicos o normativos diversos.

Este tema seguirá siendo relevante ya que las nuevas tecnologías transforman rápidamente la realidad que el derecho intenta regular, y el legislador solo puede ofrecer soluciones provisionales.

Palabras clave: Protección de datos, datos personales, nuevas tecnologías, derechos digitales

Abstract: In recent years, technology companies have been the subject of heated debate both within and outside the legal sphere regarding their responsibility for the misuse of users' personal data. The Cambridge Analytica case, which affected the personal data of millions of users, was a turning point in this debate. These cases have increased public awareness about the importance of protecting personal data and have driven the renewal of the regulatory framework for these

companies worldwide, in terms of greater demand, control, and guarantees, while also addressing the particularities of legal systems in countries that respond to diverse historical, social, economic, or normative parameters.

This topic will remain relevant as new technologies rapidly transform the reality that the law seeks to regulate, and lawmakers can only offer provisional solutions.

Keywords: Clue words: Data Protection, personal data, new technologies, digital rights.

Sumario:

Recibido: agosto 2023.
Aceptado: octubre 2023.

I. INTRODUCCIÓN: CONTEXTO DE LA RESPONSABILIDAD DE LAS EMPRESAS TECNOLÓGICAS EN EL USO DE LOS DATOS PERSONALES DE LOS USUARIOS

La tecnología ha transformado profundamente nuestras vidas y ha permitido que las empresas puedan recopilar, almacenar y procesar enormes cantidades de datos personales de los usuarios. Sin embargo, esta capacidad también ha traído problemas en torno a su privacidad y seguridad y ha generado la necesidad de regular el uso que hacen las empresas tecnológicas de esta información.

En el contexto descrito, estas empresas tienen la responsabilidad de garantizar que los datos personales de los usuarios sean tratados de manera justa y segura, y que se respeten los derechos de los usuarios sobre su propia información. En los últimos años, ha habido varios casos importantes en los que las empresas tecnológicas han sido acusadas de no proteger adecuadamente los datos personales de sus usuarios, lo que ha llevado a multas y demandas. Por lo tanto, es esencial que las empresas tecnológicas comprendan su responsabilidad en este ámbito y tomen medidas efectivas para proteger los datos personales de sus usuarios.

Según el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, y la vigente ley de protección de datos española LO 3/2018, la protección de datos personales es un derecho fundamental[1]. Las empresas tecnológicas deben proporcionar a los usuarios información clara y detallada sobre el uso que harán de sus datos personales y obtener su consentimiento para dicho

[1] REGLAMENTO EUROPEO GENERAL DE PROTECCIÓN DE DATOS (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. GARCÍA, A., "Protección de datos personales en la era digital: retos y perspectivas", en *Revista de Derecho y Sociedad*, vol. 2, nº 1 (2019) 27-41: "La Ley Orgánica 3/2018 de Protección de datos personales y garantía de derechos digitales, establece el marco normativo aplicable a la protección de datos en España. De acuerdo con esta Ley, el tratamiento de los datos personales por parte de las empresas tecnológicas debe ajustarse a los principios de licitud, lealtad y transparencia, limitación de la finalidad, minimización de datos, exactitud, integridad y confidencialidad. Además, la ley establece que los titulares de los datos tienen derecho a la protección de su información personal y a su privacidad, así como a la rectificación, oposición y supresión de sus datos en determinadas circunstancias".

uso[2], además de cumplir concretas obligaciones en materia de recopilación, almacenamiento y procesamiento de datos personales[3].

Se debe garantizar la privacidad de estos datos incluso en situaciones de vulnerabilidad de la información[4]. Si una empresa incumple ese deber de protección, será responsable por los daños ocasionados[5]. El tratamiento ilícito de datos implica una violación de la privacidad y un daño a la imagen del titular del dato[6].

Por lo tanto, las empresas tecnológicas deben implementar medidas adecuadas para la protección de los datos personales y promover una cultura de privacidad entre sus empleados y usuarios[7].

La utilización de tecnologías como el "big data" y el "machine learning" para recopilar y analizar grandes cantidades de información personal de los usuarios con el fin de mejorar sus servicios y productos, conllevan innegables riesgos, que afectan precisamente a la privacidad de los usuarios y al uso indebido de sus datos. La protección de datos personales se ha convertido en una exigencia ética y legal para las empresas tecnológicas, quienes deben garantizar la seguridad de la información de los usuarios[8].

En este sentido, la normativa española establece la obligación de las empresas de adoptar medidas técnicas y organizativas para garantizar la seguridad de los datos personales que tratan y evitar su acceso, modificación o destrucción no autorizados[9]. En caso de incumplimiento de estas obligaciones, las empresas pueden ser sancionadas por la Agencia Española de Protección de Datos con

[2] COMISIÓN EUROPEA, "Guía para usuarios: Protección de datos personales", 2020.

[3] ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS, "Directrices de la OCDE sobre privacidad y transparencia", 2016.

[4] CALDERÓN, R., "La responsabilidad civil por el uso de datos personales en la era digital", en *Revista Internacional de Derecho y Tecnología*, vol. 1, nº 2 (2019) 89-104.

[5] PÉREZ, M., "La responsabilidad civil de las empresas tecnológicas por el uso indebido de datos personales", en *Revista de Derecho Digital*, nº 8 (2018) 65-76.

[6] RODRÍGUEZ, F., "La protección de datos personales en la era digital: Retos y desafíos para el derecho", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, vol. 1, nº 1 (2019) 37-54.

[7] PÉREZ, J., "El derecho a la protección de datos en la era digital: Retos y perspectivas", en *Revista de Derecho y Tecnología*, vol. 7, nº 1(2020) 1-17. GARCÍA, A., "Protección de datos personales en la era digital: retos y perspectivas", en *Revista de Derecho y Sociedad*, vol. 2, nº 1 (2021) 27-41.

[8] ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS, "Directrices de la OCDE sobre privacidad y transparencia", 2016.

[9] Ley orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales.

multas de hasta 20 millones de euros o el 4% del volumen de negocio anual global, lo que sea mayor[10].

Así cabe hablar de dos esferas de responsabilidad. La que se mueve en el ámbito estrictamente punitivo por la vulneración de una obligación que lleva aparejada sanción, en la esfera estrictamente de derecho regulatorio, buscándose ejemplaridad y corrección de conductas por contagio a todo el sector, habida cuenta de la importancia de las sanciones y sus efectos en términos reputacionales y de marca y por otro lado, la que se desenvuelve en el ámbito de la responsabilidad civil[11], pudiendo ser esta contractual o extracontractual, requiriéndose en todo caso la existencia de un daño, una relación causal entre la conducta ilícita y este y la ausencia de obligación alguna por parte del perjudicado de soportar el daño[12] así, las empresas tecnológicas pueden ser responsables civilmente por los daños causados a los usuarios como consecuencia del uso indebido de sus datos personales[13].

II. EL IMPACTO DEL CASO CONCRETO EN EL ÁMBITO REGULATORIO

La creciente importancia de la tecnología y el uso masivo de internet han llevado a un aumento significativo en la cantidad de datos personales que se recopilan y procesan en línea, lo que ha dado lugar, a una creciente y fundada preocupación sobre la privacidad y seguridad de los datos personales de los usuarios. Los operadores que manejan ingentes cantidades de datos personales pertenecientes a millones de personas se han visto en el ojo del huracán por el manejo que hacen de esos datos.

La aparición de casos de gran impacto mediático en los que empresas tecnológicas han sido acusadas de utilizar datos personales de sus usuarios sin su consentimiento o de no proteger adecuadamente su privacidad ha llevado a la continua implementación de soluciones jurídicas que han terminado conformando todo un cuerpo de derecho regulatorio en materia de protección de datos. Este derecho se ha desarrollado para garantizar la privacidad y seguridad de los datos personales de los usuarios en línea, así como para establecer las responsabilidades de las empresas tecnológicas en la protección de estos datos, fundamental-

[10] STS de 9 de mayo de 2013, núm. 246/2013.

[11] TORRES, T., "La responsabilidad civil en la protección de datos personales", en *Revista de Derecho Privado*, nº 17 (2013) 147-172.

[12] MORENO, J., "Responsabilidad civil en el tratamiento de datos personales por parte de empresas tecnológicas", en *Actualidad Jurídica Aranzadi*, nº 924 (2021) 1-10.

[13] GARCÍA, A., "Protección de datos personales en la era digital: retos y perspectivas", en *Revista de Derecho y Sociedad*, vol. 2, nº 1 (2019) 21-41.

mente en ámbito de derecho punitivo, por cuanto la responsabilidad civil tiene sus propios parámetros de actuación.

