Universidad de San Andrés

Maestría en Derecho Empresario

Jaque a la privacidad, ¿Cómo preservarla en la era de las plataformas digitales?

Autor: Bellocq, María Victoria

Director de Tesis: Dr. Palazzi, Pablo

Buenos Aires, 10 de Noviembre de 2023

RESUMEN

Mediante la presente investigación examino el consentimiento como base legal para la recolección y procesamiento de datos personales. Es por ello que, a través la revisión de la literatura existente sobre el tema, la reglamentación nacional y derecho comparado busco proporcionar una comprensión de los desafíos y tendencias actuales en materia de protección de datos personales en oportunidad del uso de plataformas digitales.

En tanto, analizaré el impacto en la protección de datos personales con los mecanismos actualmente aplicados e implementados, con miras a establecer buenas prácticas para las empresas para abordar de manera efectiva el desafío que hoy representa la protección de la privacidad de los titulares de datos personales en los entornos digitales.

ABSTRACT

Through this investigation I examine consent as a legal basis for collection and processing of personal data. Therefore, I will review the current literature on the subject in question, local legislation, and foreign law in order to provide an understanding over the challenges and tendencies regarding data protection while using digital platforms.

Meanwhile, I will analyse the impact on data protection of current mechanisms applied and implemented aiming to establish best practices for companies to address in an effectively manner the challenges that involves today privacy of data subjects on digital environments.

INDICE

I. INTRODUCCIÓN

Con el inicio de Internet y sus interminables usos surge una mayor capacidad y facilidad en las comunicaciones, en particular mediante las plataformas digitales. Los autores coinciden al momento de definir las plataformas digitales en qué la mayoría comparte tres características básicas: son un medio tecnológico, facultan la interacción entre usuarios (o grupos de usuarios) y permiten que esos usuarios puedan realizar acciones específicas (de Reuver et al., 2018; P. Evans & Gawer, 2016)[1]. Las plataformas digitales son entonces entornos online o virtuales que permiten a los usuarios realizar distintas actividades, en un espacio colaborativo que almacena y procesa información personal generando contenido personalizado.

Las plataformas digitales son una parte esencial de la vida moderna y tienen un gran impacto en el sector empresarial y en la sociedad en general. Por la capacidad de interactuar e influenciar por medio de la comunicación a un universo ilimitado de personas, ofrecen la posibilidad de conectar con personas desconocidas, ya sea mediante un diálogo directo o por influencias de estos. Los distintos estudios conceptualizan las plataformas digitales desde un punto d vista no técnico como redes o mercados comerciales que permiten realizar transacciones en ya sea entre empresas(B2B), entre empresa y consumidor(B2C), o incluso intercambios entre consumidores(C2C) (Tan et al. 2015, Koh and Fichman 2014, Pagani 2013; Ye et al. 2012)[2] De aquí surge un modelo de negocios que se basa en el aporte de miles de usuarios, quienes brindan su información personal y la hacen disponible a distintos interlocutores, muchas veces desconocidos y con fines no del todo claros y explícitos. La posibilidad que tienen los usuarios de brindar las características de su perfil, compartiendo información personal con terceros de manera deliberada

[1] Kari Koskinen, Carla Bonina & Ben Eaton, "Development Implications of Digital Economies Paper No. 8 Digital Platforms in the Global South: Foundations and Research Agenda" (2018). Manchester, UK. Ed. Centre for Development Informatics Global Development Institute, SEED University of Manchester. Traducción de mi autoría "most digital platforms can be seen as sharing three basic characteristics: they are technologically mediated, enable interaction between user groups and allow those user groups to do particular things (de Reuver et al., 2018; P. Evans & Gawer, 2016)"

[2] Kari Koskinen, Carla Bonina & Ben Eaton, "Development Implications of Digital Economies Paper No. 8 Digital Platforms in the Global South: Foundations and Research Agenda" (2018). Traducción de mi autoria "studies have conceptualized digital platforms based on a non-technical view that presents platforms as a commercial network or market that enables transactions in the form of business-to business (B2B), business-to-customer (B2C), or even customer-to-customer (C2C) exchanges (Tan et al. 2015, Koh and Fichman 2014, Pagani 2013; Ye et al. 2012)"

brinda una mayor contingencia sobre el mal uso y abuso que se pueda dar de dicha información. Ésta es a su vez compartida con toda la comunidad de usuarios, de proveedores y de clientes de la propia plataforma, con lo cual se pierde de ese modo el control si es que no se encuentran en aplicación las medidas técnicas y organizativas adecuadas para asegurar la privacidad de los datos personales y la protección de los derechos de los titulares de datos personales.

El Reglamento General de Protección de Datos (GDPR) establece en su artículo 6(1) establece que las bases legales para la recolección y tratamiento de datos son:

a) el titular de datos personales ha brindado su consentimiento para procesar sus datos personales para uno o más fines específicos.

b) el procesamiento es necesario para el cumplimiento de un contrato en el que el titular de datos personales es parte o a pedido del titular de datos personales como paso necesario previo a la ejecución de un contrato.

c) el procesamiento es necesario para el cumplimiento de una obligación legal del responsable de datos.

d) el procesamiento es necesario para la protección de un interés vital del titular de datos personales u otra persona física.

e) el procesamiento es necesario para llevar adelante una tarea de interés público o en el ejercicio de una función oficial delegada en el responsable de los datos personales.

f)el procesamiento es necesario para los propósitos de interés legítimo perseguidos por el encargado de datos personales o por una tercera parte, excepto cuando esos intereses sean anulados por los derechos fundamentales y libertades de los titulares de los datos personales, en particular cuando el titular de datos sea un menor de edad.[3]

[3] Artículo 6(1) del Reglamento General de Datos Personales del Parlamento Europeo y el Consejo Europeo del 27 de Abril de 2016, (Regulation 2016/679) Traducción de mi autoría " Processing shall be lawful only if and to the extent that at least one of the following applies: a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the

En este trabajo me centraré en el consentimiento, la cual suele ser la base legal más utilizada en términos de plataformas digitales. Si bien dentro de esta temática se encuentra el consentimiento con relación a los datos sensibles (categoría especial de datos personales) o el consentimiento con relación a los menores de edad, entiendo que ambos temas exceden el ámbito de este documento. En primera instancia debemos definir que es el consentimiento, para luego poder abordar sus características intrínsecas e implicancia jurídica. El consentimiento es definido por la Real Academia Española como "(…)3. M. Der. Manifestación de voluntad, expresa o tácita, por la cual un sujeto se vincula jurídicamente."[4] Jurídicamente se define como una "afirmación expresa o implícita, aceptación con un curso de acción propuesto. El consentimiento es esencial en varias circunstancias. Por ejemplo, los contratos o matrimonios son inválidos a menos que ambas partes hayan prestado su consentimiento. El consentimiento debe ser brindado de manera libre e informada, sin valerse de coacción ni ardides y con suficiente capacidad legal para brindarlo…"[5] Tengamos presente que para la gran mayoría de la legislación el consentimiento para ser válido debe ser dado de manera libre, informada y concreta. El Reglamento General de Protección de Datos va más allá y dentro de estos parámetros establece mayores recaudos con miras a la protección del titular de los datos personales. En su Art 4 la REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS define las características para que el consentimiento sea considerado válido. Éste debe ser libre, específico para uno o más fines específicos y determinados, informado; y agrega como requisito que se trate de una indicación inequívoca de los deseos del titular de datos personales que por medio de una manifestación o una acción claramente afirmativa exprese su aceptación al procesamiento de sus datos personales.

data subject prior to entering into a contract; c) processing is necessary for compliance with a legal obligation to which the controller is subject; d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

[4] REAL ACADEMIA ESPAÑOLA: Diccionario de la lengua española, 23.ª ed., [versión 23.6 en línea]. <https://dle.rae.es> [29/07/2023].

[5] Oxford University Press. (2003). "Oxford Dictionary of Law," University of Oxford. Pág. 106. Traducción de mi autoría "Deliberated or implied affirmation; compliance with a course of proposed action. Consent is essential in a number of circumstances. For example, contracts and marriages are invalid unless both parties give their consent. Consent must be freely given, without duress or deception, and with sufficient legal competence to give it (…)"

De este modo, el consentimiento para el tratamiento de datos personales debe ser distinguible y separado de cualquier otra cuestión que se esté tratando; debe haber sido presentado en una forma clara y lenguaje simple, mediante una acción afirmativa que no dé lugar a duda que quiso brindar su consentimiento, y también (en cumplimiento con el deber de información) dejando asentado todos los derechos que este posee y cómo ejercerlos incluyendo la posibilidad de revocarlo. El titular de datos personales puede retirar su consentimiento para el tratamiento de datos personales en cualquier oportunidad, no obstante, todo uso que se haya hecho de los datos mientras el consentimiento persistía, es válido. La revocación del consentimiento operará a futuro y no con efectos retroactivos.

Hay usos y fines específicamente enumerados en los respectivos términos y condiciones de uso de las distintas plataformas digitales, que los usuarios deben aceptar para poder hacer uso de las mismas, como ser fines publicitarios, marketing dirigido, fines estadísticos, de estudio de mercado y de productos. La realidad es que estos términos y condiciones suelen ser textos extensos, complejos y poco claros para el común denominador; en la mayoría de las oportunidades los usuarios desconocen sus derechos y las posibilidades de ejercerlos o de optar qué información compartir (o no). De este modo, la recolección y el tratamiento de datos personales por parte de aquellas plataformas digitales plantea preocupaciones importantes sobre la privacidad y la seguridad de los usuarios. La carencia de controles adecuados y medidas eficaces de los mecanismos de control permite la exposición de aquellos datos personales que no debieran ser de público conocimiento ni de libre disponibilidad por no contar con la autorización de su titular para ser utilizada por terceros o para fines desconocidos para este.

