Doutrina Estrangeira

LA DICOTOMÍA DE LA ÉTICA Y LA LEGALIDAD DE LOS DATOS PERSONALES EN APLICACIONES DE CONTACTO

Teresa Vargas Osorno

Doctora Cum Laude en Derecho de la Universidad Complutense de Madrid, España. Abogada de la Universidad Externado de Colombia. Es Directora y Docente del Departamento de Derecho Informático de la Universidad Externado de Colombia.
E-mail: tvargas@uexternado.edu.co

Jhon Caballero Martínez

Abogado de la Universidad Externado de Colombia y Docente Investigador en el Departamento de Derecho Informático de la misma casa de estudios.
E-mail: jhon.caballero@uexternado.edu.co

Resumen: La tecnología de rastreo de contactos y productos sanitarios digitales se ha convertido en uno de los mecanismos para monitorear a los individuos y alertar rápidamente si han estado en proximidad con alguien que ha resultado contagiado con un virus. El texto presenta un análisis de los aspectos relacionados con el derecho a la privacidad y el conflicto que surge frente al principio de legalidad, para así proponer por un modelo de gobernanza de los datos basado en un marco ético-legal de referencia, el cual se ajuste al principio de responsabilidad demostrada en la implementación y funcionamiento de herramientas tecnológicas.

Palabras clave: protección de datos, ética digital, privacidad, tecnología sanitaria, gobernanza, principio de legalidad.

I Introducción

El distanciamiento social ha sido el mecanismo histórico efectivo para hacerle frente a los contagios de una pandemia,[1] pero en razón a los avances tecnológicos

[1] MUSINGUZI, Geofrey y OPPONG ASAMOAH, Benedict. The Science of Social Distancing and Total Lock Down: Does it Work? Whom does it Benefit? *Electronic Journal of General Medicine*. 2020, Vol. 17, núm. 6. ISBN 2516-3507. p. 2.

sobre analítica de datos, procesamiento de la información y masificación del uso de dispositivos móviles, algunos Estados han adoptado tecnologías de contacto para monitorear a los individuos y alertar rápidamente si han estado en proximidad con alguien que ha resultado contagiado con un virus. Sin embargo, algunos autores manifiestan que el emplear este mecanismo presenta brechas frente a la protección de los derechos individuales, en particular, la equidad, la igualdad y la privacidad.[2]

La solución que la doctrina propone es la adopción de prácticas éticas en el tratamiento de los datos personales que implica el uso de esta tecnología, pero lo que se denomina "pautas éticas" en el derecho norteamericano, no tiene la misma aplicación en el derecho latinoamericano por las limitaciones que impone el principio de legalidad.[3] Por tanto, la investigación pretende encontrar un marco ético jurídico que se ajuste a la naturaleza del ordenamiento de la región y permita aplicar políticas efectivas para una adecuada rendición de cuentas.

Así, se realiza un recuento histórico sobre el origen de la analítica de datos y por qué es importante considerar el arraigo histórico y social para entender las interpretaciones que tiene el derecho a la privacidad en los diversos ordenamientos jurídicos del mundo, y conforme al cual, se explica la noción de privacidad y la trasformación que conlleva el tratamiento de datos personales desde sus orígenes hasta la aparición de tecnologías que permitieron el procesamiento automatizado de los mismos. Luego, se ahonda sobre la dicotomía entre la moral y el derecho, en donde se encuentra un punto de concurrencia que permite la aplicación de la ética digital en aspectos normativos, y a su vez, identifica una serie de etapas para una adecuada gobernanza de la información personal, de conformidad con el principio de responsabilidad demostrada y la debida diligencia.

De acuerdo a la diferenciación entre ética y derecho, se propone un marco ético-legal de referencia para aplicar a la tecnología de rastreo de contactos digitales y productos sanitarios digitales (DCTT) que se ajusten a las buenas prácticas, pero también a las previsiones del ordenamiento jurídico. Se sugieren estrategias y aspectos a tener en cuenta para una adecuada implementación de tecnología y el consecuente tratamiento de datos personales ajustado al ordenamiento y las buenas prácticas.

---

[2] Cf. MORLEY, Jessica, *et al*. Ethical guidelines for COVID-19 tracing apps. Nature Publishing Group, Jun. 2020, Vol. 582, núm. 7810, p. 29–31. DOI 10.1038/d41586-020-01578-0.

[3] RUMOLD, Mark. *Evaluación de la legalidad y proporcionalidad de la vigilancia de las comunicaciones en la legislación de Estados Unidos*, 2016, p. 6 y ss.