El caso Cambridge Analytica, fue un ejemplo claro de cómo los grandes operadores de datos personales, se sirven de ellos sin el conocimiento y por ende ni el consentimiento de los interesados. La compañía Cambridge Analytica utilizó datos de 50 millones de usuarios de Facebook para crear perfiles psicológicos y utilizarlos con fines políticos, lo que llevó a la revelación pública del caso y la posterior investigación.[14]

El caso, como he dicho, tuvo un gran impacto[15] en la creación de un marco regulatorio más sólido en materia de protección de datos. La Unión Europea implementó el Reglamento General de Protección de Datos (RGPD) en mayo de 2018, que estableció reglas claras sobre cómo las empresas deben recopilar, procesar y almacenar datos personales de los usuarios y sanciones y multas significativas para las empresas infractoras, con notable influencia en la regulación de otros países que quisieron fortalecer la protección de datos personales, pudiendo citar a modo de ejemplo la Ley de Protección de Datos Personales de California (CCPA) en Estados Unidos[16] y la Ley de Protección de Datos Personales en Brasil de 2020, la Australiana o la Canadiense a las que me referiré más adelante.

En 2018 la Comisión Europea sancionó a Google con una multa histórica de 4340 millones de euros por abuso de posición dominante en el mercado, al imponer la Compañía restricciones contractuales a fabricantes de móviles

[14] CADWALLADR, C., & GRAHAM-HARRISON, E., "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach", en The Guardian, 2018: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[15] EUROPEAN PARLIAMENT, General Data Protection Regulation (GDPR), 2018: https://www.europarl.europa.eu/news/en/headlines/society/20180411STO00622/general-data-protection-regulation-gdpr-what-changes-from-25-may.

FEDERAL TRADE COMMISSION, "Facebook agrees to pay $5 billion and implement robust new protections of user information in settlement of data privacy cases", 2019: https://www.ftc.gov/news-events/press-releases/2019/07/facebook-agrees-pay-5-billion-implement-robust-new-protections.

INFORMATION COMMISSIONER´S OFFICE, "ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information", 2018: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/ico-issues-maximum-500-000-fine-to-facebook-for-failing-to-protect-users-personal-information/.

[16] WONG, J. V., "California passes landmark data privacy bill, giving consumers more control over their personal information", The Guardian, 2019: https://www.theguardian.com/technology/2018/jun/28/california-data-privacy-law-consumers-facebook-google.

y tabletas que utilizaban Android como sistema operativo[17]. La Comisión consideró abusivas las condiciones de preinstalación impuestas a los fabricantes de los dispositivos móviles. Decisión que fue respaldada por El Tribunal General de la Unión Europea que rebajó la sanción hasta los 4125 millones de euros al entender que la acción no había llevado a que se reforzara la posición dominante de Google en el mercado de servicios de búsqueda.

Si bien, esta multa no trajo consigo novedades regulatorias en cuanto a la protección de datos o la privacidad de los usuarios, sin embargo, sí incidió en aspectos relativos al abuso de posiciones monopolísticas y el respeto a las normas de competencia[18].

Además, este caso sirvió para reforzar la postura de la Unión Europea en la regulación de las empresas tecnológicas, especialmente en lo que se refiere a la competencia, iniciándose investigaciones sobre las prácticas de empresas como Amazon, Apple y Facebook, antecedente de anuncios sobre la imposición de limitaciones y restricciones a determinados usos de las empresas tecnológicas en lo sucesivo[19].

En 2020 Zoom fue demandado por presuntamente haber compartido información personal de sus usuarios con Facebook sin su consentimiento, lo que generó preocupación en cuanto a la privacidad y la seguridad de la popular plataforma de videoconferencia. Los informes señalaron que Zoom tenía problemas de seguridad que podrían poner en peligro los datos personales y la privacidad de los usuarios. La compañía llegó a un acuerdo de 85 millones de dólares para resolver la demanda colectiva.

Este caso generó notable alarma y una mayor atención en cuanto a la privacidad y la seguridad de las plataformas de videoconferencia, lo que llevó

[17] COMISIÓN EUROPEA (2019). "Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising": https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770. Google/AdSense, T-612/17, Tribunal General de la Unión Europea, 26 de septiembre de 2019. https://curia.europa.eu/juris/liste.jsf?num=T-612/17.

[18] EUROPEAN COMPETITION NETWORK (2019). "Joint statement on the outcome of the Google Search case." https://ec.europa.eu/competition/ecn/201903_joint_statement_google_case_en.pdf.

EUROPEN PARLIAMENT (2019). "European Parliament calls for more effective EU action against monopolies": https://www.europarl.europa.eu/news/en/press-room/20190321IPR32102/european-parliament-calls-for-more-effective-eu-action-against-monopolies.

[19] AGENCIA REUTERS, "EU to study Apple's iPhone and iPad software: sources", 2019: https://www.reuters.com/article/us-eu-apple-antitrust/eu-to-study-apples-iphone-and-ipad-software- sources-idUSKCN1R31Q6.

THE NEW YORK TIMES, "Tech Giants Prepare for a Sweeping E.U. Privacy Law to Take Effect", 2019: https://www.nytimes.com/2018/05/23/technology/eu-gdpr-privacy-law.html.

a una serie de actualizaciones y nuevas regulaciones de privacidad de datos en todo el mundo, así, la Ley CARES en Estados Unidos (Coronavirus Aid, Relief, and Economic Security Act) incluyó una sección que exige que las videoconferencias utilizadas para la telesalud han de cumplir requisitos de privacidad y seguridad[20]. En la Unión Europea, la Autoridad Europea de Protección de Datos (AEPD) publicó una declaración en la que se destacaba la importancia de cumplir con la legislación europea de protección de datos en la utilización de herramientas de videoconferencia como Zoom[21]. En el Reino Unido, el organismo regulador de privacidad (ICO) publicó una guía sobre cómo mantener la privacidad y seguridad en las videoconferencias, destacando la importancia de utilizar herramientas seguras y cumplir con la legislación de protección de datos[22]. En Canadá, la Oficina del Comisionado de Privacidad de Canadá emitió una declaración instando a las empresas a cumplir con la legislación de protección de datos al utilizar herramientas de videoconferencia[23]. En Australia, la Comisión de Protección de Datos emitió una guía que proporciona consejos prácticos para la privacidad y seguridad en las videoconferencias[24].

III. LAS PECULIARIDADES DEL SISTEMA NORTEAMERICANO

Existen varias razones por las que la regulación en materia de protección de datos en Estados Unidos es más benigna que en Europa. Algunas de estas razones incluyen:

1. Diferencias culturales: Históricamente, la cultura de Estados Unidos ha valorado más la libertad individual, la autodeterminación y el libre mercado que la privacidad personal. Lo que no quiere decir que la privacidad individual

[20] U.S. CONGRESS, Coronavirus Aid, Relief, and Economic Security Act (CARES Act). U.S. Government Publishing Office, 2020:
https://www.congress.gov/bill/116th-congress/house-bill/748/text.

[21] EUROPEN DATA PROTECTION BOARD, "Statement on the processing of personal data in the context of the COVID-19 outbreak", 2020:
https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf.

[22] INFORMATION COMMISSIONER´S OFFICE, Data protection and coronavirus: what you need to know, 2020:
https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/data-protection-and-coronavirus/.

[23] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, "Advice for video-conferencing apps and services", 2020:
https://www.priv.gc.ca/en/privacy-topics/technology/videoconferencing-apps-and-services/.

[24] OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER, Videoconferencing security tips. Office of the Australian Information Commissioner, 2020:
https://www.oaic.gov.au/privacy/guidance-and-advice/videoconferencing-security-tips/.

no se proteja o valore, sino que existe una tensión constante entre la libertad individual y la privacidad, ya que el equilibrio entre ambas varía según el contexto y la situación concreta sometida a valoración de juez. En Europa la privacidad es un derecho fundamental que ha sido protegido por la ley durante décadas, así como la protección de datos personales[25].

La primacía de la privacidad pivota normalmente sobre aspectos de seguridad jurídica como es el caso Carpenter v. Estados Unidos (2018)[26], en el que el Tribunal Supremo de EE.UU. se pronunció sobre la recopilación de datos de ubicación por parte de la policía sin una orden judicial. El tribunal determinó que la recopilación de esta información constituía una búsqueda y una incautación, lo que requería una orden judicial. Esta decisión refleja la importancia que en EE.UU. se da a la protección de la privacidad individual.

Circunstancia similar es la que recoge el caso Facebook, Inc. v. Power Ventures, Inc. (2016)[27], en el que se discutió sobre el derecho de propiedad y el control de la información personal. En concreto si el uso no autorizado de información de usuarios de Facebook por parte de una aplicación de terceros violaba la Ley de Fraude y Abuso Informático de EE.UU. El tribunal decidió que la empresa de terceros había violado la ley.