Los modelos de bases de datos y su acceso se han vuelto cada vez más complejos y a su vez, más versátiles. La interacción entre los usuarios y entre distintas plataformas permite y facilita el acceso a aquellos datos personales que fueron compartidos por los propios usuarios bajo el entendimiento de que estaban siendo resguardados y utilizados para fines determinados a los cuales inicialmente habían consentido.

En el caso de las plataformas digitales, el uso de la información personal de sus usuarios incentivando su aporte aún más allá de lo que pudiera ser estrictamente necesario con la finalidad de vender y monetizar esa información. Por supuesto que como toda empresa comercial su objetivo y razón de ser es lucrar y llevar adelante un negocio próspero,

pretender lo contrario sería desconocer la propia naturaleza empresarial de cualquier entidad en el comercio. Lo cuestionable de un comportamiento se suscita cuando pareciera que este fin es logrado mediante medidas que pudieran considerarse confusas, lo cual inicialmente podría interpretarse como un actuar desleal y, por ende, entender que el consentimiento prestado podría no haber sido verdaderamente informado.

Cada vez se escuchan más casos de investigación de diversas plataformas por los distintos organismos de contralor por supuestas violaciones a los derechos de los titulares de datos personales ya sea por sus actos u omisiones. De los más resonados localmente es el caso Citibank[6] con un profundo impacto en la operatoria de los bancos. En este caso el banco Citibank haciendo uso de los datos personales brindados por sus clientes procedió a utilizarlos para la evaluación crediticia de estos mediante un proceso automatizado. Más allá del debate acerca de la legitimidad o constitucionalidad de las decisiones tomadas en base a procesos totalmente automatizados sin intervención humana, debate que excede este trabajo, lo cierto es que el banco se valió de información para fines no consentidos y todo ello, sin el conocimiento de los titulares de dichos datos. En Argentina ha habido varias denuncias por el uso de datos para fines no consentidos, muchas de esas denuncias suelen involucrar transferencia de bases de datos entre distintos organismos estatales[7]. Otras denuncias son consecuencia de la comercialización de bases de datos por parte de las empresas responsables de estas, para fines no consentidos por sus titulares. De ahí que surjan varias cuestiones a tratar: el consentimiento informado de los titulares de datos, el uso posterior de dichos datos, el acceso autorizado a terceros y la falta de medidas apropiadas para evitar el acceso no autorizado de terceros.

Este trabajo analizará el impacto de la protección de datos personales en la obtención del consentimiento mediante plataformas digitales, a través la revisión de la literatura existente sobre el tema, la reglamentación nacional, como es la Ley 25.326 sobre protección de datos personales, el proyecto de reforma de dicha ley y también el Reglamento General de Protección de Datos (GDPR) junto con la Directiva de Privacidad y Comunicaciones Electrónicas 2002/58/EC (ePrivacy Directive), ambas normas con aplicación a

[6]Palazzi, Pablo A.(2006) "*El consentimiento para el tratamiento de datos personales (Opt-in versus opt-out bajo el régimen de la ley 25326)"*. Ed. Jurisprudencia Argentina 2006 II 379. Bs. As., Argentina.

[7] Cámara Nacional de Apelaciones en lo Contencioso Administrativo Federal, Sala V, 3-jul-2018, "Torres Abad Carmen c/ Estado Nacional s/ habeas data"

empresas radicadas en la Unión Europea y con alcance extraterritorial para aquellas empresas que aunque no se encuentren en la Unión Europea y procesen datos de ciudadanos europeos. Finalmente, el análisis jurisprudencial que hubiera en la materia tanto local como internacional. Teniendo como objetivo final proporcionar una comprensión completa de los desafíos y tendencias actuales en la protección de datos personales al obtener un consentimiento válido por medio de plataformas digitales, así como recomendaciones prácticas para las empresas y los usuarios para abordar estos desafíos de manera efectiva.

II. Implicaciones legales y regulatorias acerca del consentimiento

A. General Data Protection Regulation

Como mencioné previamente el Reglamento General de Protección de Datos en su Art. 6 establece cuales son las bases legitimas para el procesamiento de datos personales. En el Considerando 43 se expide sobre el consentimiento indicando que no será considerado libre cuando haya un desequilibrio de poder entre las partes. Del mismo modo tampoco será libre cuando hubiera lugar a varias actividades que procesen datos, si el consentimiento no puede ser brindado de manera independiente para cada una de ellas; aun cuando se trate del cumplimiento de un contrato para el que se solicita el consentimiento pese a no ser necesario para su cumplimiento.

De esta idea se desprenden los lineamientos 05/2020 fijados por el WP29 (Articulo 29 Working Party) en los que ahondare más adelante, que indican que para que el consentimiento sea libre el titular de datos personales debe tener una posibilidad real de elección sobre negar su consentimiento o de retirarlo. La Directiva 95/58/EC requería que los responsables de datos personales expidieran documentos independientes para obtener el consentimiento por el procesamiento de datos para cada fin separado de cualquier otro tipo de acuerdo que suscribiera o adhiera el titular de datos personales y que lo vinculara con el Responsable.

Bajo esta premisa es que Daniel J Solove en su trabajo "Murky Consent"[8] esboza su idea sobre la ficción del consentimiento, analizando los dos enfoques actuales. Esto es el sistema de Estados unidos donde el consentimiento se entiende dado por el mero hecho de ser informado que sus datos serán recopilados y procesados, entonces el titular de datos personales debe optar por ser excluido de ese consentimiento (sistema opt-out), por otro lado, tenemos el sistema que aplica la Unión Europea mediante el Reglamento General de Protección de Datos donde establece la necesidad de un consentimiento expreso. O sea, la tesitura opuesta a la de Estados Unidos, aquí se requiere que el titular de datos personales brinde su consentimiento mediante una acción claramente afirmativa, caso contrario se entiende que el Responsable de datos personales no cuenta con el consentimiento del titular de datos para el procesamiento de estos (sistema opt-in).

Solove propone que en ambos sistemas el consentimiento es una ficción ya que para que esté exista realmente el sujeto debería poder entender los términos de la elección que se le ofrece y realizar una evaluación a conciencia de los riesgos que ese tratamiento implica para tomar una decisión basada en costo-beneficio. Bajo el sistema opt-out la ficción se encuentra en que la inacción no es un consentimiento real, simplemente la ausencia de una negativa lo que en definitiva es una abstención no una aceptación.

Si bien el sistema opt-in es superador respecto al sistema opt-out sigue siendo deficiente, continua Solove debido a que el grado de granularidad que requiere el consentimiento expreso para que sea genuinamente informado implica textos extensos que aun utilizando lenguaje sencillo sería difícil para comprender acabadamente los riesgos que implica el tratamiento de e sus datos personales. Adicionalmente este volumen generaría lo que él denomina "fatiga del consentimiento", llevando al sujeto a restarle atención a o que se le informa y probablemente aceptar sin siquiera analizar la información. Por otro lado, la simplificación de ese aviso de privacidad para que sea fácilmente entendible y accesible llevaría a perder granularidad y no informar acabadamente sobre el tratamiento y procesamiento de los datos que serán recolectados.

[8] Solove, Daniel J. (2023) *"Murky Consent: An Approach to the Fictions of Consent in Privacy Law"*. Boston University Law Review, N° 114. Boston, USA. Ed. Boston University

Coincidentemente en el estudio realizado por Christine Utz, Martin Degeling, Sascha Fahl, Florain Schaub y Thorsten Holz[9] sobre los avisos de privacidad en las plataformas digitales de Europa que desde la entrada en vigor del Reglamento General de Protección de Datos requieren al titular de datos personales su consentimiento previo a instalar cookies. Las cookies son archivos de texto que se instalan en los distintos dispositivos (siempre que se haya consentido) almacenando información y "reenviándola" al Responsable. Esta puede ser información necesaria para que la plataforma pueda funcionar y luego hay otras como las de marketing (en general implican compartir la información con terceros para realizar acciones de marketing dirigido) o cookies analíticas (reenvía información acerca de la forma en que el usuario interactuó con la plataforma) de las más comunes que se pueden encontrar en un aviso de privacidad.

En base a este cambio operado en las plataformas digitales, el estudio se centró en estudiar la tendencia sobre aceptación del consentimiento basada en diversos factores, como ser el diseño de la plataforma. Analizaron si la posición del aviso de privacidad sobre cookies, la cantidad de opciones de consentimiento (granularidad) que brinda el aviso, la existencia de un enlace al aviso de privacidad o el uso de lenguaje técnico vs no técnico influenciaba en interacción y eventualmente en la decisión respecto a ese aviso.