II La analítica de datos y el concepto de ética digital

La analítica de datos se remota a la demarcación de las paredes o del suelo para señalar el trascurrir de los días. No obstante, con la llegada de la escritura, el tratamiento de datos se puede rastrear hasta 3200 a.C. en Mesopotamia, donde se llevaba a cabo el registro transaccional de operaciones comerciales.[4] Posteriormente, en el Egipto faraónico del año 3000 a.C., se identificó el tratamiento de información demográfica por parte del Estado, en donde los censos resultaban de la mayor importancia para tomar decisiones entorno a los impuestos y la guerra.[5]

En la historia previa a la promulgación de los derechos fundamentales, la privacidad era analizada por los involucrados en las matemáticas y la filosofía, por lo que las discusiones a lo largo de la edad media se enfocaron en la espiritualidad y la interioridad presente en el alma o mente. El filósofo griego Platón, planteó la interioridad como una relación entre el reconocimiento y la valoración personal, de tal suerte que los lideres eran descritos como personajes de evolución espiritual y ética,[6] y a su vez, Sócrates difundía el principio "conócete a ti mismo" en las escuelas socráticas, así que se evidencia la búsqueda por la interioridad perfeccionada con el objetivo de obtener sabiduría eterna.[7] Por su parte, Immanuel Kant indicó frente a la privacidad "que el individuo puede ser tratado como el dueño de sus habilidades y derechos morales"[8] de la misma manera que ocurre con las mercancías, por lo que se puede denotar la asociación de un carácter mercantil a la privacidad.

Luego, posturas como las que planteó Ferdinand Schoeman fueron trasformando dicha concepción, al expresar que es más conveniente considerar a la privacidad "como un valor independiente de su característica de proteger a las personas de un imperfecto mundo",[9] de forma tal que la privacidad se convirtió en un valor asociado al ser humano en sí mismo. De hecho, Edward Bloustein señaló que la privacidad se asocia con la dignidad humana e individualidad, en donde identificó casos de vulneración en la intrusión de los asuntos privados, la

4 KELLEHER, John D.; TIERNEY, Brendan. Data science. Cambridge, MA: The MIT Press, 2018, 5 y ss..

5 *Ibíd*. 5 y ss.

6 SCOGLIO, Stefano. Transforming privacy: a transpersonal philosophy of rights. Westport: Praeger, 1998. p. 37.

7 SCOGLIO, Stefano. Transforming privacy: a transpersonal philosophy of rights. Westport: Praeger, 1998. p 38.

8 RICHARDSON, Janice. Law and the Philosophy of Privacy. New York: Routledge, 2017, 20.

9 SCHOEMAN, Ferdinand. Privacy and intimate information. En: SCHOEMAN, Ferdinand (ed.), Philosophical Dimensions of Privacy. Cambridge: Cambridge University Press, pp. 403–418. DOI 10.1017/cbo97805 11625138.018, 404.

divulgación pública sobre hechos vergonzosos, la publicidad de aspectos en la espera pública o la apropiación del nombre o semejantes.[10]

Las corrientes utilitaristas promulgadas por Jeremy Bentham a lo largo del siglo XIX en el derecho anglosajón, conllevaron a la adopción de una postura de maximización a fin de alcanzar la mayor felicidad por parte del mayor número de personas, de manera que la privacidad se vio permeada por el "principio de utilidad", que junto al auge del liberalismo, promulgó por el "individualismo adquisitivo", de acuerdo con el cual se protege la esfera privada de los individuos y su libertad de decisión, pero se excluye el acceso a la información personal del carácter constitucional.[11]

Por su parte, Asía se vio influenciada por la corriente del comunitarismo, en donde resalta especialmente el patriotismo y la espiritual emocional que trasciende los elementos personales, por lo que en este contexto no se trata de la individualidad, si no del ejercicio de la privacidad considerando la vida pública y el sentimiento de interés público.[12]

La idea del tratamiento de datos se empezó a gestar por la probabilidad, entendida como una disciplina para la recopilación y análisis de datos, que con posterioridad acuñó la terminología de la ciencia de datos, hacia mediados del siglo XIX.[13] Uno de los principales exponentes en la materia fue el ingeniero William Playfair, quien presentó gráficos estadísticos y las bases de la exploración de datos,[14] pero con la llegada de la segunda guerra mundial, hay una aceleración de los desarrollos científicos en el área informática, cuya principal innovación para 1940 fue la computadora diseñada por Alan Turing, la cual permitió realizar cálculos estadísticos más complejos.

Desde 1948 se empiezan a presentar los primeros proyectos sobre redes neuronales, que terminan fundando las bases de la inteligencia artificial en 1960. Es aquí cuando aparece el *machine learning,* que con el avance en materia técnica, ha permitido alcanzar nuevos adelantos como el *deep learning neural networks*, la *machine vision* y el procesamiento del lenguaje natural.[15]

[10] BLOUSTEIN, Edward J. Privacy as an aspect of human dignity: an answer to Dean Prosser. En: Philosophical Dimensions of Privacy. Cambridge University Press, pp. 156–202. DOI 10.1017/cbo9780511625138.007.