En el caso United States v. Warshak (2010)[28], el tema era si el acceso del gobierno a los correos electrónicos de una persona violaba la Cuarta Enmienda de la Constitución de EE.UU. El tribunal decidió que las personas tienen una expectativa razonable de privacidad en sus correos electrónicos y que, por lo tanto, el acceso sin una orden judicial violaba la Cuarta Enmienda.

En el caso de Facebook v. Power Ventures (2016), un juez federal dictaminó que la empresa Power Ventures había violado los términos de servicio de Facebook al acceder a los datos de los usuarios de la red social sin su consentimiento. Aunque los usuarios habían otorgado permiso a Power Ventures para acceder a sus perfiles de Facebook en el pasado, Facebook cambió sus políticas y prohibió a los desarrolladores de terceros acceder a los datos de los usuarios sin su

[25] NISEENBAUM, H., "Privacy in context: Technology, policy, and the integrity of social life", Stanford University Press 2020. SOLOVE, D. J., "Understanding privacy", Harvard University Press, 2008:

[26] CORTE SUPREMA NORTEAMERICANA. Caso: Carpenter v. United States, 585 U.S. ___ , 2018: https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf.

[27] CORTE SUPREMA NORTEAMERICANA. Caso: Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058 (9th Cir. 2016): https://cdn.ca9.uscourts.gov/datastore/opinions/2016/07/12/13-17154.pdf.

[28] CORTE SUPREMA NORTEAMERICANA. Caso: United States v. Warshak, 631 F.3d 266 (6th Cir. 2010). https://law.resource.org/pub/us/case/reporter/F3/631/631.F3d.266.08-3997.pdf.

consentimiento expreso. El juez determinó que Power Ventures había violado estos términos y no podía seguir accediendo a los datos de los usuarios de Facebook.

En cambio en los siguientes casos la libertad individual se impone al derecho de privacidad, normalmente en el ámbito comercial:

En el caso de Spokeo, Inc. v. Robins (2016)[29], la Corte Suprema de EE.UU. dictaminó que un individuo no puede demandar a una empresa por violación de su privacidad si no puede demostrar un daño real o concreto. En este caso, la empresa Spokeo había publicado información incorrecta sobre el demandante en su sitio web, pero la corte determinó que esto no era suficiente para justificar una demanda por daños y perjuicios.

En el caso de In re Nickelodeon Consumer Privacy Litigation (2016)[30], la Corte de Apelaciones del Noveno Circuito de EE.UU. dictaminó que la empresa Nickelodeon no había violado las leyes de privacidad infantil al recopilar información de los niños a través de su sitio web sin el consentimiento de sus padres. Los demandantes argumentaron que Nickelodeon había utilizado tecnologías de seguimiento para recopilar información de identificación personal (PII) de los niños, pero la corte determinó que esta información no era lo suficientemente sensible como para justificar una violación de privacidad.

En el caso United States v. Microsoft (2018)[31], la Corte Suprema de los Estados Unidos abordó la cuestión de si las empresas estadounidenses están obligadas a proporcionar datos almacenados en servidores en el extranjero al gobierno de EE. UU. en virtud de una orden de registro. La corte dictaminó que la Ley de Privacidad de las Comunicaciones Electrónicas no otorga a los tribunales de EE. UU. la autoridad para emitir órdenes de registro que exigen la producción de datos almacenados en el extranjero.

Por lo que respecta al caso In re Google Inc. Cookie Placement Consumer Privacy Litigation (2020)[32]: la Corte de Apelaciones del Noveno Circuito de Estados Unidos sostuvo que Google no había violado la ley de privacidad de

[29] CORTE SUPREMA NORTEAMERICANA. Caso: Spokeo, Inc. v. Robins, 578 U.S. ___ , 2016: https://www.supremecourt.gov/opinions/15pdf/13-1339_5h26.pdf.

[30] CORTE SUPREMA NORTEAMERICANA. Caso: In re Nickelodeon Consumer Privacy Litigation, 827 F.3d 262 (3d Cir. 2016): https://www2.ca3.uscourts.gov/opinarch/141368p.pdf.

[31] CORTE SUPREMA NORTEAMERICANA. Caso: United States v. Microsoft Corp., 584 U.S. ___, 2018: https://www.supremecourt.gov/opinions/17pdf/17-2_6j37.pdf.

[32] CORTE SUPREMA NORTEAMERICANA. Caso: In re Google Inc. Cookie Placement Consumer Privacy Litigation, 964 F.3d 1020 (9th Cir. 2020): https://cdn.ca9.uscourts.gov/datastore/opinions/2020/03/27/17-16278.pdf.

California al colocar cookies en los navegadores de los usuarios sin su consentimiento explícito. La Corte argumentó que la recopilación de datos de navegación sin consentimiento no constituye una interceptación electrónica prohibida por la ley de privacidad de California. Posición que difiere de la europea al exigir el consentimiento explícito del usuario para la recopilación de datos.

También podemos citar el cercano caso Facebook, Inc. v. Duguid (2021)[33]: En el caso Facebook Duguid, el Tribunal Supremo de los Estados Unidos abordó la interpretación del alcance de la Ley de Protección de la Privacidad de las Comunicaciones Electrónicas (ECPA). En su decisión, el tribunal adoptó una interpretación formalista de la ECPA que difería de la interpretación basada en principios de privacidad utilizada en la Unión Europea. En concreto determinó que un mensaje de texto enviado por una empresa no es un "sistema telefónico automático" y, por lo tanto, no está cubierto por la Ley de Protección al Consumidor de Llamadas Telefónicas.

En concreto, el tribunal sostuvo que la ECPA debía ser interpretada literalmente y que no permitía la interpretación basada en principios de privacidad, como la utilizada en Europa. Esta decisión refleja la tendencia de los tribunales estadounidenses a adoptar una interpretación más formalista de las leyes en materia de privacidad y a confiar en la literalidad del texto de las leyes, mientras que en Europa se tiende a adoptar una interpretación más amplia basada en principios de privacidad.

2. Estructura legal diferente: Mientras que Europa tiene una regulación de privacidad coherente y uniforme en el Reglamento General de Protección de Datos (RGPD), Estados Unidos se rige en materia de privacidad por una serie de leyes estatales y federales que a menudo son inconsistentes y dan una visión fragmentada de la regulación en el país, que dispone de un sistema de derecho común, basado en la jurisprudencia, mientras que los países europeos integrantes de la Unión tienen sistemas de derecho civil basados en códigos legales y legislación estatal en materia de protección de datos que son fiel trasunto del RGPD europeo[34].

Podemos citar a modo de ejemplo como incoherencias dentro del fragmentado sistema norteamericano, que crean un panorama complejo para las empresas

[33] CORTE SUPREMA NORTEAMERICANA. Caso: Facebook, Inc. v. Duguid, 593 U.S. ___, 2021: https://www.supremecourt.gov/opinions/20pdf/19-511_gfbh.pdf.

[34] SCHWARTZ, P. M., & SOLOVE D. J., "Privacy, data protection, and cybersecurity in Europe and the United States", en *Columbia Business Law Review*, 1(1) (2011) 130-192. GREENLEAF, G. W. & WATERS, N., *Global data privacy laws*, Edward Elgar Publishing, 2018.

que operan en varios estados o para los consumidores que desean proteger sus datos personales en diferentes lugares, las siguientes[35]:

a. Mientras que la CCPA establece que las empresas deben proporcionar información sobre los datos personales que recopilan y venden a terceros, la Ley de Protección de Datos del Estado de Maine prohíbe a las empresas vender datos personales de los residentes del estado sin su consentimiento explícito.

b. La Ley de Protección de Datos de Virginia establece que las empresas deben proporcionar a los residentes del estado acceso a sus datos personales, así como la opción de corregir y eliminar dichos datos. En cambio, la Ley de Protección de Datos de Florida no proporciona tales derechos a los residentes del estado.

c. La Ley de Protección de Datos de Vermont establece que las empresas deben proporcionar a los residentes del estado acceso a sus datos

[35] Ley de Privacidad del Consumidor de California: California Consumer Privacy Act (CCPA) (2018). https://oag.ca.gov/privacy/ccpa.

Ley de Protección de Datos del Estado de Maine: An Act to Protect the Privacy of Online Consumer Information, 2019:

https://legislature.maine.gov/legis/bills/getPDF.asp?paper=SP0007&item=1&snum=129.

Ley de Protección de Datos del Estado de Virginia: Virginia Consumer Data Protection Act, 2021: https://lis.virginia.gov/cgi-bin/legp604.exe?211+sum+SB1392.