En resumen, el estudio estableció que efectivamente el posicionamiento influenciaba en la interacción y a mayor granularidad, especificidad y opciones las personas tenían una importante tendencia a rechazar y limitar considerablemente el procesamiento de sus datos. El desafío entonces se encuentra no solo en cumplir con el Reglamento General de Protección de Datos (y la Directiva de Privacidad y Comunicaciones Electrónicas), sino que adicionalmente debe lograr la obtención del consentimiento sin abrumar al titular de datos que en tal caso restaría atención al aviso de privacidad y la información que contiene. Concluye así que, si bien los titulares de datos personales preferirían interactuar con los avisos de privacidad, especialmente aquellos que quieren restringir o limitar el uso de cookies, seguir con excesivo rigorismo la letra de la regulación vigente llevaría a que menos del 0,1% de los usuarios de las plataformas consientan de manera activa el uso de cookies.

[9]Christine Utz, Martin Degeling, Sascha Fahl, Florain Schaub y Thorsten Holz, 2019, "(Un)informed consent: Studying GDPR consent notices in the Field, Conference on Computer and Communications Security (CCS'19), Londres, Reino Unido

Por otro lado, Solove argumenta que el sujeto no cuenta con capacidad para prestar su consentimiento de manera significativa, sea por falta de entendimiento de las complejidades inherentes a las actividades de procesamiento y los riesgos vinculados, cómo por tecnicismos que dificultan la comprensión de la información entre otros. Plantea que ante este escenario una alternativa sería la regulación de los casos en los que los datos personales podrían ser recolectados, usados y compartidos. No obstante, esta alternativa lleva implícitamente a anular o limitar la autonomía de la voluntad de las personas y atentar contra la libertad de elegir.

Considera que en lugar de luchar por volver legitimo el consentimiento que entiende ficticio es aceptarlo como tal ya que la éste por naturaleza es complejo y dinámico. Al mismo tiempo la tecnología en constante evolución, dificultando que el titular de Datos Personales pueda otorgar su consentimiento de manera informada, que indefectiblemente sería inabarcable y si tratara de proporcionar de manera completa y acabada.

Propone una posición intermedia que él denomina “murky consent”, que entiende realista y pragmática ya que permitiría cierto grado de autonomía individual debido a que el consentimiento brindado por el titular de datos personales serviría para un uso muy limitado de estos siendo el equilibrio entre un consentimiento ficticio y un paternalismo gubernamental.

Sugiere que las autoridades deberían permitir el procesamiento de datos personales mediante el consentimiento del Titular de datos personales en casos determinados y limitados a ciertas reglas que permitan al titular brindar su consentimiento para el procesamiento dentro de lo que serían actividades con un riesgo calculado aceptable. Estás reglas cumplirían la función de barreras protectoras en las cuales los Responsables de Datos Personales y los Titulares de Datos personales pueden moverse, lo que permitiría a las personas ejercer la autonomía de la voluntad dentro de los límites establecidos como riesgos apropiados en relación con los propósitos buscados mediante el procesamiento de sus datos.

En algún punto esto simplificaría la carga de los Responsables de Datos Personales que indica el art. 7 (1) del Reglamento General de Protección de Datos en la que éste debe poder demostrar que el titular de datos personales a brindado su consentimiento para el procesamiento, ya que estaría operando dentro de los límites fijados por la autoridad.

Cumpliendo asimismo con los requisitos que mencioné previamente para entender que el consentimiento es válido, esto es que sea libre, específico, informado e inequívoco. Características que son detalladas en el considerando 32 del Reglamento General de Protección de Datos:

"*1. El consentimiento debería ser una acción afirmativa y clara que establezca una indicación libre, informada e inequívoca que el titular de datos está de acuerdo con el procesamiento de sus datos personales, sea por una declaración escrita – incluyendo medios electrónicos- o por una declaración oral.*

2. Esto podría incluir un recuadro para tildar cuando se visita un sitio web, eligiendo configuraciones técnicas para servicios de la sociedad de la información[10] *o cualquier otra declaración o conducta que indique claramente en este contexto la aceptación del titular de datos al procesamiento propuesto de sus datos personales.*

3. El silencio, las casillas pre tildadas o la inacción no deberían constituir como consentimiento.

4. El consentimiento debe abarcar todas las actividades de procesamiento llevadas a cabo para el mismo fin o fines.

5. Cuando el procesamiento tenga varios fines, el consentimiento debería ser por cada uno de ellos.

6. Si el consentimiento del titular de datos personales debe ser brindado mediante una solicitud por medios electrónicos, el pedido debe ser claro, conciso y no innecesariamente interrumpir el uso del para el cual es brindado."[11]

[10] Los servicios de la sociedad de la información son definidos por el Art.4 (25) del Reglamento General de Datos Personales que se remite al Art 1 (1b) de la Directiva 2015/1535 del Parlamento Europeo y del Consejo como "todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios." Traducción de mi autoría ('**Information society service**' means any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services).

[11] Considerando 32, Artículo 6(1) del Reglamento General de Protección de Datos del Parlamento Europeo y el Consejo Europeo del 27 de Abril de 2016, (Regulation 2016/679) Traducción de mi autoría "Conditions for Consent: 1Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. 2This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data

Al requerir que el consentimiento se dado de manera explícita y mediante una acción afirmativa, fija un estándar para las empresas que gestionan las plataformas digitales ya que deberán guardar evidencia de la obtención de este consentimiento por medio electrónicos.

En línea con esto el Considerando 42 del Reglamento General de Protección de Datos esclarece que es el Responsable de los datos quien debe demostrar que ha dado cumplimiento con la normativa, invirtiendo así la carga de la prueba. Por lo tanto, al procesar datos utilizando el consentimiento como base legal debe asegurarse que el titular de datos es consciente que está dando su consentimiento y el alcance de éste. Ahonda aún más que en los consentimientos pre redactados cómo son los que se encuentran en las plataformas digitales, hay que utilizar lenguaje simple, claro y fácilmente accesible. Para que el consentimiento sea informado debe contar con cierta información que considera básica como ser la identificación de la finalidad para la que serán recolectados y procesados sus datos personales, quien actuara como Responsable de los datos personales, en el acápite D explicaré como la Ley argentina amplia los requisitos necesarios para que el consentimiento sea considerado informado. Finalmente destaca que el consentimiento no será considerado libremente dado si no se le ofreció una posibilidad genuina y real de elección o si el ejercicio de esta al rechazar o restringir el uso de sus datos personales repercutirían en detrimento del titular de datos personales.

B. Privacy and Electronic Communications Directive 2002/58/EC[12]

También conocida como "ePrivacy Directive", actualizada por la Directiva 2006/24/EC y la Directiva 2009/136/EC, es el instrumento legal publicado por la Comi-

subject's acceptance of the proposed processing of his or her personal data. 3Silence, pre-ticked boxes or inactivity should not therefore constitute consent. 4Consent should cover all processing activities carried out for the same purpose or purposes. 5When the processing has multiple purposes; consent should be given for all of them. 6.If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise, and not unnecessarily disruptive to the use of the service for which it is provided."

[12] Directive 2002/58/EC of the European Parliament and of the Council, amended by Directive 2006/24/EC and Directive 2009/136/EC of the European Parliament and of the Council.

sión Europea que se ocupa de aquellas cuestiones que trajo aparejadas los avances tecnológicos con relación a la protección de la privacidad en el sector de las comunicaciones y servicios electrónicos, rastreo y monitoreo por medios digitales a usuarios.

En su considerando 17, la Directiva de Privacidad y Comunicaciones Electrónicas aclara que, a los fines de la interpretación de ésta, el consentimiento de los usuarios o suscriptores tendrán el mismo significado que el consentimiento del titular de datos personales de acuerdo con la definición de la Directiva 95/46/EC, sin importar si se trata de personas de existencia física o jurídica. Continúa diciendo que el consentimiento puede ser otorgado por cualquier método apropiado que permita una indicación libre, especifica e informada de los deseos del usuario, incluyendo tildar un recuadro al visitar un sitio web.[13] El Comité Europeo de Protección de Datos (EDPB) en su opinión 05/2019 estableció en el punto 2.3 sobre el Articulo 2(f) de la Directiva de Privacidad y Comunicaciones Electrónicas que al referirse al consentimiento del usuario o suscriptor se corresponde con el consentimiento del titular de datos de la ahora GDPR.

Eleni Klosta argumenta que las normas del Reglamento General de Protección de Datos referidas al consentimiento son aplicables al sector de las comunicaciones electrónicas, salvo que la Directiva de Privacidad y Comunicaciones Electrónicas contenga alguna previsión especifica que regule el tema en cuestión. Sería la aplicación de la doctrina en que una ley en materia especifica (lex specialis) predomina sobre una ley generalista (lex generalis), que sería el caso del Reglamento General de Protección de Datos.[14]

La Directiva de Privacidad y Comunicaciones Electrónicas trata sobre una temática especifica de las Comunicaciones electrónicas, como son las cookies en su Art. 5(3):

"Los Estados Miembros deben asegurar que, al almacenar información, o al obtener acceso a la información ya almacenada en el dispositivo del suscripto o usuario, solo sea permitido bajo la condición de que éste ha dado su consentimiento, habiendo sido provisto de información clara y completa de acuerdo con la Directiva 95/46/EC,

[13]Directive 2009/136/EC, (Whereas 17) ": For the purposes of this Directive, consent of a user or subscriber, regardless of whether the latter is a natural or a legal person, should have the same meaning as the data subject's consent as defined and further specified in Directive 95/46/EC. Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website".