[11] SCOGLIO, Stefano. Transforming privacy: a transpersonal philosophy of rights. Westport: Praeger, 1998. pp. 26 y ss.

[12] SCOGLIO, Stefano. Transforming privacy: a transpersonal philosophy of rights. Westport: Praeger, 1998, pp. 43 y ss..

[13] HALD, Anders. A history of probability and statistics and their applications before 1750. Hoboken N.J: Wiley, 2003. 3 y ss.

[14] KELLEHER, John D. y TIERNEY, Brendan. *Data science*. Cambridge, MA: The MIT Press, 2018. ISBN 9780262347020. p. 12.

[15] KELLEHER, John D. y TIERNEY, Brendan. *Data science*. Cambridge, MA: The MIT Press, 2018. ISBN 9780262347020. p. 14.

El auge del capitalismo llevó a la expansión de la privacidad, en donde el control de la información personal se convirtió en una discusión de relevancia, tanto así, que para 1990 las empresas notaron que habían acumulado tal cantidad de datos, que les era imposible analizarla en detalle, por lo que los esfuerzos tecnológicos en analítica de datos se enfocaron en el desarrollo de capacidad de relacionamiento entre bases de datos y su optimización.[16] La importancia sobre el tratamiento de los datos personales ha ganado importancia gracias a que el volumen de los datos se ha incrementado, cada vez hay más variedad de datos y la velocidad de procesamiento ha mejorado notablemente.[17]

Así las cosas, la privacidad puede ser entendida "como un estado o condición de acceso limitado a una persona",[18] que por su carácter descriptivo y prescriptivo involucra el ejercicio de derechos fundamentales como la intimidad, la autonomía, la libertad y el libre desarrollo de la personalidad. Así mismo, debido a su carácter subjetivo, entraña un carácter personalísimo y espiritual,[19] en la medida que cada quien decide el alcance y dimensión de la misma.

Desde la noción filosófica planteada por Stefano Scoglio, la privacidad es "el lugar para cultivar y experimentar (aunque sea parcialmente) el sentido de nuestra universalidad y santidad interior, porque la privacidad es el retiro de las condiciones y apegos particulares de uno y por lo tanto hacia nuestro yo menos condicionado y por lo tanto más universal",[20] pero al no existir una visión jurídica universal de privacidad, el desarrollo de su contenido se ha visto permeado por las bases históricas que dejan como consecuencia conflictos de privacidad entre las interpretaciones desarrolladas por Estados Unidos, Europa Occidental y China, en donde lo que debe considerarse como privado presenta interpretaciones diferenciales.[21]

De acuerdo con lo expuesto por James Whitman, la privacidad distingue aspectos que involucran la dignidad humana y el desenvolvimiento de la libertad, en donde el núcleo esencial de la privacidad se compone de los derechos a la propia imagen, el nombre y la reputación, lo cual resultó insuficiente, por lo que se presente el derecho a controlar la información sobre sí mismo, que es básicamente

[16] KELLEHER, John D. y TIERNEY, Brendan. Data science. Cambridge, MA: The MIT Press, 2018. p. 8.
[17] KELLEHER, John D. y TIERNEY, Brendan. Data science. Cambridge, MA: The MIT Press, 2018. p. 9.
[18] SCHOEMAN, Ferdinand. Privacy and intimate information. En : SCHOEMAN, Ferdinand (ed.), Philosophical Dimensions of Privacy. Cambridge : Cambridge University Press, p. 403–418. DOI 10.1017/cbo9780511625138.018. p. 3.
[19] SCOGLIO, Stefano. Transforming privacy: a transpersonal philosophy of rights. Westport : Praeger, 1998. p. 29.
[20] SCOGLIO, Stefano. *Transforming privacy*: a transpersonal philosophy of rights. Westport: Praeger, 1998. p. 42.
[21] WHITMAN, James Q. The Two Western Cultures of Privacy: Dignity versus Liberty. *Yale Law Journal*. 2004, Vol. 113. DOI 10.2139/ssrn.476041. p. 1155.

el llamado derecho a la autodeterminación informativa de raíces alemanas.[22] En tal sentido, quienes administran datos derivados del ejercicio del derecho a la privacidad, tienen el potencial de afectar a los titulares con exposición no deseada, humillaciones, discriminación o perfilamiento no deseado.