Ley de Protección de Datos del Estado de Florida: Florida Information Protection Act, 2014: https://www.flsenate.gov/Laws/Statutes/2014/501.171.

Ley de Protección de Datos del Estado de Vermont: Act 171: An Act Relating to Data Brokers and Consumer Protection, 2018:

https://legislature.vermont.gov/assets/Documents/2018/Docs/ACTS/ACT171/ACT171%20As%20Enacted.pdf.

Ley de Protección de Datos del Estado de Oklahoma: Oklahoma Personal Data Protection Act, 2010:

https://www.ok.gov/oag/documents/Oklahoma%20Personal%20Data%20Protection%20Act.pdf.

Ley de Privacidad del Consumidor de California: California Consumer Privacy Act (CCPA), 2018: https://oag.ca.gov/privacy/ccpa.

Ley de Protección de Datos del Estado de Texas: Texas Identity Theft Enforcement and Protection Act, 2005: https://statutes.capitol.texas.gov/Docs/BC/htm/BC.521.htm.

Ley de Protección de Datos del Estado de Nueva York: New York State SHIELD Act, 2019: https://www.nysenate.gov/legislation/bills/2019/s5575.

Ley de Protección de Datos del Estado de Carolina del Norte: North Carolina Identity Theft Protection Act, 2005:

https://www.ncleg.gov/EnactedLegislation/Statutes/PDF/ByArticle/Chapter_75C/Article_2.pdf.

Ley de Protección de Datos del Estado de Illinois: Illinois Personal Information Protection Act, 2005: https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2256&ChapterID=64.

Ley de Protección de Datos del Estado de Dakota del Norte: North Dakota Century Code, 2015: https://www.legis.nd.gov/cencode/t51c16.pdf.

personales, así como la opción de corregir y eliminar dichos datos. Por otro lado, la Ley de Protección de Datos de Oklahoma no establece tales derechos para los residentes del estado.

d. La Ley de Protección de Datos del Estado de Colorado establece que las empresas deben notificar a los residentes del estado en caso de una violación de seguridad que comprometa su información personal. Por otro lado, la Ley de Protección de Datos del Estado de Texas no requiere dicha notificación a los residentes.

e. La Ley de Protección de Datos del Estado de Nevada establece que los consumidores tienen el derecho de optar por no participar en la venta de su información personal, mientras que la Ley de Protección de Datos del Estado de Carolina del Sur no proporciona dicha opción a los consumidores.

f. Mientras que la CCPA establece que las empresas deben proporcionar información sobre los datos personales que recopilan y venden a terceros, la Ley de Protección de Datos del Estado de Texas no requiere que las empresas proporcionen tal información a los consumidores.

g. La Ley de Protección de Datos del Estado de Nueva York establece que las empresas deben proporcionar a los residentes del estado acceso a sus datos personales, así como la opción de corregir y eliminar dichos datos. Sin embargo, la Ley de Protección de Datos del Estado de Carolina del Norte no establece tales derechos para los residentes del estado.

h. La Ley de Protección de Datos del Estado de Illinois establece que las empresas deben obtener el consentimiento explícito de los consumidores antes de recopilar y procesar ciertos datos personales. Por otro lado, la Ley de Protección de Datos del Estado de Dakota del Norte no establece requisitos similares para obtener el consentimiento de los consumidores antes de recopilar y procesar datos personales.

3. Influencia corporativa: En Estados Unidos, las empresas tienen una gran influencia en la formulación de políticas públicas, incluyendo la regulación de la privacidad. Las empresas tecnológicas en particular han luchado contra la regulación de la privacidad y han ejercido una gran influencia sobre los legisladores[36].

[36] OBAR, J. A., & OELDORF-HIRSCH, A., "The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services", en Information,

En el caso Equifax de 2017[37], la empresa de informes crediticios sufrió una brecha de seguridad que comprometió los datos personales de más de 147 millones de personas. A pesar de la magnitud del incidente, la empresa no enfrentó consecuencias legales significativas y la Comisión Federal de Comercio no impuso multas importantes. Esto ha llevado a algunas críticas en los medios y por parte de defensores de la privacidad de que la influencia corporativa ha impedido que se tomen medidas más duras contra las empresas que no protegen adecuadamente los datos personales.

En el famosísimo caso de Facebook y Cambridge Analytica de 2018[38], se reveló que la consultora política había utilizado datos personales de usuarios de Facebook sin su consentimiento para influir en las elecciones presidenciales de los Estados Unidos en 2016. Aquí también, a pesar de la magnitud del incidente, Facebook no enfrentó consecuencias legales significativas por parte de la Comisión Federal de Comercio, lo que algunos interpretaron como evidencia de la influencia corporativa en la regulación de la privacidad de los datos personales en los Estados Unidos.

En el caso Google Street View de 2010, se descubrió que los vehículos de Google que tomaban imágenes para el servicio de Google Street View también habían recopilado datos de redes inalámbricas no seguras en todo el mundo.

La Comisión Federal de Comercio no impuso ninguna multa significativa a Google[39]. Se argumentó en medios que esto fue en parte debido a la influencia corporativa y la presión política ejercida por Google.

4. Diferencias políticas: En general, los políticos estadounidenses tienden a favorecer una regulación más ligera y una intervención gubernamental limitada

Communication & Society, 21(9) (2018) 1280-1302. FROOMKIN A. M., "The death of privacy?, en *Stanford Law Review*, 52(5) (2010) 1461-1543.

[37] CORTE SUPREMA NORTEAMERICANA. Caso: In re Equifax Inc. Customer Data Security Breach Litigation, 928 F.3d 690 (11th Cir. 2019):
https://law.justia.com/cases/federal/appellate-courts/ca11/17-15444/17-15444-2019-07-19.html.

[38] OFICINA DEL COMISIONADO DE INFORMACIÓN DEL REINO UNIDO, "Informe final de la Investigación sobre el uso de datos de Facebook por parte de Cambridge Analytica", 2018:
https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf.
COMITÉ SELECTO DE INTELIGENCIA DEL SENADO DE EE.UU., "Infome final sobre Actividades de influencia extranjera en las elecciones de EE. UU", 2016, Volumen 2: Cambridge Analytica y otras cuestiones relacionadas con la privacidad y la seguridad de los datos, 2019: https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

[39] FEDERAL TRADE COMMISSION VS GOOGLE INC., 736 F.3d 1236 (9th Cir. 2013): https://law.justia.com/cases/federal/appellate-courts/ca9/10-60309/10-60309-2013-09-10.html.

en el mercado. En Europa, por otro lado, la protección de la privacidad es vista como una responsabilidad del gobierno y se aplica una regulación más estricta[40].

En 2017, la Corte Suprema de los Estados Unidos dictaminó en el caso "Spokeo v. Robins", al que nos hemos referido en líneas anteriores, que un demandante no puede demandar a una empresa de manera automática por violaciones técnicas de la ley de protección de datos si no puede demostrar que sufrió algún daño real. La sentencia se interpretó como una victoria para las empresas, ya que reducía la cantidad de demandas potenciales.

No obstante lo apuntado, los daños punitivos no gozan de predicamento en Europa salvo en el Reino Unido.

En 2018, la Corte de Apelaciones del Noveno Circuito de los Estados Unidos dictaminó en el caso "ZL Technologies v. LinkedIn"[41] que los sitios web y las empresas de redes sociales no violan la ley de protección de datos al acceder a los datos públicos de los usuarios en línea, como su nombre y su perfil público. La sentencia se interpretó asimismo como una victoria para las empresas de tecnología, ya que les permitía utilizar los datos públicos de los usuarios para mejorar sus productos y servicios sin temor a demandas.

En 2020, la Corte Suprema de los Estados Unidos dictaminó en el caso "Barr v. American Association of Political Consultants"[42] que la Ley de Protección de la Privacidad del Consumidor de Telecomunicaciones de 1991, que prohibía las llamadas automáticas o mensajes de texto a números móviles sin el consentimiento previo del titular, era inconstitucional. De esta forma los partidos políticos podían enviar mensajes de texto automatizados sin tener que obtener el consentimiento previo de los destinatarios.

5. Diferencias históricas: En Europa, la protección de datos surgió como una respuesta a los abusos del poder estatal durante la Segunda Guerra Mundial y la preocupación por la protección de la privacidad de los ciudadanos frente a

[40] BRUNTON, F. & NISSENBAUM, H., "Vernacular resistance to data collection and analysis: A political theory of obfuscation", en *First Monday*, 20(5) (2015). MAYER-SCHÖNBERGER, V. & CUKIER, K., "Big data: A revolution that will transform how we live, work, and think", en *Houghton Mifflin Harcourt*, 2013.