[14] Eleni Kosta (2013), "*Consent in European Data Protection Law*", Martinus Nijhoff Publishers, Paises Bajos

sobre la finalidad del procesamiento. Esto no evitará cualquier almacenamiento o acceso técnico para solo fin de llevar adelante la transmisión de la comunicación por una red electrónica de comunicación, o por ser estrictamente necesario para el proveedor de un servicio de información social explícitamente solicitado por el suscriptor o usuario para proveer el servicio. "[15]

Gracias a la actualización que recibió la Directiva 2002/58/EC en el 2009 la directiva tomo el nombre coloquial de la "Ley de cookies" debido al especial interés que tomo sobre el consentimiento específico para cada tipo de cookie, ya que cada una tiene fines distintos, por ende, debe obtenerse consentimientos separados, individualizados e informados.

La clave está en que la Directiva de Privacidad y Comunicaciones Electrónicas se centra en las comunicaciones electrónicas y en particular las cookies que permiten obtener muchos más datos personales, en particular las cookies sobre comportamiento. Podría decirse que las plataformas digitales están regidas principalmente por esta Directiva, en ausencia de una norma específica que regule algún aspecto, deberá recurrir a el Reglamento General de Protección de Datos en búsqueda de claridad.

El Comité Europeo de Protección de Datos en su opinión 5/2019, Art 4.1 (40) sobre la interacción entre la Directiva de Privacidad y Comunicaciones Electrónicas y el Reglamento General de Protección de Datos explica que en el Art5(3) de la Directiva de Privacidad y Comunicaciones Electrónicas es requerido el consentimiento previo para almacenar o acceder a información (que son datos personales) en un dispositivo del usuario o suscriptor y toma preminencia respecto al Art. 6 del Reglamento General de Protección de Datos. Lo mismo sucede en los casos del Art. 9 y 13 de la ePrivacy que requiere

[15] Traducción de mi autoría: Directive 2002/58/EC Article. 5(3) Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

el consentimiento para determinadas acciones, por lo que el Encargado de Datos Personales no podrá hacer uso de las demás bases legales establecidas en el Art. 6 del Reglamento General de Protección de Datos para el procesamiento de los datos personales.[16]

Así las cosas, la Directiva de Privacidad y Comunicaciones Electrónicas da un rol de mayor preponderancia al consentimiento para varias actividades procesadoras de datos. Por ejemplo, en su Art. 6(3) para las comunicaciones electrónicas con fines de marketing o para ofrecer servicios de valor agregado puede procesar la información brindada por el usuario o suscriptor por el tiempo necesario para cumplir esa finalidad y siempre que éste haya dado su consentimiento previo. Asimismo, los usuarios o consumidores deben tener la posibilidad de retirar su consentimiento en cualquier momento.

De esta forma la ePrivacy continúa dando un rol central al consentimiento con miras a que el titular los datos personales siempre tenga control de estos mediante una elección genuina de aportar (o no) sus datos y poder detener el procesamiento en cualquier momento mediante la retractación de su decisión. Esto se evidencia nuevamente en la ePrivacy que encuentra su correlato en el derecho de información esgrimido en el Reglamento General de Protección de Datos, cuando en el Art. 6(4) párrafo 4 establece que el proveedor de servicios (quien ocupara el rol de Encargado de tratamiento) debe informar al suscriptor o usuario del tipo de datos que se procesarán, y la duración del procesamiento cuando la finalidad sea la facturación del servicio al suscriptor o cuando se trate del procesamiento de pagos; y previamente a obtener el consentimiento en el caso comunicaciones con fines de marketing o que agreguen valor a los servicios. No obstante, el usuario o suscriptor de be contar en todo momento con la posibilidad de retirar su consentimiento para el procesamiento de su información.

Continua la Directiva de Privacidad y Comunicaciones Electrónicas en su Art 9 acerca de la información sobre localización, permitiendo el procesamiento de esos datos

[16] EDPB Opinion 05/2019 Art 4.1 (40) A similar situation occurs with regards article 5(3) of the ePrivacy Directive, insofar as the information stored in the end-user's device constitutes personal data. Article 5(3) of the ePrivacy Directive provides that, as a rule, prior consent is required for the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user. To the extent that the adopted information stored in the end-users device constitutes personal data, article 5(3) of the ePrivacy Directive shall take precedence over article 6 of the GDPR with regards to the activity of storing or gaining access to this information. The outcome is similar in the interplay between article 6 of the GDPR and articles 9 and 13 of the ePrivacy Directive. Where these articles require consent for the specific actions they describe, the controller cannot rely on the full range of possible lawful grounds provided by article 6 of the GDPR.

siempre que sean anonimizados o con el consentimiento de los usuarios o suscriptores, siempre fijando un límite temporal para el procesamiento basado en la necesidad para la provisión del servicio. Nuevamente solicita que el consentimiento sea previo e informado, en particular sobre el tipo de datos de localización que se recopilara, la finalidad, durante cuánto tiempo el Responsable conservará esos datos para su procesamiento y si esos datos serán compartidos con terceros bajo el propósito de brindar un valor agregado al servicio. La norma también prevé que en estos casos el usuario o suscriptor conserve la posibilidad de retirar su consentimiento en cualquier oportunidad.[17]

El objetivo último que persigue la Directiva de Privacidad y Comunicaciones Electrónicas es que el usuario sea previamente informado sobre las implicaciones de aceptar las cookies en su dispositivo, para ello esa información deberá sr brindada en un lenguaje claro y fácilmente accesible para el usuario promedio. El uso de cookies requiere del consentimiento libre e inequívoco del usuario, lo que significa que el usuario debe consentir mediante una acción claramente afirmativa.

En enero del año 2023, Apple fue multada con 8 millones de euros por la Comisión Nacional de informática y libertades de Francia por publicidad dirigida no consentida. Durante el 2021 y 2022 se encontró que los usuarios del celular iPhone IOS 14.6 contaban con identificadores instalados para brindar publicidad personalizada al ingresar a la aplicación "App Store" y que no había sido previamente consentida.[18] En definitiva, lo que se penaliza es que Apple no cumplió con el precepto de la norma, no pueden instalarse cookies hasta tanto el usuario haya brindado su consentimiento.

C. Lineamientos 05/2020 sobre el consentimiento bajo el Reglamento General de Protección de Datos

Como ya comenté anteriormente el Comité Europeo de Protección de Datos adoptó como lineamientos el trabajo acordado por el Art.29 Working Party con relación al consentimiento según el Reglamento General de Protección de Datos, actualizando dichos lineamientos en virtud de algunas clarificaciones sobre la operatividad del Reglamento

[17] Directiva 2002/58/EC, Articulo 9 (1) y (2).

[18] Deliberación SAN-2022-025 del 29 de diciembre de 2022 de Comisión Nacional de Tecnologías de la Información y Libertades, Francia

General de Protección de Datos y la Directiva 2002/58/EC. Dado que la noción de consentimiento utilizada en dicha normativa ha evolucionado y por ende es que el Comité considera que ciertas aclaraciones son necesarias.

En estos lineamientos se reitera que el consentimiento es una de las seis bases legales para procesar datos personales y que solo puede ser considerada una base legal apropiada cuando el titular de datos personales tiene control real y se le ofrece una genuina elección con relación a la aceptación o rechazo del procesamiento de sus datos. El consentimiento es una herramienta que otorga el control al sujeto, sin embargo, cuando ese control es ilusorio el consentimiento se vuelve inválido y por tanto el procesamiento ilegal. La posibilidad que las personas acepten (y consientan) al tratamiento de sus datos debería estar sujeto a rigurosos requerimientos y su obtención de modo alguno podría disminuir las obligaciones del Responsable de Datos Personales.[19]

Los lineamientos recuerdan que en el Art.95 el Reglamento General de Protección de Datos establece que las obligaciones y requisitos para el procesamiento de datos personales en conexión con la provisión de servicios de comunicación electrónica que sea de disponibilidad pública no será reforzado ya que la Directiva de Privacidad y Comunicaciones Electrónicas contempla normas específicas para estas actividades. No obstante, cuando ésta no establezca obligaciones al respecto, el Reglamento General de Protección de Datos operará en ausencia de legislación específica, por lo que debe interpretarse que estas no son obligaciones adicionales, sino condiciones previas. Consecuentemente los requisitos del Reglamento General de Protección de Datos que hacen a la validez del consentimiento son perfectamente aplicables a las actividades que se encuentran alcanzadas por la Directiva de Privacidad y Comunicaciones Electrónicas.

Así los lineamientos comienzan a explicar que la definición del consentimiento en el Art.4 (11) del Reglamento General de Protección de Datos sique la noción esbozada por su predecesora (Directiva 95/46/EC), no obstante, el Articulo 7 y los considerandos 32, 33, 42 y 43 incorporan obligaciones a los Responsables para cumplir con los elementos del consentimiento y cumplir así con esté requerimiento, previo al procesamiento.

[19] Comité Europeo de Protección de Datos, "Lineamientos 05/2020 sobre consentimiento bajo el Reglamento Europeo de Protección de Datos"

Indiqué previamente que los elementos para que el consentimiento sea reputado válido son: libremente dado, específico, informado e inequívoco.

Al hablar de libre, hago referencia a que debe haber una elección de poder negar el consentimiento o retirarlo con la misma facilidad con la que fue otorgado. Entonces, el consentimiento es reputado libre cuando el Titular de datos personales tiene la posibilidad de negar su consentimiento sin miedo a represalias o una consecuencia negativa. De ello se desprende que ante una situación donde no igualdad entre las partes, como puede ser una relación laboral o una relación contractual con cláusulas de adhesión difícilmente puedan cumplir con este requerimiento.