Por otra parte, la ética digital encuentra relevancia por los dilemas de la segunda guerra mundial, en donde los científicos que desarrollaron la bomba atómica se preguntaron sobre la responsabilidad de su uso y los riesgos que implicaba ponerla en manos de un ser humano,[23] por lo que se trata de un antecedente notable sobre las graves consecuencias que presentó la tecnología y las limitaciones que el desarrollo científico debe tener en primacía de los principios y garantías fundamentales que el derecho natural impone. De ahí que James H. Moor la definiera como "el análisis de la naturaleza y el impacto social de la tecnología informática",[24] con el objetivo de enfatizar sobre la formulación y justificación del uso de la tecnología para la consecución de un proyecto.

De acuerdo con esta definición preliminar, un marco ético se refiere no solo a las consideraciones teóricas respecto de las consecuencias de un proyecto, sino también sobre la claridad en la puesta marcha, por lo que se requiere seguridad sobre un plan de acción y una respuesta en cuanto a las posibles consecuencias que tendrían que enfrentarse en diversas circunstancias. No obstante, las consideraciones éticas tienen lugar sobre la incertidumbre de una situación, de manera que aquellos hechos que plantean campos de acción claros y seguros no consideran estos cuestionamientos con un enfoque moral.

Lo anterior plantea una maleabilidad lógica que refiere que la tecnología sirve para transmitir pensamientos, de forma tal que impacta la concepción filosófica, que para Marx se representaba en el carácter colectivo de la propiedad de los bienes, mientras que para Kant y Betham, las teorías éticas se refieren al reconocimiento del ser humano como individuo independiente, el cual toma decisiones racionales en medio de la existencia de un contrato social.[25] Para mediados del siglo XX, las nociones de ética derivaban de desarrollos filosóficos locales, pero se presentaban discusiones que se referían a la posibilidad de

[22] WHITMAN, James Q. The Two Western Cultures of Privacy: Dignity versus Liberty. *Yale Law Journal* [en línea]. 2004, Vol. 113. DOI 10.2139/ssrn.476041. p. 1161.

[23] WIENER, Norbert. *The human use of beings*. Vol. 140. [S. l.]: [s. n.], 1965. ISBN 1853430757. DOI 10.1097/00005053-196501000-00001. p. XXVII.

[24] MOOR, James. Whats is computer ethics? *Metaphilosophy*. John Wiley & Sons, Ltd, Oct. 1985, Vol. 16, núm. 4, pp. 266–275. DOI 10.1111/j.1467-9973.1985.tb00173.x.

[25] GORNIAK-KOCIKOWSKA, Krystyna. The computer revolution and the problem of global ethics. *Science and Engineering Ethics*. Opragen Publications, 1996, Vol. 2, núm. 2, pp. 177–190. DOI 10.1007/BF025 83552.

considerar una ética de la sociedad de la información de carácter global,[26] lo cual se logró con la intervención de la innovación en la guerra y la masificación de internet.

Desde entonces, las cuestiones éticas derivadas del uso de la tecnología dejaron de ser campo de acción de la ética informática, para dar lugar a la filosofía de la información como disciplina encargada de analizar los cambios sociales por la evocación de desarrollos tecnológicos y la transformación de un mundo analógico a un mundo digital.[27] De ahí que autores como Luciano Floridi y Deborah G. Johnson se refieran a la relación epistémica que los seres humanos tienen con las tecnologías de la información,[28] en la medida que la acción humana tiene importancia moral en el uso, tratamiento y destrucción de información.[29]

La doctrina en la materia indica que la ética aplicada expone el concepto de transparencia como una forma de reconocer y valorar el diseño de una tecnología, cuyo eje trasversal es la privacidad como un derecho propio con valor intrínseco. Sin embargo, la adopción de tecnologías en el marco de la transformación digital ha facilitado que se recopilen cada vez más datos personales, de modo que se presenta ambigüedad sobre el tratamiento y alcance del consentimiento.[30] Es de la mayor importancia tener en cuenta los antecedentes descritos, en la medida que las discusiones sobre la privacidad y ética se remontan los precedentes históricos que se han visto marcados por características propias del contexto social.

III El conflicto de la moral y el derecho

La recopilación de datos personales por medio de aplicaciones es un asunto tan pretérito como el nacimiento de los teléfonos inteligentes sobre los cuales se realiza el etiquetamiento de comportamientos, mediante el análisis de archivos, contactos y localización.[31] Ello es posible gracias a la inclusión del número IMEI

[26] BYNUM, Terrell Ward. Computer ethics: Its birth and its future. *Ethics and Information Technology*. Kluwer Academic Publishers, 2001, Vol. 3, núm. 2, p. 109–112. DOI 10.1023/A:1011893925319. p. 111.