[41] CORTE SUPREMA NORTEAMERICANA. Caso: ZL Technologies vs. LinkedIn Corp. 789 F.3d 1101 (9th Cir. 2015): https://scholar.google.com/scholar_case?case=15973756508800261 00&q=ZL+Technologies+v.+LinkedIn&hl=en&as_sdt=2006.

[42] CORTE SUPREMA NORTEAMERICANA. Caso: Barr. vs. American Association of Political Consultants Inc. 140 S. Ct. 233 5, 2020: https://www.supremecourt.gov/opinions/19pdf/19-631_2c8f.pdf.

los gobiernos y las empresas[43]. En Norteamérica, la protección de datos se ha centrado principalmente en la protección de los derechos de propiedad intelectual y de la competencia, así como en la prevención del fraude[44].

Es importante tener en cuenta que, aunque las leyes de privacidad son más laxas en Estados Unidos que en Europa, esto no significa necesariamente que las empresas estadounidenses tengan menos responsabilidad en la protección de los datos personales de los usuarios. Las empresas pueden enfrentar demandas por incumplimiento de contrato, engaño al consumidor y otras violaciones legales si no protegen adecuadamente los datos personales de los usuarios además hay que significar que estas diferencias no son universales ni se aplican a todos los individuos o empresas en cada país. En ambos lugares existen debates y controversias en torno a la protección de datos y la privacidad, y las regulaciones y su aplicación están en constante evolución.

IV. IMPACTO DE LA REGULACIÓN EUROPEA EN CANADA, AUSTRALIA Y BRASIL

La implementación del Reglamento General de Protección de Datos (RGPD) de la Unión Europea en mayo de 2018 ha tenido un impacto significativo en la forma en que se manejan los datos personales en todo el mundo, incluso en países como Canadá, Australia y Brasil.

En Canadá, el RGPD llevó a la revisión y actualización de la Ley de Protección de Información Personal y Documentos Electrónicos (Ley PIPEDA) en noviembre de 2018. La ley canadiense incorporó disposiciones que se asemejan a las del RGPD, incluyendo la obligación de notificar a los individuos afectados por una violación de datos en un plazo de tiempo determinado. La ley también introdujo una nueva sección que establece que los proveedores de servicios deben contar con el consentimiento explícito de los individuos antes de recopilar, usar o divulgar su información personal[45].

[43] WESTIN, A. F., "Social and political dimensions of privacy", en *Journal of Social Issues*, 59(2) (2003) 431-453. ROTHSTEIN, M. A., "Genetic exceptionalism and legislative pragmatism", en *Hastings Center Report*, 40(1) (2010) 16-19.

[44] ARCHIBUGI, D., y FILIPETTI, A., "Privacy, Security and Data Protection in the European Union and the United States: A Critical Comparison":
https://www.researchgate.net/publication/277903271_Privacy_Security_and_Data_Protection_in_the_European_Union_and_the_United_States_A_Critical_Comparison.

[45] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, The Personal Information Protection and Electronic Documents Act (PIPEDA), 2019:
https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/.

Uno de los casos recientes en Canadá que pone de manifiesto la influencia del derecho europeo es el caso Telus Communications Inc. v. Wellman, de 2019[46]. El Tribunal Supremo de Canadá examinó el alcance de la notificación obligatoria de violaciones de seguridad, en concreto si Telus Communications estuvo obligada a notificar a sus clientes sobre una violación de seguridad de datos que había ocurrido en 2014, en la que se había expuesto información personal de aproximadamente 134.000 clientes.

El tribunal tuvo en cuenta la jurisprudencia europea, especialmente el caso Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (STJUE de 13 de mayo de 2014, asunto C-131/12), que sentó un precedente importante en el ámbito del derecho al olvido en Europa. El tribunal canadiense concluyó que la notificación obligatoria de violaciones de seguridad de datos debería ser interpretada de manera amplia, para garantizar una protección efectiva de los datos personales de los individuos.

El tribunal también señaló que, aunque PIPEDA y el Reglamento General de Protección de Datos (RGPD) de la Unión Europea tienen diferencias significativas, ambos comparten el objetivo de proteger los datos personales de las personas. Por lo tanto, el tribunal decidió que la jurisprudencia europea era relevante en la interpretación de las disposiciones de PIPEDA relacionadas con la notificación de violaciones de seguridad de datos.

En Australia, la Ley de Privacidad de 1988 se actualizó en febrero de 2018 para alinearse con los estándares internacionales de privacidad, incluyendo el RGPD. La nueva ley de privacidad australiana incluyó disposiciones como la definición de "datos personales", la obligación de notificar a los individuos afectados por una violación de datos y la regulación de la transferencia de datos personales a países fuera de Australia. También se estableció un nuevo esquema de informe de violaciones de datos que requiere que las organizaciones notifiquen a la Comisión Australiana de Información y Privacidad sobre cualquier violación de seguridad que tenga el potencial de causar daño grave a los individuos afectados[47].

Uno de los casos más recientes y relevantes en Australia donde se ha puesto de manifiesto la influencia del derecho europeo en protección de datos es el caso de Privacy Commissioner v Facebook Inc (Nº 2) [2020] FCA 1307.

[46] TRIBUNAL SUPREMO DE CANADA,Telus Communications Inc. v. Wellman, 2019: https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/17545/index.do.

[47] OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER, Australian Privacy Act reform, 2018: https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-act-reform/.

En este caso, la Comisionada de Privacidad de Australia presentó una demanda contra Facebook por violaciones a la Ley de Privacidad de Australia, específicamente en relación con la divulgación de datos personales de usuarios a la consultora política Cambridge Analytica. Facebook argumentó que la demanda no podía proceder porque la compañía no tenía presencia física en Australia y que la ley australiana no se aplicaba a ella.

Sin embargo, el tribunal australiano determinó que Facebook sí tenía presencia en Australia y que la ley de privacidad australiana sí se aplicaba a la compañía. En su razonamiento, el tribunal hizo referencia a las disposiciones del RGPD europeo, y señaló que la ley australiana de privacidad estaba alineada con los estándares internacionales de privacidad de datos establecidos por el RGPD. El tribunal también señaló que Facebook había violado la privacidad de los usuarios al permitir que Cambridge Analytica accediera a sus datos personales sin su consentimiento[48].

Este caso resalta la necesidad de una regulación global de protección de datos y la importancia de que los países armonicen sus leyes de protección de datos con los estándares internacionales para proteger efectivamente los derechos de los usuarios.

En Brasil, la Ley General de Protección de Datos (LGPD) entró en vigencia en agosto de 2020, en gran parte debido también al Reglamento Europeo. La LGPD se basa en gran medida en el mismo y establece disposiciones similares, como la obligación de obtener el consentimiento explícito de los individuos antes de recopilar, usar o divulgar su información personal, la obligación de notificar a los individuos afectados por una violación de datos y la regulación de la transferencia de datos personales a países fuera de Brasil[49].

V. EL IMPACTO DE LAS NUEVAS TECNOLOGÍAS EN LA PROFILAXIS DIGITAL

En la profilaxis digital podemos aglutinar el conjunto de medidas preventivas y prácticas de seguridad que se toman para proteger la privacidad y seguridad de los datos digitales a fin de minimizar los riesgos relacionados con la exposición de información personal y la vulnerabilidad a ataques informáticos, fraudes en línea, suplantación de identidad, robo de contraseñas, entre otros riesgos asociados a la era digital.

[48] TRIBUNAL FEDERAL DE AUSTRALIA, Privacy Commissioner v Facebook Inc (No 2) [2020] FCA 1307, 2020: https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2020/2020fca1307.

[49] SENADO FEDERAL DO BRASIL, Lei Geral de Proteção de Dados Pessoais (LGPD), 2018: https://www.senado.gov.br/atividade/rotinas/materia/getPDF.asp?t=223688&tp=1.

Supone la adopción de una serie de hábitos y prácticas como la utilización de contraseñas seguras y complejas, la actualización periódica del software y de las aplicaciones, la activación de la autenticación de dos factores, la utilización de redes VPN para navegar de forma segura y el cifrado de los datos almacenados en dispositivos o en la nube que incluyen la educación y la sensibilización de los usuarios sobre la importancia de proteger su información personal y la adopción de políticas y medidas de privacidad por parte de las empresas y organizaciones que manejan datos de los usuarios.

La inteligencia artificial (IA) y la computación cuántica son tecnologías que van a cambiar con rapidez y de una forma drástica la forma de hacer las cosas en el mundo en que vivimos. En la era digital actual, es fundamental implementar medidas preventivas para proteger la privacidad y seguridad de los datos personales. Sin embargo, la creciente complejidad de las amenazas en línea hace que sea cada vez más difícil abordar una protección eficaz. La IA y la computación cuántica están cambiando el panorama de la seguridad digital, y las medidas que se adopten no solo han de integrar esta nueva tecnología sino proteger el tratamiento de los datos personales de las amenazas que las mismas puedan comportar.

