

PRIVACIDAD Y BLOCKCHAIN^{1 2}

PRIVACY AND BLOCKCHAIN

Santiago Grigera del Campillo³ ()*

“Privacy is the power to selectively reveal oneself to the world”³

Eric Hughes.

RESUMEN: La tecnología nos ha cambiado la vida en todo sentido. Estamos más conectados que nunca antes en la historia, lo que implica que también estamos más expuestos que nunca. Los datos han revolucionado todas las industrias, hasta las más tradicionales. Para evitar arrepentirnos en el futuro de nuestras conductas actuales debemos tomar cartas en el asunto. ¿Será Blockchain la tecnología que empodere al usuario nuevamente?

PALABRAS CLAVES: Privacidad- criptografía- Big data- aprendizaje automático- Inteligencia artificial- Blockchain- identidad digital- Autodeterminación informativa- Blockchain permissionadas- Derechos de protección de datos.

ABSTRACT: Technology has changed our lives in every way. We are more connected than ever before in history, which means that we are also more exposed than ever. Data has revolutionized all industries, even the most traditional. To avoid regretting our current behaviors in the future, we must take action on the matter. Will Blockchain be the technology that empowers the user again?

KEY WORDS: Privacy- cryptography- Big data- machine learning- Artificial intelligence- Blockchain- digital identity- Informative self-determination- Permissible Blockchain- Data protection rights.

¹ Artículo recibido el 25 de marzo de 2021 y aprobado para su publicación el 30 de junio de 2021

² El presente es trabajo presentado se realizó en el marco de la DIPLOMATURA EN TECNOLOGÍA BLOCKCHAIN APLICADA A LOS NEGOCIOS Y LAS RELACIONES JURIDICAS, en el año 2019.

³ (*) Abogado (UNC). Especialista en Derecho Informático (Universidad de Buenos Aires). Profesor en la Diplomatura en Tecnología Blockchain aplicada a los negocios y las relaciones (UCCOR), Profesor en Diplomatura de Derecho Digital: Herramientas teóricas prácticas (Acción Jurídica). Prosecretario de la Sala de Derecho y Tecnología del Colegio de Abogados de Córdoba. Maestrando en Derecho de la Ciberseguridad y entorno digital, Universidad de León, España.

³ Eric Hughes (1993). A Cypherpunk's Manifesto. Traducción: “La privacidad es el poder de revelarse selectivamente al mundo”. Recuperado de <https://www.activism.net/cypherpunk/manifesto.html> consultado el 24/04/2020.



Artículo publicado bajo Licencia Creative Commons Atribución-No Comercial-Sin Derivar. ©
Universidad Católica de Córdoba

DOI [http://doi.org/10.22529/rbia.2021\(2\)02](http://doi.org/10.22529/rbia.2021(2)02)

“Llueven datos. De redes sociales, tarjetas de crédito, teléfonos, celulares, páginas web y buscadores, dispositivos GPS, relojes inteligentes, rastreadores satelitales, análisis clínicos, cámaras de fotos y cualquier otro objeto interconectado electrónicamente. Y ante tanta lluvia, las reacciones son dispares.” Así comienza el capítulo introductorio del libro “big data” de Walter Sosa Escudero⁶. Evidentemente estamos inmersos en un mar de datos. Cada persona gestiona no menos de 15 cuentas, perfiles, contraseñas y demás información a diario. En la era de la datatización e información, producimos, reproducimos, almacenamos y consumimos contenido en inmensas cantidades. Con tantos frentes abiertos a menudo se nos hace difícil poder hacer una correcta gestión de nuestra privacidad. Nadie conoce con exactitud dónde está nuestra información, quién accede a ella, qué usos y tratamientos se realizan sobre la misma.