[27] CASTAÑO, Daniel. La gobernanza ética de los sistemas de inteligencia artificial y la agencia humana. En : HENAO, Juan Carlos y CASTAÑO, Daniel (ed.), *Transformación digital, disrupción tecnológica y sociedad*. Bogotá : Universidad Externado de Colombia. En proceso de publicación. p. 18

[28] FLORIDI, Luciano. *Philosophy and computing: an introduction*. London: Routledge, 1999. ISBN 0415180244. p. 18.

[29] JOHNSON, Deborah. Computer ethics. En : FLORIDI, Luciano (ed.), *The Blackwell Guide to the Philosophy of Computing and Information*. Nueva Jersey: Blackwell Publishing Ltd, 2004. p. 67.

[30] JOHNSON, Deborah. Computer ethics. En : FLORIDI, Luciano (ed.), *The Blackwell Guide to the Philosophy of Computing and Information*. Nueva Jersey: Blackwell Publishing Ltd, 2004. pp. 70 y 71.

[31] ENCK, William, *et al*. TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones. *OSDI'10: Proceedings of the 9th USENIX conference on Operating systems design and implementation*. 2010, pp. 393–407. DOI 10.5555/1924943.

(como identificador único), la *sim card*, los dispositivos de posicionamiento global (GPS) integrados, el *bluetooth*, la cámara (para captar imagen y video), el micrófono (para captar audio), sumado a la posibilidad de integrar redes sociales o cuentas de servicios tecnológicos, conllevan a un perfilamiento cada vez más preciso de los usuarios para identificar patrones e intereses.

El desarrollo de modelos de identificación en sociedades democráticas había tenido un mayor enfoque hacia la publicidad y el mercadeo que sobre la vigilancia estatal en sí misma, por lo que la finalidad aludida por las empresas tecnológicas obedece, por lo general, a la necesidad de personalización para conocer a los usuarios y sus intereses de consumo.[32] Así pues, los flujos de seguimiento que emplean información personal han tenido cierta aceptación jurídica desde la visión del derecho privado, en tanto que los ordenamientos jurídicos reconocen la autonomía de la voluntad y el aforismo del *pacta sunt servanda* en el negocio jurídico.[33]

Esta visión contractualista fue la que adoptó el derecho constitucional en América Latina para hacer frente al perfeccionamiento del consentimiento de cara al derecho a la autodeterminación informática, en donde se observa una política de privacidad como un mecanismo de autorregulación, de tal suerte que su aceptación representa el consentimiento del titular frente al tratamiento de sus datos personales.[34] No obstante, la presentación de estas cláusulas ha resultado problemática, en la medida que se trata de un contrato de adhesión que no garantiza su cumplimiento y resulta extenso e incómodo en lectura.

Al respecto, la región ha seguido el estándar europeo, conforme a la influencia de la Red Iberoamericana de Protección de Datos (RIPD) y la identificación de afinidades respecto del contexto constitucional.[35] Si bien la iniciativa buscó reunir las propuestas y políticas locales para así promulgar una declaración uniforme, al final la regulación se demarcó en el derecho nacional, por lo que hay países que han adoptado principios, derechos y deberes frente al tratamiento de datos personales, así como otros, en donde el régimen de protección brilla por su ausencia.

De ahí que exista confusión respecto a la aplicación de la ética digital en el campo de la privacidad, en tanto que, en los esquemas robustos de protección,

[32] LI, Jing, *et al*. A personalized requirement identifying model for design improvement based on user profiling. *Artificial Intelligence for Engineering Design, Analysis and Manufacturing*. Cambridge University Press (CUP), Febrero 2020, Vol. 34, núm. 1, pp. 55–67. DOI 10.1017/s0890060419000301.

[33] HINESTROSA, Fernando. *Tratado de las obligaciones II: de las fuentes de las obligaciones: negocio jurídico*. Bogotá: Universidad Externado de Colombia, 2015. p. 122.

[34] REMOLINA ANGARITA, Nelson. *Tratamiento de datos personales: Aproximación internacional y comentarios a la ley 1581 de 2012*. Bogotá: Legis, 2013. ISBN 9789587670868. p. 21.

[35] RED IBEROAMERICANA DE PROTECCIÓN DE DATOS. *Reglamneto de la RIPD*, 2003.

la ética ha venido a ser un complemento al carácter prescriptivo del derecho positivo. Mientras que en los ordenamientos que no reconocen protección jurídica a los datos, la ética de la privacidad se ha enmarcado como una de las buenas prácticas para ganar la confianza de usuarios.