La computación cuántica va a mejorar seguridad y la privacidad de los datos. Por ejemplo, desarrollando algoritmos de cifrado más avanzados que serían extremadamente difíciles de descifrar, permitirá evaluar e identificar rápidamente las vulnerabilidades de seguridad en sistemas y redes, lo que mejorará la seguridad y la privacidad de los datos[50]. La capacidad de las computadoras cuánticas para procesar grandes cantidades de datos en paralelo también facilitará el análisis de grandes conjuntos de datos que permitan obtener información valiosa para la investigación y el desarrollo de nuevas tecnologías[51], pero también para otros fines que pueden poner en riesgo para la privacidad de los usuarios[52].

La posibilidad de hacer cálculos extremadamente rápidos puede amenazar la seguridad de los algoritmos de cifrado actuales cuyas claves podrían ser descifrados

[50] ELKINS, A., "Quantum computing is coming for your data", TechCrunch, 2018: https://techcrunch.com/2018/09/28/quantum-computing-is-coming-for-your-data/.

WEHNER, S. & WILDE, M., "Quantum computing and cryptography", 2018: https://arxiv.org/abs/1801.01465.

[51] HARDESTY, L., "Quantum computers pose a security threat that we're still totally unprepared for", en MIT Technology Review (2018):

https://www.technologyreview.com/2018/07/10/141371/quantum-computers-pose-imminent-threat-to-todays-encryption/.

[52] KRAWCZYK, H., "Post-quantum cryptography: What it is and why we need it", en Communications of the ACM, 64(1), 40-44 (2021):

https://cacm.acm.org/magazines/2021/1/249182-post-quantum-cryptography/fulltext.

fácilmente. Las computadoras cuánticas también podrían ser utilizadas para hackear y obtener acceso no autorizado a sistemas y redes, lo que podría conducir a robos de datos y violaciones de la privacidad[53].

En términos generales, la IA se refiere a la capacidad de las máquinas de realizar tareas que normalmente requerirían inteligencia humana, como el reconocimiento de patrones, la toma de decisiones y el procesamiento del lenguaje natural. En el campo de la profilaxis digital, la IA puede ser utilizada para detectar patrones y comportamientos anómalos en el tráfico de datos y alertar sobre posibles amenazas de seguridad. Además, la IA puede ser programada para aprender de forma autónoma y mejorar tanto su capacidad de detección de amenazas y fraudes como para automatizar tareas de monitorización y análisis de datos. Por otro lado, la IA también puede ayudar a reducir la carga de trabajo de los profesionales de seguridad informática, permitiéndoles centrarse en tareas más complejas y críticas y puede ser utilizada para crear sistemas de seguridad más avanzados y personalizados que se adapten a las necesidades específicas de una empresa o individuo.

Pero también hay riesgos. Uno de ellos es el que supone el sesgo en los algoritmos utilizados en los sistemas de IA. Si los datos utilizados para entrenar el modelo de IA están sesgados, el sistema también puede ser sesgado, lo que puede llevar a decisiones inexactas o discriminatorias. Otro problema es la falta de transparencia en cómo se utilizan los datos recopilados por los sistemas de IA, lo que puede generar preocupaciones de privacidad y falta de control por parte de los usuarios sobre sus datos. Además, la IA no puede reemplazar completamente la necesidad de una gestión adecuada de la seguridad y la privacidad por parte de las empresas y organizaciones, por lo que una excesiva dependencia puede llevar a a una reducción de la capacidad de toma de decisiones humanas, lo que podría tener consecuencias impredecibles en el futuro.[54] Una de las mayores preocupaciones es la posibilidad de que la IA se

[53] NARAYANAN, A. & MANICKAM, P., "The impact of quantum computing on cryptography and data security: A survey", en Journal of Information Privacy and Security, 15(3) (2019) 142-155: https://www.tandfonline.com/doi/abs/10.1080/15536548.2019.1604862.

[54] MITTAL, S.; VATSA, M. & SINGH, R., "Privacy-preserving machine learning for health care data", en *IEEE Transactions on Information Forensics and Security*, 14(3) (2019) 762-777.

YAQOOB, I.; HASHEM, I. A. T.; AHMED, E. & SHOJAFAR, M., "Artificial intelligence-based techniques for cyber security: A comprehensive review", en IEEE *Communications Surveys & Tutorials*, 22(3) (2020) 1549-1597.

WANG, Y. & ZHAO, Z., "A survey on machine learning for Internet of Things security", en *Journal of Network and Computer Applications*, 177 (2021), 102953.

MOHAMMADI, E.; KARIMIPOUR, H. & CHEN, T., "A survey on machine learning for intrusion detection systems", en *Journal of Network and Computer Applications*, 150 (2020), 102498.

vuelva demasiado sofisticada y sea capaz de detectar patrones de comportamiento que violen la privacidad de los usuarios.

La protección de datos personales se ha convertido en un tema crucial en la era digital en la que vivimos. Con el avance acelerado de las nuevas tecnologías como la Inteligencia Artificial (AI) y la computación cuántica, se han creado nuevos retos para la protección de datos. Es fundamental que el legislador se adelante a la previsión de estos problemas y establezca un marco legal sólido que proteja adecuadamente los derechos de los usuarios y consumidores.

El legislador debe actuar con prontitud y no esperar a que surjan casos concretos para poner en evidencia las debilidades del sistema actual. Es crucial que la legislación sea proactiva y no reactiva. Si esperamos a que ocurran problemas para abordarlos, los usuarios y consumidores pueden sufrir daños irreparables. Es necesario evitar que los derechos de los ciudadanos se vean perjudicados antes de que el legislador tome medidas.

Además, los problemas que van a aparecer como resultado de las nuevas tecnologías son comunes y transversales. Es decir, afectan a todos los sectores y áreas, y por tanto, es necesario un análisis conjunto y no fragmentario de los mismos. Solo así se podrán encontrar soluciones completas y efectivas que protejan adecuadamente los derechos de los usuarios y consumidores.

En definitiva, es necesario que el legislador en materia de protección de datos actúe con prontitud y establezca un marco legal sólido que anticipe los problemas que las nuevas tecnologías puedan suponer sobre la protección de datos.

VI. CONCLUSIONES

1. Casos como el de Cambridge Analytica, Zoom y Google han sido fundamentales en la consecución de una mayor conciencia pública sobre la importancia de proteger los datos personales y han impulsado, por su impacto innegable en la multitud de usuarios afectados más allá de cualquier frontera, la conformación de un régimen regulatorio más estricto y garantista respecto de la gestión y protección de los datos de los usuarios por las empresas tecnológicas, con las particularidades que dicha regulación supone en sistemas a priori tan diversos como el norteamericano y el europeo, con el Reglamento Europeo de 2018 como uno de sus exponentes más reseñables, con una capacidad notable de irradiación sobre terceros países.

KUHLMANN, D. & SELZAM T., "Artificial intelligence and privacy", en *Privacy and Cybersecurity Law* in the Digital Age (2020) 315-334. Springer, Cham.

2. Si bien es cierto que los aspectos regulatorios a nivel global presentan un trato cada vez más homogéneo, todavía existen particularidades derivadas del sistema jurídico, político, económico, histórico y social del país cuyos ciudadanos se ven afectados, especialidades que inevitablemente se irán limando, habida cuenta de las exigencias de la propia globalización y de que los intereses económicos cada vez son menos locales o regionales y la movilidad de empresas y ciudadanos cada vez es mayor.

3. Es innegable que la tecnología está en permanente cambio y evolución, y la aparición de nuevas tecnologías como la Inteligencia Artificial o la computación cuántica implica nuevos retos y problemas en materia de protección de datos. Estas tecnologías permiten el procesamiento de grandes cantidades de información en tiempo real y la toma de decisiones cada vez más complejas, lo que aumenta la importancia de proteger la privacidad de los usuarios y garantizar la transparencia y responsabilidad en el uso de sus datos personales. Además, estas nuevas tecnologías plantean cuestiones sobre la seguridad y la privacidad de los datos en un nivel completamente nuevo, lo que requerirá que los reguladores y legisladores estén a la altura de estos desafíos y trabajen para desarrollar soluciones innovadoras y efectivas para abordarlos.