¿Qué tipo de información existe sobre nosotros online? La realidad es que es imposible saberlo. La información que subimos voluntariamente a internet, con seguridad no es lo único que existe. Empresas, gobiernos, sistemas informáticos y terceros ajenos también producen información que nos incumbe. Algoritmos y máquinas realizan prácticas de data mining que elaboran perfiles impredecibles e inaccesibles sin que lo sepamos y eso también habla de nosotros, nos define e identifica. Nuestra identidad digital está conformada no sólo por lo que proporcionamos a internet sino también por lo que generan, interpretan o conciben los demás como consecuencia de nuestra interacción en la red. Con las búsquedas que realizamos, sitios a los que accedemos, noticias o foros donde nos unimos e interactuamos, perfiles que visitamos, imágenes que comentamos; vamos dejando rastros invisibles al ojo humano pero que engrosa una huella que alimenta bases de datos extrañas.

La privacidad en la actualidad es un privilegio que no muchos se pueden dar el gusto de disfrutar, al menos en la vida online.

La noción de privacidad concebida como un derecho inherente a toda persona humana, ha sido foco de grandes debates a lo largo de la historia. Aún hoy resulta difícil

⁶ Sosa Escudero Walter (2019). “big data”. pp 19. Siglo Veintiuno Editores Argentina S.A. 3ra Edición. Ciudad Autónoma de Buenos Aires.

encontrar un concepto que satisfaga todas sus acepciones y complejidades que trae aparejada. A fines de los 60's y junto con la evolución de la tecnología y el surgimiento de internet la concepción de privacidad ha ido mutando, haciéndose cada vez más difusa y compleja. No ha sido sino después del escándalo de Cambridge Analytica y Facebook, que muchas personas, Gobiernos y privados han empezado a ser más conscientes de lo que suben a internet.

Según Palazzi, la privacidad es un concepto complejo y sujeto a distintas visiones legales, históricas, económicas y sociológicas. No hay en el derecho comparado unanimidad sobre este concepto, sus fundamentos, sobre cuál debe ser su ámbito de aplicación y cuáles son sus límites⁷.

Ha quedado en evidencia como consecuencia de la pandemia del coronavirus que dependiendo las costumbres, historias y realidades sociales la concepción de privacidad varía en los distintos países. Podemos observar las medidas de países orientales totalmente intrusivas- según la perspectiva de privacidad de países occidentales - en cuanto a la gestión y control de la pandemia. Países como China, Taiwán, Singapur o Corea del Sur, desde principios de la crisis sanitaria obligaron a sus ciudadanos a la utilización de aplicaciones donde se podían hacer seguimientos por GPS de sus puntos de contacto, ubicación y en algunos casos, pueden acceder a información de la temperatura corporal en tiempo real de los ciudadanos, calificando el riesgo como alto, moderado o bajo para poder ingresar a un local o salir a la vía pública. Contrariamente, países como España, por trabas y discusiones relacionadas a las normativas robustas aplicables en materia de privacidad, tardaron algunos meses en acceder al seguimiento por GPS pero con algunas garantías tomando como recaudos que los datos estuvieran anonimizados. Hasta un grupo de profesionales expertos en privacidad y seguridad enviaron una carta al Gobierno⁸ con recomendaciones para la

⁷ Palazzi Pablo A. (2019). Delitos contra la intimidad informática. pp 19. 1ra edición CABA, Argentina. CDYT colección Derecho y Tecnología

⁸Recuperado de https://www.eldiario.es/tecnologia/privacidad-Gobierno-iniciativas-tecnologicas-coronavirus_0_1007900137.html. Consultado el 25/04/2020.

implementación de medidas tecnológicas durante la pandemia. Misma postura tomaron países como Bélgica, Austria y Alemania⁹.

En el libro *Understanding privacy* del autor Daniel J. Solove¹⁰ refiere a distintas concepciones destacadas respecto del término privacidad recopiladas a lo largo de la historia. Por mencionar dos de ellas que no son de su autoría se destacan- en una versión traducida- “el corazón de nuestra libertad” y el “comienzo de toda libertad”.

En un sentido similar, una autora local, Johanna Caterina Faliero ha escrito: “El anonimato y la privacidad son expresiones de nuestra libertad y autodeterminación informativa, y genuinos derechos humanos, fundamentales, esenciales irrenunciables y basales en la era digital en la que estamos inmersos”¹¹.