El Reglamento General de Protección de Datos hace mención específicamente a la disparidad entre las partes cuando quien actúa como Responsable de los datos personales es una autoridad pública, aunque no está prohibido el consentimiento como base legal para éstas, deberán realizar una evaluación a conciencia si es la mejor opción y que factibilidad de demostrar el cumplimiento de este requisito hay. Los lineamientos dan cuenta de algunos ejemplos en los que podría proceder el procesamiento de datos por parte de autoridades públicas utilizando el consentimiento como base legal y sin recaer en este dilema.

En estos casos de disparidad en la relación entre las partes será difícil demostrar que efectivamente el consentimiento no se encontraba viciado por este temor a un perjuicio para el Titular de datos personales y serán casos excepcionales en los que pueda demostrarse que en estos vínculos que en apariencia podrían verse en distintas posiciones de poder, en el caso concreto no resulta tener injerencia.

Los lineamientos analizan también el consentimiento para el procesamiento brindado en el marco de una relación contractual, en esta el Titular de datos personales actúa bajo el entendimiento que su consentimiento para el procesamiento es necesario para el cumplimiento de ese contrato. Esto puede que sea el caso, o bien puede ser una práctica en la que se solicita el consentimiento para el procesamiento de datos personales que no son necesarios para el cumplimiento del contrato, y aun así está atado a los términos y condiciones del contrato en sí. Por ende, el Titular de datos personales entiende que el cumplimiento de ese contrato está condicionado a que brinde su consentimiento. Es otro

de los ejemplos en los que se denota que el Titular de datos personales no fue libre al momento de tomar su decisión, no tuvo control sobre su información.

Por otro lado, si el Responsable de datos personales requiere ciertos datos para el poder cumplir con el contrato que vincula a las partes, esa deberá ser la base legal que utilice (Art. 6(1)b) y no el consentimiento. Para ello debe haber una relación directa y objetiva entre el procesamiento y la finalidad del contrato, adoptando una postura restrictiva al interpretar qué datos son necesarios para el cumplimiento de un contrato.

Tampoco sería considerado libre, aquel consentimiento que fuera condición para acceder a servicios y funcionalidades, como son los pop-ups que surgen al acceder a distintas plataformas digitales que imposibilitan el acceso a su contenido hasta tanto el usuario acepte el almacenamiento y acceso a las cookies, cuando no hay opción para rechazar el procesamiento mediante cookies. En ese sentido se expide la Directiva 2002/58/EC y los Lineamientos del 05/2020 siguen la misma idea.

La posibilidad de retirar el consentimiento va de la mano del concepto de libertad en la elección, de la misma manera facilidad con la que el Titular de Datos Personales brindó su consentimiento debiera poder arrepentirse y rechazar todo procesamiento futuro retirando su consentimiento, incluso solicitando la eliminación de sus datos teniendo control sobre estos.

La granularidad del consentimiento, esto es la posibilidad de brindar consentimientos separados para cada finalidad y cada procesamiento, está directamente relacionada con los principios de información y especificidad que afectan a la libertad del consentimiento, principios expresados por el Reglamento General de Protección de Datos y aplicables a todas las situaciones previstas por la Directiva de Privacidad y Comunicaciones Electrónicas.

De acuerdo a esto considero importante remarcar que la granularidad permite cumplir con la mayoría de los requisitos de validez del consentimiento, esto debido a que tiene impacto en los siguientes aspectos: A) principio de transparencia haciendo honor a la necesidad de información completa y clara; B) especificidad, la información al ser granular permite informar al sujeto titular de datos personales sobre cada actividad procesadora y los fines que abarca; C) inequívoca, toda vez que permite aceptar (o no) cada alternativa por separado, lo que requerirá una acción afirmativa indiscutible; y finalmente

D) libre, el titular de datos personales tiene la capacidad de elegir si aceptar o no, esto es ejercer su facultad de rechazar el procesamiento de manera total o parcial.

Si bien la Directiva 2002/58/EC se encuentra en revisión para eventualmente ser reemplazada por la Regulación sobre Privacidad en las comunicaciones electrónicas, el consentimiento en este borrador se encuentra vinculado a la definición que brinda el Reglamento General de Protección de Datos por lo que los Responsables de Datos Personales para las actividades procesadoras de datos personales por medio de mensajes de marketing online, métodos de rastreo online, cookies en aplicaciones, incluyendo dentro de su alcance a los servicios de mensajería online y otras plataformas precisarán obtenerlo bajo los requerimientos que eventualmente establezca dicha Regulación. Hasta tanto sea aprobada por los Estados Miembros, los Responsables de Datos Personales deberán regirse por la aún vigente Directiva de Privacidad y Comunicaciones Electrónicas y estos lineamientos cuya finalidad es esclarecer su alcance.

Al momento de entrar en vigor el Reglamento General de Protección de Datos el mismo legislador solicitó a la Comisión Europea la actualización de esta norma. A octubre del 2023 el proyecto de reforma se encuentra en tratamiento y continúa siendo debatido.

D. Ley de Protección de los Datos Personales de Argentina

En octubre del año 2000, el Congreso sancionó la primera ley de protección de datos de Argentina inspirada en la Directiva 95/46/CE, predecesora del Reglamento General de Protección de Datos. Dando de esta manera un marco legal más extenso y detallado del derecho a la protección de los datos personales amparado por el Art. 43 de la Constitución Nacional Argentina.

El espíritu y misión de esta ley es enunciado en el Art.1, cuando informa que tiene por objeto la protección de los datos personales almacenados en registros públicos o privados para preservar el derecho al honor, a la intimidad y el acceso a la información. A diferencia de la legislación europea, la legislación argentina actual hace extensiva la protección de los datos a las personas de existencia ideal, no solamente a las personas físicas.

Con relación al consentimiento Ley de Protección de los Datos Personales de Argentina tiene un enfoque bastante distinto a la regulación europea, ya que en lugar de establecer cuáles serían las bases legales para el procesamiento establece que el consentimiento es el medio por defecto para que el tratamiento sea lícito. Sin el consentimiento del titular de datos personales no podría haber tratamiento, tal como comienza el enunciando el Art. 5

1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo con las circunstancias.

El referido consentimiento prestado con otras declaraciones deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6° de la presente ley. [20]

En la segunda parte del Art. 5 establece las excepciones por las cuales no se requeriría el consentimiento para el procesamiento de los datos personales.

2. No será necesario el consentimiento cuando:

a) Los datos se obtengan de fuentes de acceso público irrestricto;

b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;

c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;

d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;

[20] ARTICULO 5° — (Consentimiento), Ley 25.326 de Protección de Datos Personales, publicada en el Boletín Oficial del 30 de octubre de 2000

e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526. [21]

Si bien podría interpretarse que algunos de estos 5 puntos podrían constituir bases legales para el tratamiento, lo cierto es que no lo son. Como dije inicialmente y el propio articulo lo indica, son situaciones que con carácter de excepción habilitan el procesamiento aún sin haber obtenido el consentimiento del titular de datos personales.

Es todo un cambio de paradigma respecto al esquema europeo, que otorga un mayor espectro de bases para el tratamiento. En Argentina por el contrario el consentimiento es suficiente para cualquier actividad, liberando al Responsable de datos personales de realizar cualquier tipo de análisis respecto al tratamiento que va a realizar y si esa fuera la mejor base para garantizar la licitud de éste.

Lo único que se requiere para que el tratamiento sea lícito es que el consentimiento sea válido, bajo ley argentina será considerado como tal cuando reúna los requisitos de informado, libre y expreso sin adentrarse demasiado en estos. En oposición al Reglamento General de Protección de Datos, donde hay varios artículos que aclaran la definición de consentimiento, los requisitos que este debe tener, la forma de obtenerlo y otros tantos considerandos que ahondan en mayores detalles y aclaraciones. Adicionalmente al Reglamento, se cuentan con los distintos Lineamientos que emite el Comité Europeo de Protección de Datos, algunos dirigidos específicamente a tratar el consentimiento, interpretando la norma y dando recomendaciones al respecto sobre distintas situaciones que pudieran generar dudas.

El Decreto 1558/2001, que se encarga de reglamentar la Ley 25.326 tampoco aporta demasiado al tratar el Art. 5 donde la aclaración que realiza es que el consentimiento será informado cuando la explicación al titular de datos sea dada previamente a que este exprese su voluntad de una forma adecuada a su nivel social y cultural. En cuanto a la revocación de éste indica que no tiene límite temporal, no obstante, no tendrá efectos retroactivos.

[21] Comité Europeo de Protección de Datos, "Lineamientos 05/2020 sobre consentimiento bajo el Reglamento Europeo de Protección de Datos"

Tampoco el requisito de inequívoco surge de la norma argentina, lo cual abre un gran abanico de posibilidades donde el consentimiento podría ser interpretado como otorgado, aunque no fuera realmente la voluntad del sujeto. Al no contar con este requisito como necesario para su validez, en esas situaciones el consentimiento sería valido y por ende el tratamiento que se hubiera realizado en consecuencia también.

Para males, el Art.5 de la ley implícitamente da su beneplácito para que la solicitud del consentimiento para el tratamiento de datos personales se encuentre embebida en cualquier otro texto que refiera a otra temática, pudiendo ser términos y condiciones para la prestación de un servicio o un contrato de adhesión. Mientras se cumpla con el deber de información que fija el Art. 6 de la misma ley y que se encuentre destacada la solicitud de consentimiento, el modo de obtención estaría alineado con la norma.