4. Es preocupante que, en materia de protección de datos, como hemos visto, el legislador se muestra pasivo y aguarda a que los avances tecnológicos expongan los datos personales de una multitud de usuarios a riesgos potenciales antes de tomar medidas reguladoras adecuadas que normalmente vienen después de que el problema ha aflorado. En lugar de esperar a que ocurran violaciones de datos y riesgos de seguridad, es deseable una labor profiláctica del legislador anticipándose a los problemas que puedan surgir y establecer medidas de protección sólidas que eviten que estos se produzcan. A menudo las compañías tecnológicas están en una posición privilegiada para utilizar estos avances tecnológicos en su propio beneficio, lo que aumenta aún más la necesidad de que los reguladores estén vigilantes y actúen rápidamente para proteger los derechos de los usuarios.

5. La computación cuántica y la inteligencia artificial (IA) plantean nuevos riesgos en materia de protección de datos que aún no están suficientemente regulados. Por ejemplo, la computación cuántica puede permitir la desencriptación de datos en un tiempo récord, lo que pone en peligro la seguridad de la información y la privacidad de los usuarios. Además, la IA puede generar perfiles extremadamente detallados de los usuarios y sus comportamientos, lo que podría utilizarse para tomar decisiones que afecten a sus derechos y libertades. Estos riesgos son particularmente preocupantes porque las leyes y regulaciones actuales pueden no ser capaces de abordarlos de manera efectiva, ya que la

computación cuántica y la IA son tecnologías emergentes y en constante evolución. Por lo tanto, es necesario que los reguladores presten una atención especial a estos riesgos y trabajen en la creación de marcos legales y reguladores adaptativos y flexibles para proteger la privacidad de los usuarios en un futuro cercano.

VII. BIBLIOGRAFÍA

Libros y revistas:

- BRUNTON, F. & NISSENBAUM, H., "Vernacular resistance to data collection and analysis: A political theory of obfuscation", en *First Monday*, 20(5) (2015).

- CALDERÓN, R., "La responsabilidad civil por el uso de datos personales en la era digital", en *Revista Internacional de Derecho y Tecnología*, vol. 1, nº 2 (2019).

- FROOMKIN A. M., "The death of privacy?", en *Stanford Law Review*, 52(5) (2010).

- GARCÍA, A., "Protección de datos personales en la era digital: retos y perspectivas", en *Revista de Derecho y Sociedad*, vol. 2, nº 1 (2021).

- GREENLEAF, G. W. & WATERS, N., "Global data privacy laws", Edward Elgar Publishing, 2018.

- KUHLMANN, D. & SELZAM T., "Artificial intelligence and privacy", en *Privacy and Cybersecurity Law in the Digital Age* - Springer, Cham 2020.

- MAYER-SCHÖNBERGER, V., & CUKIER, K., "Big data: A revolution that will transform how we live, work, and think", Houghton Mifflin Harcourt 2013.

- MITTAL, S.; VATSA, M. & SINGH, R., "Privacy-preserving machine learning for health care data", en *IEEE Transactions on Information Forensics and Security*, 14(3) (2019) 762-777.

- MOHAMMADI, E.; KARIMIPOUR, H. & CHEN, T., "A survey on machine learning for intrusion detection systems", en *Journal of Network and Computer Applications*, 150 (2020) 102498.

- MORENO, J., "Responsabilidad civil en el tratamiento de datos personales por parte de empresas tecnológicas", en *Actualidad Jurídica Aranzadi,* nº 924 (2021).

- OBAR, J. A. & OELDORF-HIRSCH, A., "The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services", en *Information, Communication & Society*, 21(9) (2018).

- ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS, *Directrices de la OCDE sobre privacidad y transparencia*, 2016.

- PÉREZ, J., "El derecho a la protección de datos en la era digital: Retos y perspectivas", en *Revista de Derecho y Tecnología*, vol. 7, nº, 1 (2020).

- PÉREZ, M., "La responsabilidad civil de las empresas tecnológicas por el uso indebido de datos personales", en *Revista de Derecho Digital*, nº 8 (2018).

- RODRÍGUEZ, F., "La protección de datos personales en la era digital: Retos y desafíos para el derecho", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, vol. 1, nº 1 (2019).

- ROTHSTEIN, M. A., "Genetic exceptionalism and legislative pragmatism", en *Hastings Center Report*, 40(1) (2010).

- SCHWARTZ, P. M., & SOLOVE, D. J., "Privacy, data protection, and cybersecurity in Europe and the United States", en *Columbia Business Law Review*, 1(1) (2011).

- SOLOVE, D. J., *Understanding privacy*, Harvard University Press, 2008.

- TORRES, T. T., "La responsabilidad civil en la protección de datos personales", en *Revista de Derecho Privado*, nº 17 (2013).

- WANG, Y. & ZHAO, Z., "A survey on machine learning for Internet of Things security", en *Journal of Network and Computer Applications*, 177 (2021) 102953

- WESTIN, A. F., "Social and political dimensions of privacy", en *Journal of Social Issues*, 59(2) (2003).

- YAQOOB, I.; HASHEM, I. A. T.; AHMED, E. & SHOJAFAR, M., "Artificial intelligence-based techniques for cyber security: A comprehensive review", en *IEEE Communications Surveys & Tutorials*, 22(3) (2020).

Páginas web consultadas:

- ARCHIBUGI, D. y FILIPETTI, A., "Privacy, Security and Data Protection in the European Union and the United States: A Critical Comparison": https://www.researchgate.net/publication/277903271_Privacy_Security_and_Data_Protection_in_the_European_Union_and_the_United_States_A_Critical_Comparison.

- CADWALLADR, C. & GRAHAM-HARRISON, E., "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach", en *The Guardian*, 2018: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

- CALDERÓN, R., "La responsabilidad civil por el uso de datos personales en la era digital", en *Revista Internacional de Derecho y Tecnología*, vol. 1, nº 2 (2019) 89-104. https://revistas.ucm.es/index.php/IDTE/article/view/64633.

- COMISIÓN EUROPEA, "Guía para usuarios: Protección de datos personales", 2020: https://ec.europa.eu/info/sites/default/files/2019-02/data_protection_for_users_es.pdf.

- COMISIÓN EUROPEA, *Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising*, 2019: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770.

- COMITÉ SELECTO DE INTELIGENCIA DEL SENADO DE EE.UU, "Actividades de influencia extranjera en las elecciones de EE. UU. de 2016", en *Cambridge Analytica y otras cuestiones relacionadas con la privacidad y la seguridad de los datos*, 2019, vol. 2: https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

- CORTE SUPREMA NORTEAMERICANA. Caso Barr v. American Association of Political Consultants, Inc., 140 S. Ct. 2335 (2020): https://www.supremecourt.gov/opinions/19pdf/19-631_2c8f.pdf.

- CORTE SUPREMA NORTEAMERICANA. Caso Carpenter v. United States, 585 U.S. ___ (2018): https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf.

- CORTE SUPREMA NORTEAMERICANA. Caso In re Equifax Inc. Customer Data Security Breach Litigation, 928 F.3d 690 (11th Cir. 2019): https://law.justia.com/cases/federal/appellate-courts/ca11/17-15444/17-15444-2019-07-19.html.

- CORTE SUPREMA NORTEAMERICANA. Caso In re Google Inc. Cookie Placement Consumer Privacy Litigation, 964 F.3d 1020 (9th Cir. 2020): https://cdn.ca9.uscourts.gov/datastore/opinions/2020/03/27/17-16278.pdf.

- CORTE SUPREMA NORTEAMERICANA. Caso In re Nickelodeon Consumer Privacy Litigation, 827 F.3d 262 (3d Cir. 2016): https://www2.ca3.uscourts.gov/opinarch/141368p.pdf.

- CORTE SUPREMA NORTEAMERICANA. Caso: Facebook, Inc. v. Duguid, 593 U.S. ___ (2021): https://www.supremecourt.gov/opinions/20pdf/19-511_gfbh.pdf.

- CORTE SUPREMA NORTEAMERICANA. Caso: Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058 (9th Cir. 2016): https://cdn.ca9.uscourts.gov/datastore/opinions/2016/07/12/13-17154.pdf.

- CORTE SUPREMA NORTEAMERICANA. Caso: Federal Trade Commission v. Google Inc., 736 F.3d 1236 (9th Cir. 2013): https://law.justia.com/cases/federal/appellate-courts/ca9/10-60309/10-60309-2013-09-10.html.

- CORTE SUPREMA NORTEAMERICANA. Caso: Spokeo, Inc. v. Robins, 578 U.S. ___ (2016): https://www.supremecourt.gov/opinions/15pdf/13-1339_5h26.pdf.

- CORTE SUPREMA NORTEAMERICANA: Caso United States v. Microsoft Corp., 584 U.S. ___ (2018): https://www.supremecourt.gov/opinions/17pdf/17-2_6j37.pdf.