Si bien como referimos anteriormente, la privacidad es un derecho fundamental receptado por todos los países, ni la constitución de EEUU ni la Argentina mencionan la palabra “privacidad” en sus respectivas Cartas Magnas. Tampoco lo menciona el CCCN sin perjuicio que existen múltiples normas que aluden a ello. En el Código Penal Argentino, la palabra “privacidad” se menciona una sola vez en el epígrafe del Capítulo III, Título V “Delitos contra la Libertad” y fue introducida mediante la ley de delitos informáticos Nro.26.388, en el año 2008. Por último, aunque parezca sorprendente tampoco se menciona la palabra en cuestión en la ley 25326 de protección de los datos personales.

Diversos tratados, declaraciones y plexos normativos a nivel internacional reconocen a la privacidad, por ejemplo, el artículo 12 de Declaración Universal de los Derechos Humanos, establece:

⁹ Recuperado de <https://www.top10vpn.com/news/surveillance/covid-19-digital-rights-tracker/>. Consultado el 25/04/2020.

¹⁰ Daniel J. Solove (2008). *UNDERSTANDING PRIVACY*. pp. 1-11, Cambridge, Mass.: Harvard University Press, Cambridge, Massachusetts London, England 2008, recuperado de: https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2075&context=faculty_publications, consultado el 23/04/20.

¹¹ Faliero Johanna Caterina (2019). “El anonimato: epítome de la seguridad informática y privacidad en el ecosistema crypto”. Artículo compilado en “Fintech: Aspectos Legales”. Tomo I. pp 101-102. Ed. CDYT Derecho y Tecnología. Ciudad Autónoma de Bs As.

“Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.”

En el derecho constitucional local resaltan los arts 18 y 19 CN:

“...El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación...”

“Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe.”

La Cuarta Enmienda de EEUU establece:

“El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas.”

Se ha escrito mucho al respecto de los alcances de esta enmienda y ha habido casos realmente relevantes en la historia americana como por ejemplo, “Katz” y “Carpenter”. La conclusión sin perjuicio de la complejidad del análisis que excede este trabajo, redundante en que existe una expectativa razonable de privacidad en el uso de la tecnología.

Habiendo dado un panorama para nada suficiente de distintas acepciones de la privacidad, reconociendo que puede abarcar otros tantos aspectos como circunstancias intervenga una persona -en su sentido amplio-, es momento de definir qué entiende nuestra ley por base de datos, registro o archivo. La respuesta la encontramos en el artículo 2 de la ley 25.326: Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su

formación, almacenamiento, organización o acceso. El mismo artículo entre otros conceptos, también define al “responsable” como a la persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.

A pesar de la vasta normativa local sobre privacidad, en lo que hace a su faz digital y específicamente a los datos personales, da la sensación que nuestros derechos van menguando a medida que avanza la tecnología. Simplemente entiendo que no son lo suficientemente protegidos. Al menos no como en otras partes del mundo como en los países europeos donde hay un régimen sancionatorio robusto, serio, considerando a la privacidad desde el diseño y por defecto.

En nuestro país rige una ley con casi 20 años de antigüedad y con sanciones por incumplimiento ínfimas que lejos de disuadir, resulta más conveniente no respetar la ley desde que se pueden obtener ganancias absurdas con un tratamiento desmedido de datos personales. Evitando entrar en ese análisis, lo cierto es que todos estos conceptos tienen relevancia actualmente por que los optimistas consideramos que el desorden y despilfarro informativo podría encontrar una respuesta interesante a partir de la tecnología Blockchain.

Blockchain, fue concebida para realizar transacciones de manera anónima, transparente, inmutable, segura, trazable y despojada de arbitrariedades o de un control central, como ocurre con las grandes redes sociales.

Hay esperanza que blockchain ayude a recomponer la identidad digital de las personas empoderando al titular de los datos. Distintos especialistas en tecnología y privacidad coinciden sobre este tema. Por ejemplo, se podría identificar la trazabilidad de los consentimientos proporcionados por los titulares, y las cesiones de información entre distintas partes, circunstancia que en la actualidad, poco se respeta.