Es cierto que la ley argentina tiene varias deficiencias, que con el correr de los años se han vuelto más patentes conllevando a la necesidad de una reforma de esta. El 30 junio del año 2023 el Proyecto de ley fue finalmente elevado a estudio por el Congreso de la Nación, donde espera ansioso ser aprobado.

Dentro de las distintas mejoras que propone se encuentra la ampliación de las bases legales para el tratamiento de datos personales, asemejándose al Reglamento General de Protección de Datos. Otra importante mejora relacionada con el objeto de estudio de este trabajo es la incorporación mediante el Art. 14 de una definición más completa y exhaustiva del consentimiento, los requisitos que debe tener y una explicación del significado de cada uno de estos. En ese sentido indica que "(…) se requiere que este sea expreso, previo, libre, especifico, informado e inequívoco, para una o varias finalidades determinadas ya sea mediante una declaración o una clara acción afirmativa"[22], evidenciando un avance significativo en lo que a obtención del consentimiento implica, conllevando a los Responsables de datos personales a equiparar esfuerzos a aquellos sujetos a normativa europea si quieren tratar datos bajo este proyecto de ley.

Lamentablemente la normativa argentina tampoco ha evolucionado hacia la promulgación de una ley que regule de manera específica las comunicaciones electrónicas, lo que sería una suerte de paralelismo a la Directiva de Privacidad y Comunicaciones

[22] Artículo 14 del Proyecto de ley del 29 de junio de 2023, mensaje 2023-87-APN-PTE sobre "Ley de Protección de los datos personales"

Electrónicas. Por lo que las plataformas digitales deben regirse por la vieja Ley 25.326 que, teniendo al menos 23 años de retraso tecnológico, es el único parámetro con el que se cuenta para operar en Argentina.

III. Desafíos y tendencias actuales en la protección de datos personales de las plataformas digitales para la obtención del consentimiento.

Con este escenario legislativo el gran desafío de los Responsables de bases de datos de las plataformas digitales es lograr cumplir con el principio de transparencia, de forma tal que el consentimiento pueda ser reputado válido conforme los requisitos y muy específicas características que previamente enuncié.

La falta de un consentimiento válido repercute en un gran perjuicio tanto para el titular de los datos personales como para el Responsable, quien no se podrá valer de ese dato para llevar adelante la actividad procesadora para la cual recolectó el dato y teniendo que asumir sanciones económicas impuestas por tribunales administrativos e indemnizaciones por condenas judiciales ante posibles reclamos de los Titulares de datos personales o autoridades gubernamentales.

A esto se le suma que los titulares de datos personales son quienes brindan la información propia y muchas veces ajena, quienes a su vez comparten la información obtenida de las plataformas digitales. En estos casos el consentimiento puede que no se haya brindado por los terceros involucrados de manera indirecta, sea para brindar su información como para que sea publicada y compartida con otros. No obstante, el Responsable tiene la obligación de demostrar que obtuvo esos datos fundamentados en un base legitima para el procesamiento, y si esa base es el consentimiento se encontraría en una posición difícil.

Recordando el principio de responsabilidad proactiva (accountability) es el Responsable de la base de datos personales quien debe arbitrar las medidas técnicas y organizativas para asegurar la protección del dato y principalmente la legitimidad de ese dato. Es quien debe evaluar qué medidas tomará para obtener un consentimiento válido.

Ahora bien, en el ecosistema digital esto prueba ser un punto complejo, como demostrar que la persona del otro lado de la pantalla tiene la capacidad para comprender los

alcances del tratamiento al cual está consintiendo. Esto sin adentrarme en una problemática más compleja sobre el sujeto, quien puede ser un menor o una persona con discapacidad intelectual, problemática que merece un análisis independiente. Aún sin tomar en consideración estos supuestos, tratándose de una persona adulta con pleno uso de sus capacidades cognitivas tendría que evaluarse el grado de comprensión que tiene en la materia.

Me atrevería a decir que la mayoría de los usuarios de las distintas plataformas digitales son iliteratos con relación al procesamiento de su información y a los derechos que tienen en su calidad de titulares de datos personales. La falta de formación y conciencia en la importancia que reviste el compartir datos personales y su procesamiento conlleva a que el consentimiento que se brinde en esos términos carezca de sustancia.

Esto no podría ni debería endilgarse a los Responsables del tratamiento de datos personales, por más claros y específicos que puedan ser los avisos de privacidad y solicitudes de consentimiento muchas veces el cabal entendimiento del tema implica un nivel de conocimiento que el usuario promedio no tiene. En base al informe de la Oficina australiana de la Comisión de información sobre la encuesta realizada en el año 202023 en relación a la actitud adoptada por la comunidad australiana en torno a la privacidad, la revista de la Academia de ciencias de marketing publica un artículo dónde concluye que el 58% de los usuarios no comprenden lo que las firmas hacen con los datos que recolectan, y el 49% sienten que son incapaces de proteger su información por falta de conocimiento o tiempo, así como por la complejidad que implica. 24.

Lo que denota que los titulares de datos personales desconocen cuáles son sus derechos en torno a sus datos y mucho más grave es que consientan sin saber realmente sobre que consienten.

[23] Australian Community Attitudes to Privacy Survey 2020. Office of the Australian Information Commissioner, https://www.oaic.gov.au/__data/assets/pdf_file/0015/2373/australian-community-attitudes-to-privacy-survey-2020.pdf

[24] Sara Quach, Park Thaichon, Kelly D. Martin, Scott Weaven & Robert W. Palmatier (2022) "Digital technologies: tensions in privacy and data", Journal of the Academy of Marketing Science, Ed Springer

A su vez la velocidad de la propia dinámica tecnológica en el uso de las plataformas implica acciones rápidas para acceder al contenido deseado, ¿cómo pretender que un titular de datos personales dedique tiempo específico educarse, comprender y entender la información que se le presenta?

En marzo de 2022 el Comité europeo de protección de datos publicó los lineamientos sobre "Patrones obscuros en las plataformas digitales, cómo reconocerlas y evitarlas", posteriormente en febrero de 2023 el Comité europeo de protección de datos actualizó esos lineamientos que prevén buenas prácticas para los Responsables de datos personales para reconocer y evitar el uso de patrones engañosos y oscuros.[25]

Estos patrones son aquellos que interfieren en la experiencia del usuario de las plataformas digitales a fin de influenciar a que el usuario tome decisiones inintencionadas, sin darle un mayor análisis en su perjuicio atentando indirectamente contra la autonomía de su voluntad. Se dividen en 6 categorías, siendo la primera "overloading" que apunta a aquellas interacciones que imponen al usuario grandes cantidades de solicitudes, información, opciones y posibilidades que generan que el titular de datos personales comparta más datos o permita inintencionalmente el procesamiento de datos contrario a sus expectativas.

Si bien esta guía concluye con un anexo con recomendaciones sobre buenas prácticas para evitar estos patrones engañosos, en relación con la categoría "overloading" resulta de particular interés a los fines de este trabajo ya que denota las vicisitudes que deben afrontar los Responsables de plataformas digitales al obtener el consentimiento diseñando interfaces alineadas al RGPD en defensa de los titulares de datos personales a quienes busca otorgar mayor control sobre sus datos y facilitar el ejercicio de sus derechos.

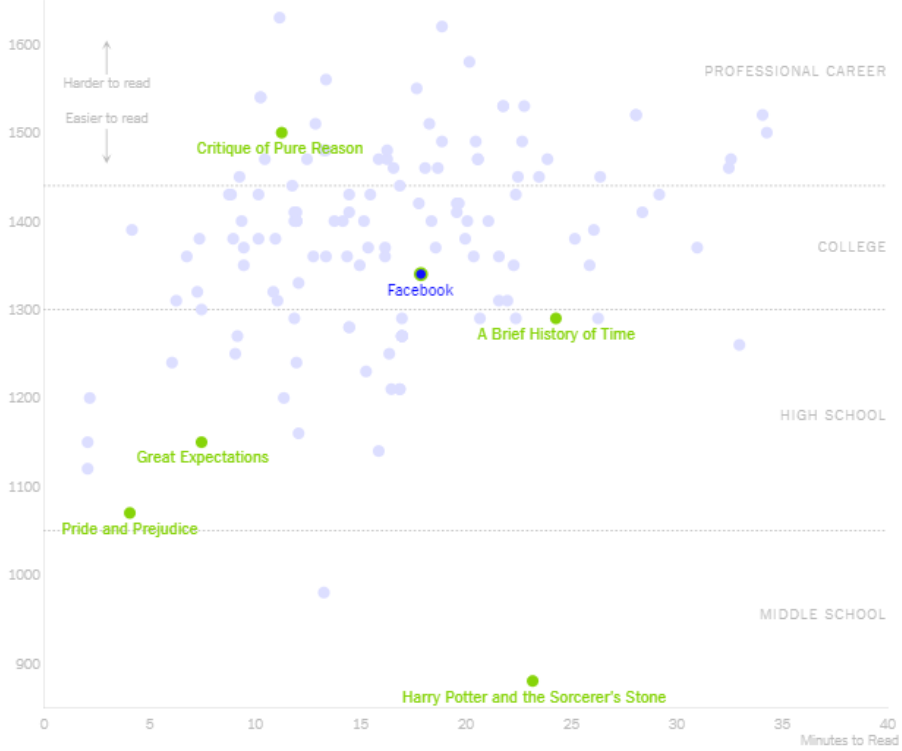
Otra de las cuestiones relacionadas que se presenta en los entornos digitales es la "fatiga del consentimiento", ya Solove había hecho su aporte en ese sentido, indicando que la sobreinformación y la solicitud constante para varios propósitos cuando es sumamente detallada y segmentada termina siendo en perjuicio del titular de datos personales. Éste se encuentra en una situación de agotamiento y la consecuencia es que desestime la

[25] Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them

información que tiene a su disposición, aceptando todo sin realizar una evaluación de los riesgos que asume al tomar esa decisión.