- CORTE SUPREMA NORTEAMERICANA: Caso United States v. Warshak, 631 F.3d 266 (6th Cir. 2010): https://law.resource.org/pub/us/case/reporter/F3/631/631.F3d.266.08-3997.pdf.

- CORTE SUPREMA NORTEAMERICANA. Caso: ZL Technologies, Inc. v. LinkedIn Corp., 789 F.3d 1101 (9th Cir. 2015): https://scholar.google.com/scholar_case?case=15973756508800261 00&q=ZL+Technologies+v.+LinkedIn&hl=en&as_sdt=2006.

- EUROPEAN DATA PROTECTION BOARD, "Statement on the processing of personal data in the context of the COVID-19 outbreak": https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf.

- ELKINS, A., Quantum computing is coming for your data. TechCrunch, 2018: https://techcrunch.com/2018/09/28/quantum-computing-is-coming-for-your-data/

- EUROPEAN COMPETITION NETWORK, "Joint statement on the outcome of the Google Search case", 2019: https://ec.europa.eu/competition/ecn/201903_joint_statement_google_case_en.pdf.

- EUROPEAN PARLIAMENT, General Data Protection Regulation (GDPR), 2018: https://www.europarl.europa.eu/news/en/headlines/society/20180411STO00622/general-data-protection-regulation-gdpr-what-changes-from-25-may.

- EUROPEAN PARLIAMENT, "European Parliament calls for more effective EU action against monopolies", 2019: https://www.europarl.europa.eu/news/en/press-room/20190321IPR32102/european-parliament-calls-for-more-effective-eu-action-against-monopolies.

- FEDERAL TRADE COMMISSION, "Facebook agrees to pay $5 billion and implement robust new protections of user information in settlement of data privacy cases", 2019: https://www.ftc.gov/news-events/press-releases/2019/07/facebook-agrees-pay-5-billion-implement-robust-new-protections.

- GENERAL DATA PROTECTION REGULATION (GDPR), https://www.europarl.europa.eu/news/en/headlines/society/20180411STO00622/general-data-protection-regulation-gdpr-what-changes-from-25-may

- HARDESTY, L., "Quantum computers pose a security threat that we're still totally unprepared for", en . *MIT Technology Review* (2018): https://www.technologyreview.com/2018/07/10/141371/quantum-computers-pose-imminent-threat-to-todays-encryption/.

- INFORMATION COMMISSIONER´S OFFICE, Data protection and coronavirus: what you need to know, 2020: https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/data-protection-and-coronavirus/.

- INFORMATION COMMISSIONER´S OFFICE, ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information, 2018: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/ico-issues-maximum-500-000-fine-to-facebook-for-failing-to-protect-users-personal-information/.

- KRAWCZYK, H., Post-quantum cryptography: What it is and why we need it", en *Communications of the ACM*, 64(1) (2021) 40-44: https://cacm.acm.org/magazines/2021/1/249182-post-quantum-cryptography/fulltext.

- Ley de Privacidad del Consumidor de California: California Consumer Privacy Act (CCPA), 2018: https://oag.ca.gov/privacy/ccpa.

- Ley de Protección de Datos del Estado de Maine: An Act to Protect the Privacy of Online Consumer Information, 2019: https://legislature.maine.gov/legis/bills/getPDF.asp?paper=SP0007&item=1&snum=129.

- Ley de Protección de Datos del Estado de Virginia: Virginia Consumer Data Protection Act, 2021: https://lis.virginia.gov/cgi-bin/legp604.exe?211+sum+SB1392.

- Ley de Protección de Datos del Estado de Florida: Florida Information Protection Act, 2014: https://www.flsenate.gov/Laws/Statutes/2014/501.171.

- Ley de Protección de Datos del Estado de Vermont: Act 171: An Act Relating to Data Brokers and Consumer Protection, 2018: https://legislature.vermont.gov/assets/Documents/2018/Docs/ACTS/ACT171/ACT171%20As%20Enacted.pdf.

- Ley de Protección de Datos del Estado de Oklahoma: Oklahoma Personal Data Protection Act, 2010: https://www.ok.gov/oag/documents/Oklahoma%20Personal%20Data%20Protection%20Act.pdf.

- Ley de Privacidad del Consumidor de California: California Consumer Privacy Act (CCPA), 2018: https://oag.ca.gov/privacy/ccpa.

- Ley de Protección de Datos del Estado de Texas: Texas Identity Theft Enforcement and Protection Act, 2005: https://statutes.capitol.texas.gov/Docs/BC/htm/BC.521.htm.

- Ley de Protección de Datos del Estado de Nueva York: New York State SHIELD Act, 2019: https://www.nysenate.gov/legislation/bills/2019/s5575.

- Ley de Protección de Datos del Estado de Carolina del Norte: North Carolina Identity Theft Protection Act, 2005: https://www.ncleg.gov/EnactedLegislation/Statutes/PDF/ByArticle/Chapter_75C/Article_2.pdf.

- Ley de Protección de Datos del Estado de Illinois: Illinois Personal Information Protection Act, 2005: https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2256&ChapterID=64.

- Ley de Protección de Datos del Estado de Dakota del Norte: North Dakota Century Code, 2015: https://www.legis.nd.gov/cencode/t51c16.pdf.

- NARAYANAN, A. & MANICKAM, P., The impact of quantum computing on cryptography and data security: A survey. Journal of Information Privacy and Security, 15(3) (2019) 142-155: https://www.tandfonline.com/doi/abs/10.1080/15536548.2019.1604862.

- OFICINA DEL COMISIONADO DE INFORMACIÓN DEL REINO UNIDO, "Informe final en investigación sobre el uso de datos de Facebook por parte de Cambridge Analytica", 2018: https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf.

- OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER, 2020. Videoconferencing security tips. Office of the Australian Information Commissioner: https://www.oaic.gov.au/privacy/guidance-and-advice/video conferencing -security-tips/.

- OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER, Australian Privacy Act reform, 2018: https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-act-reform/.

- OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, The Personal Information Protection and Electronic Documents Act (PIPEDA), 2019: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda.

- OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, Advice for videoconferencing apps and services, 2020: https://www.priv.gc.ca/en/privacy-topics/technology/videoconferencing-apps-and-services/

- ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS, "Directrices de la OCDE sobre privacidad y transparencia", 2016: http://www.oecd.org/internet/empresas/directrices-privacidad-transparencia.htm

- PÉREZ, J., "El derecho a la protección de datos en la era digital: Retos y perspectivas", en *Revista de Derecho y Tecnología*, vol. 7, nº 1 (2020) 1-17: https://revistas.ucm.es/index.php/RDTI/article/view/69763.

- REUTERS Agency, EU to investigate Apple over Spotify's complaint, 2019: URL: https://www.reuters.com/article/us-eu-apple-antitrust/eu-to-investigate-apple-over-spotifys-complaint-idUSKCN1R00Q1.

- REUTERS Agency, EU to study Apple's iPhone and iPad software: sources, 2019: https://www.reuters.com/article/us-eu-apple-antitrust/eu-to-study-apples-iphone-and-ipad-software-sources-idUSKCN1R31Q6.

- SENADO FEDERAL DO BRASIL, Lei Geral de Proteção de Dados Pessoais (LGPD), 2028: https://www.senado.gov.br/atividade/rotinas/materia/getPDF.asp?t=223688&tp=1.

- THE NEW YORK TIMES, "Tech Giants Prepare for a Sweeping E.U. Privacy Law to Take Effect", 2019: https://www.nytimes.com/2018/05/23/technology/eu-gdpr-privacy-law.html.

- TRIBUNAL FEDERAL DE AUSTRALIA, Caso Privacy Commissioner v Facebook Inc (No 2) [2020] FCA 1307: https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2020/2020fca1307.

- TRIBUNAL GENERAL DE LA UNIÓN EUROPEA, Google/AdSense, T-612/17, Tribunal General de la Unión Europea, 26 de septiembre de 2019: https://curia.europa.eu/juris/liste.jsf?num=T-612/17.

- TRIBUNAL SUPREMO DE CANADÁ, Caso Telus Communications Inc. v. Wellman, 2019: https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/17545/index.do

- U.S. CONGRESS, Coronavirus Aid, Relief, and Economic Security Act (CARES Act). U.S. Government Publishing Office, 2020: https://www.congress.gov/bill/116th-congress/house-bill/748/text.

- WEHNER, S. & WILDE, M., Quantum computing and cryptography. arXiv preprint arXiv:1801.01465, 2018: https://arxiv.org/abs/1801.01465.

- WONG, J. V, California passes landmark data privacy bill, giving consumers more control over their personal information. *The Guardian*, 2019: https://www.theguardian.com/technology/2018/jun/28/california-data-privacy-law-consumers-facebook-google.