Resulta muy ilustrativa a este respecto la entrevista realizada por el Prof. Solove a Steve Shillingford, donde se explican las bondades de Blockchain en materia de privacidad¹². Se

¹² Solove Daniel (2018). “Why Blockchain Is a Game-Changer for Privacy: An Interview with Steve Shillingford”. Recuperado de: <https://teachprivacy.com/why-blockchain-is-a-game-changer-steve-shillingford/>. Consultado el 25/04/2020.

transcriben algunos fragmentos sin perjuicio que se invita a su lectura en el link citado: “...La tecnología de cadenas de bloques puede eliminar la necesidad de que las empresas y otras organizaciones mantengan repositorios centralizados de datos de identificación. También permitiría que los usuarios tengan un control permanente sobre quién puede acceder a sus datos...” (...) “El blockchain le da a una persona la capacidad de publicar solo la información que decida divulgar. Nada más y nada menos. Y no más agendas ocultas, no vender datos personales sin su consentimiento, no preocuparse por la privacidad.

Un artículo publicado en el sitio MIT Technology Review¹³, vaticina un futuro similar. Agrega que sistemas como Bitcoin, que usa criptografía y una red de ordenadores para facilitar el intercambio seguro de monedas digitales sin un intermediario, pueden hacer algo similar para las credenciales de identidad. Varios emprendimientos están desarrollando este tipo de proyectos como Evernym y UPort.

Como se advierte existen razones para pensar que un ecosistema donde el titular pueda ser protagonista de sus datos e información con capacidad para decidir y conocer qué ocurre desde que presta su consentimiento para los distintos tratamientos parece un verdadero cambio de paradigma y resulta prometedor.

Guiados por la corriente del Reglamento General de Protección de Datos Europeo, las nociones de Privacidad desde el diseño y por defecto, cobran vital relevancia para que las organizaciones tengan como foco y prioridad de la privacidad del usuario en todas las etapas del proyecto. Por supuesto que a primera impresión parecería que la tecnología blockchain y los datos personales pueden no ser del todo compatibles, pero actualmente se están llevando a cabo proyectos muy interesantes que desafían estas aseveraciones. Una empresa fundada por Rand Hindi, un joven emprendedor tecnológico, desarrolló dispositivos IOT similares a los lanzados por las grandes tecnológicas como Amazon y Google pero con un enfoque

¹³ Mike Orcutt (2017). “Blockchain' podría derrocar a las contraseñas y devolver la identidad digital sus usuarios”. Recuperado de: <https://www.technologyreview.es/s/9821/blockchain-podria-derrocar-las-contrasenas-y-devolver-la-identidad-digital-sus-usuarios>. Consultado el 25/04/2020.

proteccionista de la información personal de los usuarios. “Cuando comienzas a combinar la criptografía tradicional con el aprendizaje automático, con Blockchain, puedes ofrecer exactamente lo mismo que la gente hace centralmente absorbiendo tus datos en sus servidores, pero de una manera completamente descentralizada y completamente privada.” Fragmento de entrevista realizada por “criptovest.com” a Rand Hindi sobre su empresa SNIPS¹⁴.

De todos modos, no podemos ignorar que, encontrándose esta tecnología en pleno desarrollo, aún existen ciertos debates respecto del ejercicio de algunos derechos de protección de datos personales en países con normativas más estrictas (RGPD) como los europeos, cuestiones que serán abordadas en otro artículo. Para terminar la idea, existe un compromiso para encontrar una solución pacífica en el debate y se han conformado diversos organismos de investigación que se abocan a estudiar y ver de qué manera pueden adaptarse la realidad tecnológica con las leyes.

¹⁴ Recuperado de <https://cryptovest.com/news/interview-rand-hindi-of-snips-shares-thoughts-on-privacy-blockchain-and-more/>, Consultado el 27/04/20.