A fin de cuentas, este perjuicio también resulta en detrimento del Responsable de Datos Personales ya que volverá a estar en una situación de incumplimiento, puesto que el Titular de Datos personales no estaría informado y su consentimiento carecería de eficacia. En función del Art. 7(4) del Reglamento General de Protección de Datos, queda en cabeza del Responsable de Datos Personales demostrar que cumple con la legislación vigente, entonces el consentimiento brindado ante la imposibilidad de acceder al contenido de la plataforma por un exceso de información que limite severamente la experiencia del usuario parecería ser una situación difícil de defender.

El diario New York Times publicó un artículo en junio de 2019 en base a un estudio realizado por Kevin Litman-Navarro en el cual se analizo 150 avisos de privacidad de distintas plataformas digitales de renombre, llegando a la conclusión que en su mayoría eran de difícil comprensión. Para llegar a este resultado tomó la prueba de Lexile desarrollado por la compañía Metrametrics que indica el grado de comprensión de palabras de un texto necesario para acceder a determinado nivel educativo, en la gran mayoría de los casos las políticas de privacidad excedían las 1440 palabras fijadas según la mencionada prueba como necesarias para un profesional como ser un abogado o médico. El cuadro que sigue ejemplifica la comparación que se hizo entre los avisos de privacidad y algunas obras literarias más renombradas:



El único que se destaco por su simpleza y corta extensión fue el aviso de privacidad de la BBC que transcribo a continuación:

> *"Tenemos una razón válida para utilizar tu información personal. Se llama base 'legal para el procesamiento'. A veces podemos pedirte permiso para hacer cosas, como cuando te suscribís a un correo electrónico. Otras veces, cuando vos esperarías de manera razonable que nosotros utilicemos tu información personal, no te pedimos permiso, pero solo cuando la ley dice que esta bien que la usemos y se ajusta a los derechos que tenés"*[26]

Resta ver si este muy breve aviso de privacidad puede entenderse que cumple con los lineamientos establecidos por la Regulación General de Datos Personales o quizás caiga en el dilema de brindar información simple, pero a su vez insuficiente y por ende no cumplir con el derecho de información de los titulares de datos personales

Esto pone de relevancia la problemática de cumplimiento de brindar información precisa y completa informado que datos se recabaran, porque y para que, y a su vez que la misma sea brindada de una forma clara y comprensible para el titular de datos personales.

El principio de responsabilidad proactiva (accountability) no es enunciado en la Ley 25.326, al menos de manera expresa, sin embargo en el RGPD fija este principio y en las Directrices establece que "es obligación de los responsables del tratamiento de datos encontrar nuevas soluciones que funcionen dentro de los parámetros de la ley y que respalden mejor la protección de datos personales y los intereses de los titulares de los datos "[27], por lo tanto los Responsables son quienes tienen la obligación de demostrar que su cumplieron los preceptos legales, invirtiendo así la carga de la prueba.

De acuerdo con la Directiva de Privacidad y Comunicaciones Electrónicas europea clarifica y amplia la necesidad de solicitar el consentimiento en los dispositivos donde sea posible utilizar la huella digital como medio de autenticación, que igualmente estarán regidos por las normas sobre uso de "cookies". Por lo tanto, previo a poder utilizar el

[26] Kevin Litman-Navarro (2019) "*We Read 150 Privacy Policies. They Were an Incomprehensible Disaster*"., The Privacy Project. Ed. New York Times. Nueva York, USA
[27] Directrices sobre el consentimiento en el sentido del Reglamento (EU) 2016/679, pág. 3)

método de identificación en necesario solicitar al usuario su consentimiento para almacenar ese dato personal.

La Directiva de Privacidad y Comunicaciones Electrónicas continua en el mismo sentido requiriendo el consentimiento previo de los usuarios para recibir comunicaciones con fines de marketing, temperamento opuesto al establecido por la legislación argentina donde se permite la comunicación para fines de marketing directo sin el consentimiento del usuario. La elección es posterior al envío de la comunicación, esto es una vez recabado el dato y procesado es que el usuario puede optar por ser excluido.

Esto saca a relucir otra dificultad aparejada a la obtención del consentimiento, esto es que según cada ordenamiento tendrá distintas reglas de juego. Hay normas que protegen a sus ciudadanos, otras que son de aplicación para los Responsables establecidos en esa jurisdicción y otras en algunos casos tienen aplicación extraterritorial que puede llegar a entrar en colisión con la normativa local. A esto se suma que hay muchos temas que no están regulados, generado lagunas legales que son suplidas por normas generales que probablemente no hayan previsto tener ese alcance y que tienen deficiencias propias de no haber tenido presente esa temática al momento de legislar.

Las distintas apreciaciones sean por diversas legislaciones u opiniones jurisprudenciales no uniformes sobre cómo debe ser la obtención del consentimiento, lleva a criterios distintos que complejizan la operatoria comercial. Ya que parecería que no hay una solución o respuesta genérica y uniforme que pueda ser aplicable a la problemática. Por el contrario, parecería ser que el Responsable de la base de datos deberá analizar caso por caso como implementar una solución, lo que prueba ser bastante complejo e ineficiente si se toma en consideración el volumen de la circulación de datos y la velocidad con que lo hacen.

Otra complejidad que trae aparejada el consentimiento es que los titulares de datos personales deben poder retractarse. El Decreto N.º 1558/01 que reglamenta la Ley 25.326 sobre protección de datos personales reza así:

> *ARTICULO 5: El consentimiento informado es el que está precedido de una explicación, al titular de los datos, en forma adecuada a su nivel social y cultural, de la información a que se refiere el artículo 6 de la Ley N 25.326. La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES*

establecerá los requisitos para que el consentimiento pueda ser prestado por un medio distinto a la forma escrita, el cual deberá asegurar la autoría e integridad de la declaración. El consentimiento dado para el tratamiento de datos personales puede ser revocado en cualquier tiempo. La revocación no tiene efectos retroactivos.[28]

Entonces, además de obtener el consentimiento cumpliendo los recaudos del Art. 6 de la Ley de protección de datos personales de Argentina debe preverse la posibilidad de retirarlo en cualquier momento. En ese sentido la RGPD en su Art. 7(3) sigue esta misma línea donde el titular de datos puede retractar su consentimiento en cualquier oportunidad, debiendo ser informado de tal posibilidad previo a que el titular de datos personales otorgue su consentimiento y sin que esto afecte la legalidad del tratamiento que se haya dado previo a la retractación.

No obstante, agrega un detalle más, el consentimiento debe ser tan fácil de revocar como lo fue de otorgarse.[29] Los lineamientos de la Comisión europea sobre el consentimiento a la luz de la RGPD precisan mayores detalles sobre la cuestión:

"Retiro del consentimiento:

113. El Articulo 7(3) del RGPD prescribe que el Responsable debe asegurar que el consentimiento pueda ser retractado por el Titular de datos personales tan fácilmente como lo fue brindarlos y en cualquier oportunidad. El RGPD no establece que brindar y retractar el consentimiento deben ser realizado por medio de la misma acción.

114. Sin embargo, cuando el consentimiento es obtenido valiéndose de medios electrónicos a través de un clic del mousse, deslizar o presionar una tecla, el titular de datos debe, en la práctica, poder retirar su consentimiento con una simplicidad equivalente. Cuando el consentimiento se obtenido por intermedio del uso de un servicio de interfase de usuario especifico (por ejemplo una web, una aplicación, una cuenta a la que hay que identificarse, la interfase de un dispositivo de servicio de Internet of Things o de un correo

[28] Decreto Nacional N.º 1558/01 reglamentario de la Ley 25.326 sobre protección de datos personales de Argentina.
[29] Artículo 7(3) del Reglamento General de Protección de Datos del Parlamento Europeo y el Consejo Europeo del 27 de Abril de 2016, (Regulation 2016/679)

electrónico), no hay duda que el titular de datos personales debe poder retirar su consentimiento por intermedio de la misma interfase, ya que cambiar a otra interfase por el solo motivo de poder retirar el consentimiento requeriría un esfuerzo innecesario. Asimismo, el titular de datos personales deberá poder retirar su consentimiento sin ningún perjuicio. Esto significa, entre otras cosas, que el Responsable de los datos personales debe hacer posible la retractación del consentimiento sin costo alguno ni disminuir el nivel de servicios.''[30]

De acuerdo con la Directiva de Privacidad y Comunicaciones Electrónicas europea este principio también aplica a las cookies, para las cuales hay que obtener el consentimiento de los usuarios previo a su uso y la posibilidad también de retirar el consentimiento en cualquier momento y oportunidad con la misma facilidad con la que se pudo otorgar. También especifica que cuando los usuarios o suscriptores hayan brindado su consentimiento para el procesamiento de datos de geolocalización y otro tráfico de datos, tales usuarios o suscriptores deben continuar teniendo la posibilidad de rechazar temporalmente el tratamiento de dichos datos por cada conexión a una red y para cada transmisión de una comunicación utilizando medios simples y libres de cargos.