Al respecto, es menester recordar lo que indicó Hans Kelsen sobre la diferenciación entre una regla de derecho y una regla moral, ya que la primera cuenta con un carácter prescriptivo de deber establecido por el derecho positivo, pero "desde que una norma moral es aplicada en virtud de una norma jurídica adquiere, por tal circunstancia, el carácter de una norma jurídica".[36] Es decir, el ordenamiento jurídico puede autorizar la aplicación de normas morales, pero por el sólo hecho de hacerlo, se convierte en una regla de derecho. A su vez, Lon Fuller manifestó en cuanto al análisis de la moral interna del derecho, que si bien la moral puede ayudar y dar eficacia al derecho, "no deberá hacernos creer que puede adoptarse cualquier fin substancial sin comprometer la legalidad".[37]

De conformidad con los principios liberales y democráticos, se instaura la manifestación del poder constituyente como reconocimiento de la soberanía del pueblo, en donde la Constitución Política es la manifestación de una norma jurídica, y como tal, expresa un catálogo de principios y derechos fundamentales.[38] En esta medida, el principio de legalidad es uno de los principios primordiales del Estado de Derecho, el cual "constituye una limitación a la actividad de la administración, por cuanto significa que ella no puede hacer cuanto quiera sino solamente aquello que le permita la ley",[39] por lo que el establecimiento de aplicaciones de contacto y el tratamiento de datos personales realizado por el Estado debe ceñirse a lo establecido por el ordenamiento jurídico y no a las prácticas morales delimitadas por la ética digital.

Conforme lo señala Carlos Lara, las cuestiones éticas "han permitido entregar uno o varios marcos de referencia frente a posibilidades de desarrollo tecnológico que involucran riesgos altos. Sin embargo, todavía se trata de iniciativas de sistematización de directrices no obligatorias, de adopción ideal pero no imperativa", por lo que este autor sugiere acudir a los instrumentos internacionales para completar los vacíos regulatorios existentes.

---

[36] KELSEN, Hans. *Teoría pura del derecho*. Buenos Aires: Editorial Eudeba, 2015. ISBN 9789502308869. p. 45.

[37] FULLER L., Lon. *La moral del derecho*. Ciudad de México: Editorial F. Trillas, 1964.

[38] RAMÍREZ CLEVES, Gonzalo. Teoría de la constitución, constitución y poder constituyente. En: CORREA HENAO, Magdalena, OSUNA PATIÑO, Néstor y RAMÍREZ CLEVES, Gonzalo (ed.), *Lecciones de derecho constitucional*. Bogotá: Universidad Externamdo de Colombia, 2017. pp. 33 y 77.

[39] RODRÍGUEZ, Libardo. *Derecho administrativo: general y colombiano*. Bogotá: Editorial Temis, 2017. ISBN 9789583511486. p. 105.

En consecuencia, lo que parte de la doctrina norteamericana ha denominado "pautas éticas", no tiene la misma aplicación en el derecho latinoamericano por las limitaciones que impone el principio de legalidad.[40] Sin embargo, ello no obsta para que no se consideren cuestiones éticas en el tratamiento de datos personales, en la medida que el ordenamiento jurídico previó el principio de responsabilidad demostrada –*accountability*– como uno de los mecanismos adicionales al marco legal para garantizar una adecuada protección.[41] En tal sentido, la normativa se extiende a las políticas y procedimientos internos del responsable del tratamiento para que se produzca una efectiva rendición de cuentas frente a la autoridad de datos personales,[42] y de esta manera, se establezca un Programa Integral de Gestión de Datos Personales, en el cual las cuestiones éticas tienen la gran importancia.[43]

Al respecto, el profesor Daniel Castaño indica que "las regulaciones generales de protección de datos personales son insuficientes para garantizar el derecho a la privacidad frente a los retos derivados de su procesamiento automatizado",[44] razón por la cual es necesario considerar la existencia de una intersección donde concurren principios éticos y jurídicos.[45] De acuerdo con tal postura, la privacidad en la función administrativa requiere del "diseño e implementación de herramientas o métodos 'X-por-diseño' (X= Legalidad, Privacidad o Ética Digital) para integrar la legalidad, la privacidad y la ética digital dentro de las tecnologías",[46] por lo que el componente de ética de la privacidad se integra al diseño de la tecnología en atención al principio de responsabilidad demostrada y no al componente normativo de derecho.

En concordancia con lo anterior, la profesora Carolina Aguerre se refiere a dicha intersección como un marco de gobernanza necesario, en donde la modularidad por capas facilita la transparencia al tener en cuenta la dimensión

[40] RUMOLD, Mark. *Evaluación de la legalidad y proporcionalidad de la vigilancia de las comunicaciones en la legislación de Estados Unidos*. [S. l.]: [s. n.], 2016, pp. 6 y ss.

[41] ARTICLE 29 DATA PROTECTION GROUP. *Opinion 3/2010 on the principle of accountability*, 2010. Disponible en : https://www.dataprotection.ro/servlet/ViewDocument?id=654. Acceso en: 13 jun. 2020.

[42] ARTICLE 29 DATA PROTECTION GROUP. *Opinion 3/2010 on the principle of accountability*, 2010. Disponible en : https://www.dataprotection.ro/servlet/ViewDocument?id=654. Acceso en: 13 jun. 2020.

[43] PERILLA, Mario y RAMÍREZ, Daniel. *Guía para la implementación del principio de responsabilidad demostrada en el tratamiento de datos personales*. [S. l.] : [s. n.], 2015.

[44] CASTAÑO, Daniel. La gobernanza de la Inteligencia Artificial en América Latina: entre la regulación estatal, la privacidad y la ética digital. En: AGUERRE, Carolina (ed.), *Inteligencia Artificial en América Latina y el Caribe. Ética, Gobernanza y Políticas*. Buenos Aires: CETyS Universidad de San Andrés, 2020. p. 9.

[45] CASTAÑO, Daniel. La gobernanza de la Inteligencia Artificial en América Latina: entre la regulación estatal, la privacidad y la ética digital. En: AGUERRE, Carolina (ed.), *Inteligencia Artificial en América Latina y el Caribe. Ética, Gobernanza y Políticas*. Buenos Aires: CETyS Universidad de San Andrés, 2020. p. 3.

[46] CASTAÑO, Daniel. *GovTech: Legalidad, Privacidad y Ética Digital*. Bogotá : Alcaldía Mayor de Bogotá, 2019. ISBN 9789585251618. p. 17.

técnica de los algoritmos, la ética y los aspectos jurídicos.[47] De modo tal que la ética se diferencia de los aspectos legales, pero confluye con la gobernanza de datos que implica "la disponibilidad, la usabilidad, la integridad y la seguridad de los datos".[48]

De hecho, una publicación del Banco Interamericano de Desarrollo destacó la gestión ética de los datos como una forma de reivindicar la percepción del sector público y la rendición de cuentas, en donde se considera a la privacidad como un derecho protegido por el ordenamiento jurídico, pero también se resalta la importancia de contar con marcos de referencia que consideren nuevas precauciones y derechos digitales.[49] De esta manera, dentro del marco normativo de protección de datos es posible prever marcos de referencia, que si bien tratan cuestiones morales, se adhieren a una norma jurídica convirtiéndose en derecho positivo.

En el entretanto y mientras hay mayores discusiones sobre el tema, en América Latina la aplicación de buenas prácticas se circunscribe al principio de responsabilidad demostrada, el cual pretende la mitigación de los riesgos y la protección de las garantías fundamentales a través del cumplimiento de los principios establecidos por el ordenamiento jurídico. Así pues, los marcos éticos en la gobernanza de los datos permiten añadir escalabilidad al cumplimiento normativo y demuestran con claridad la adopción de medias proactivas para proteger la privacidad.[50]

Sin embargo, el advenimiento del *accountability* modifica el alcance legal y lo amplia, ya que este principio no se somete únicamente a los principios coexistentes, sino a los riesgos que implica el manejo de información personal.[51] De ahí que se haga énfasis en la rendición de cuentas y la intervención de la autoridad de protección de datos, puesto que como lo señala Stefano Rodotà, "los

[47] AGUERRE, Carolina. Estrategias nacionales de IA y gobernanza de datos en la región. En: AGUERRE, Carolina (ed.), *Inteligencia Artificial en América Latina y el Caribe. Ética, Gobernanza y Políticas*. Buenos Aires : CETyS Universidad de San Andrés., 2020. pp. 3 y 4.

[48] AGUERRE, Carolina. Estrategias nacionales de IA y gobernanza de datos en la región. En: AGUERRE, Carolina (ed.), *Inteligencia Artificial en América Latina y el Caribe. Ética, Gobernanza y Políticas*. Buenos Aires : CETyS Universidad de San Andrés., 2020. p. 5.

[49] BUENADICHA SÁNCHEZ, César, *et al*. *La gestión ética de los datos*. Washington D.C.: Banco Interamericano de Desarrollo, marzo 2019. DOI 10.18235/0001623. pp. 6, 8 y 25.

[50] DEMETZOU, Katerina. GDPR and the concept of risk: The role of risk, the scope of risk and the technology involved. En : *IFIP Advances in Information and Communication Technology*. Vol. 547 [en línea]. Springer New York LLC, 20 agosto 2019, p. 137–154. [Consultado el 23 junio 2020]. ISBN 9783030167431. DOI 10.1007/978-3-030-16744-8_10. p. 143.