Todo ello lleva a preguntarse como obtener y conservar los datos que generan una ganancia comercial y una ventaja competitiva con beneficios económicos por medio de la monetización de los datos y a su vez cumplir con este variopinto mosaico de expresiones jurídicas.

[30] Directrices sobre el consentimiento en el sentido del Reglamento (EU) 2016/679. Traducción de mi autoría "Withdrawal of consent: 113. Article 7(3) of the GDPR prescribes that the controller must ensure that consent can be withdrawn by the data subject as easy as giving consent and at any given time. The GDPR does not say that giving and withdrawing consent must always be done through the same action. 114. However, when consent is obtained via electronic means through only one mouse-click, swipe, or keystroke, data subjects must, in practice, be able to withdraw that consent equally as easily. Where consent is obtained through use of a service-specific user interface (for example, via a website, an app, a log-on account, the inter-face of an IoT device or by e-mail), there is no doubt a data subject must be able to withdraw consent via the same electronic interface, as switching to another interface for the sole reason of withdrawing consent would require undue effort. Furthermore, the data subject should be able to withdraw his/her consent without detriment. This means, inter alia, that a controller must make withdrawal of consent possible free of charge or without lowering service levels".

IV. Recomendaciones prácticas para las empresas y los usuarios para abordar estos desafíos "Best Practices".

El objetivo del Responsable de Datos Personales es obtener los datos para su utilización bajo un cometimiento válido. Es mi entender que esto podría probar ser de muy difícil cumplimiento, ya que demostrar que obtuvo un consentimiento válido significaría conocer la identidad del titular de datos personales para corroborar si el aviso de privacidad que presenta es lo suficientemente comprensible, no obstante, debe ser lo suficientemente detallado. Verificar que efectivamente ese titular de datos personales se encuentra con capacidades suficientes para brindar su consentimiento de forma válida y lograr informar a ese titular de datos personales cuales son sus derechos y como ejercerlos. Todo esto sin que ese aviso de privacidad resulte innecesariamente disruptivo. Y aun así subsistiría la duda ya que los avisos de privacidad no son negociables, por ende, tampoco podría haber brindado su consentimiento de manera libre.

De ahí que mi primera conclusión sería considerar el tratamiento de datos personales en base al consentimiento como base legal muy frágil y eventualmente efímera en el tiempo. Esto también teniendo en cuenta la facultad que tiene el titular de datos personales de ejercer su derecho de retractación, evitando que sus datos se utilicen desde ese momento en adelante, particularmente cuando hay varias opiniones que sugieren renovar periódicamente la solicitud de consentimiento para poder demostrar que este sigue siendo vigente.

La propuesta inicial sería entonces que el Responsable de los datos personales realice un examen a conciencia sobre la actividad procesadora de datos y determine cual sería la base legal apropiada para el tratamiento, buscando apoyarse en otra que no sea el consentimiento. De esta manera la propia actividad, los desarrollos que se realicen para obtener los datos y las mismas plataformas estarán enfocadas en demostrar otra base legal que haga necesaria la recolección y tratamiento de los datos personales sin necesidad de requerir el consentimiento del titular de datos personales.

Esto no significa de modo alguno que considere que se debe restar control y autonomía a los titulares de datos personales, por el contario considero que la privacidad de los datos personales sobre todo en el uso de las plataformas digitales resulta un tema harto

complejo y a través de la solicitud de un consentimiento a un titular de datos que probablemente carezca del conocimiento técnico necesario para realizar una evaluación de riesgo acabada. Tendría más sentido que sea el Responsable de los datos personales quien realice esta evaluación y de acuerdo con los fines proyectados establezca una base legal "real" y que asegure efectivamente la privacidad de los titulares de datos personales y la tranquilidad para el Responsable de los datos personales que puede tratarlos y monetizarlos mientras subsista esa base legal que lo habilitó a su recolección inicial.

BIBLIOGRAFÍA.

Australian Community Attitudes to Privacy Survey 2020. Office of the Australian Information Commissioner, https://www.oaic.gov.au/__data/assets/pdf_file/0015/2373/australian-community-attitudes-to-privacy-survey-2020.pdf

Elettra Bietti, (2020) "*Consent as a Free Pass: Platform Power and the Limits of the Informational Turn*", Nueva York, USA. Ed. Pace Law Review, Volume 40, Issue 1 Article 7.

Bridewell (2022) "*10 Ways GDPR Will Impact Your Business Operations – Part 1*", England. Ed. Bridewell.

Privacy and Electronic Communications Directive 2002/58/EC (ePrivacy Directive).

CNFContAdm, Sala V, 3-jul-2018, "Torres Abad Carmen c/ Estado Nacional s/ habeas data"

Decreto Reglamentario 1558/2001, sobre la Ley de Protección de Datos Personales de Argentina.

Cade Diehm, Kelsey Smith, Ame Elliott and Georgia Bullen (2021) *"The Limits to Digital Consent: Understanding the risks of ethical consent and data collection for underrepresented communities"*. New York, USA, Ed. Simply Secure and The New Design Congress.

Directive 2002/58/EC of the European Parliament and of the Council, amended by Directive 2006/24/EC and Directive 2009/136/EC of the European Parliament and of the Council.

Directive 2009/136/EC of the European Parliament and of the Council.

Eduardo Ferreyra (2019) "E*l RGPD y la ley argentina de protección de datos personales. Análisis comparativo"*, Bs As, Argentina. Ed. Asociación por los Derechos Civiles.

Deliberación SAN-2022-025 del 29 de diciembre de 2022 de Comisión Nacional de Tecnologías de la Información y Libertades (https://www.legi-france.gouv.fr/cnil/id/CNILTEXT000046907077)

General Data Protection Regulation (Regulation 2016/679)

Guidelines 05/2020 on consent under Regulation 2016/679, European Data Protection Board.

Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them. European Data Protection Board

González Allonca, Juan Cruz - Ruiz Martínez, Esteban (2016) "*Big Data: riesgos y desafíos en el tratamiento masivo de datos personales*". 1 - LA LEY2016-B, 1051, Buenos Aires, Argentina Ed Thomson Reuters.

Handbook on European data protection law (2018), Luxembourg. European Union Agency for Fundamental Rights and Council of Europe.

Eleni Kosta (2013) *"Consent in European Data Protection Law"*, Paises Bajos . Ed. Martinus Nijhoff Publishers.

Eleni Kosta, Irene Kamara, Ronald Leenes (2022) "*Research Handbook on EU Data Protection Law",* UK. Edward Elgar Publishing Limited.

Kari Koskinen, Carla Bonina & Ben Eaton (2018) "*Development Implications of Digital Economies Paper No. 8 Digital Platforms in the Global South: Foundations and Research Agenda*", UK. Ed. Centre for Development Informatics Global Development Institute, SEED University of Manchester,

Ley 25326, Ley de Protección de Datos Personales de Argentina, publicada en el Boletín Oficial de la República Argentina del 30 de octubre de 2000.

Philip Leith, (2015) "*Privacy in the Information Society",* UK. Ed. Taylor & Francis.

Kevin Litman-Navarro (2019) "*We Read 150 Privacy Policies. They Were an Incomprehensible Disaster*"., The Privacy Project. Nueva York, USA. Ed. New York

Times. (https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html?mtrref=undefined&gwh=640DFC0A6D64EA7398EA228FC9080A59&gwt=pay&assetType=)

Moerel, E.M.L. and Prins, J.E.J. (2016) *"Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things"*. Tilburg, Países Bajos. Ed. Tilburg Institute for Law, Technology, and Society.

Opinion 05/2019, European Data Protection Board

Palazzi, Pablo, (2006) "*El consentimiento para el tratamiento de datos personales (Opt-in versus opt-out bajo el régimen de la Ley 25326)*", Bs. As., Argentina. Ed. Jurisprudencia Argentina, 2006-II-379,.

Proyecto de Ley de Protección de Datos Personales del 29 de junio de 2023, mensaje 2023-87-APN-PTE

Sara Quach, Park Thaichon, Kelly D. Martin, Scott Weaven & Robert W. Palmatier (2022) "Digital technologies: tensions in privacy and data", Journal of the Academy of Marketing Science, Ed Springer

REAL ACADEMIA ESPAÑOLA: *Diccionario de la lengua española*, 23.ª ed., [versión 23.6 en línea]. <https://dle.rae.es> [29/07/2023].

Oxford University Press. (2003). "Oxford Dictionary of Law," University of Oxford. Pag 106

Spinello, Richard A. (2011). *"Privacy and Social Networking Technology".* The International Review of Information Ethics, Vol 16. Edmonton, Canada, Ed. International Center for Information Ethics University of Alberta

Solove, Daniel J. (2023) *"Murky Consent: An Approach to the Fictions of Consent in Privacy Law"*. Boston University Law Review, N° 114. Boston, USA. Ed. Boston University

Utz Chistine, Degeling Martin, Fahl Sascha, Schaub Florian and Holz Thorsten (2019) *"(Un (informed Consent: Studying GDPR Consent Notices in the Field",* London United Kingdom. Ed. ACM SIGSAC