[51] DEMETZOU, Katerina. GDPR and the concept of risk: The role of risk, the scope of risk and the technology involved. *IFIP Advances in Information and Communication Technology*. Vol. 547. New York: Springer LLC, 20 ago. 2019, p. 137–154. ISBN 9783030167431. DOI 10.1007/978-3-030-16744-8_10. p. 145.

datos personales siguen siendo una 'necesaria utopía'",[52] por lo que los principios democráticos y las cuestiones éticas se han convertido en una necesidad para enfrentar la erosión de los principios que rigen el sistema de protección de datos personales.[53]

En esta medida, "la rendición de cuentas constituye el último intento de encontrar una solución para una gama irresolublemente compleja de cuestiones",[54] pero como lo indica Charle Raad, los criterios que determinan la demostración del cumplimiento se fijan con participación de terceros y reguladores externos, cuyas valoraciones presentan diferencias materiales y conceptuales de acuerdo con el contexto en el que se desarrolla el tratamiento de la información.[55] De hecho, el principio de responsabilidad demostrada reviste tal importancia que además de fundir como garantía del cumplimiento de los deberes de protección de datos, es construido a la par por la jurisprudencia y la autoridad de datos personales.[56]

Al respecto, el profesor Paul De Hert asocia la definición de *accountability* a la responsabilidad ética, puesto que lo que pretende el principio es "mejorar el rendimiento general de las personas y las organizaciones mediante el desarrollo y la promoción de instrumentos responsables y conocimientos profesionales",[57] lo cual se expresa con un mandato ético de gobernanza a modo de rendición de cuentas. De ahí que el cumplimiento de la responsabilidad demostrada se materialice con la aplicación de políticas de privacidad vinculadas a criterios externos y la puesta en marcha de mecanismos para la toma de decisiones en una gestión ética de los datos personales,[58] en donde la adopción de certificados, el mejoramiento de estructura administrativa y la capacitación de los trabajadores son mecanismos para demostrar una gobernanza de datos adecuada en derecho.[59]

---

[52] RODOTÀ, Stefano. Data Protection as a Fundamental Right. En: GUTWIRTH, S.; POULLET, Y.; DE HERT P.; DE TERWANGNE, C.; NOUWT, S. (Ed.)., *Reinventing Data Protection?* Netherlands: Springer, 2009, pp. 77–82. DOI 10.1007/978-1-4020-9498-9_3. p. 78.

[53] RODOTÀ, Stefano. Data Protection as a Fundamental Right. En: GUTWIRTH, S.; POULLET, Y.; DE HERT P.; DE TERWANGNE, C.; NOUWT, S. (Ed.)., *Reinventing Data Protection?* Netherlands: Springer, 2009, pp. 77–82. DOI 10.1007/978-1-4020-9498-9_3. p. 78.

[54] GUAGNIN, Daniel, *et al*. Introduction. En: *Managing Privacy through Accountability*. London: Palgrave Macmillan, 2012. ISBN 9781349350452. p. 6.

[55] RAAD, Charles. The Meaning of 'Accountability' inthe Information Privacy Context. En: *Managing Privacy through Accountability*. London : Palgrave Macmillan, 2012. ISBN 9781349350452. p. 26.

[56] CASTAÑO, Daniel. Nudge + código. Una arquitectura digital para el precedente judicial. En : RINCÓN CÓRDOBA, Jorge (ed.), *Las trasformaciones de la administración pública y del derecho administrativo*. Bogotá: Universidad Externado de Colombia, 2019. p. 259.

[57] DE HERT, Paul. Accountability and SystemResponsibility: New Concepts in Data Protection Law andHuman Rights Law. En: *Managing Privacy throughAccountability*. London: Palgrave Macmillan, 2012. p. 195.

[58] CENTRE FOR INFORMATION POLICY LEADERSHIP AT SECRETARIAT TO THE GALWAY PROJECT. *Data Protection Accountability: The Essential Elements A Document for Discussion*. [S. l.]: [s. n.], 2009.

[59] GUAGNIN, Daniel, *et al*. Introduction. En: *Managing Privacy through Accountability*. London: Palgrave Macmillan, 2012. ISBN 9781349350452. p. 7.

Lo anterior no es ajeno al sector público, puesto que conforme a lo señalado por el politólogo Richard Mulgan, el *accountability* funge como valor político, y como tal, tiene un margen de discrecionalidad administrativa que va más allá de la dirección política[60]. Es decir, que "la rendición de cuentas o responsabilidad interna tiene que ver con el profesionalismo y la moralidad o conciencia personal de los funcionarios públicos y otras personas en el ejercicio de sus funciones, y especialmente de su discreción".[61]

IV Las aplicaciones de contacto y su marco ético-legal de referencia

El distanciamiento social ha sido el mecanismo histórico efectivo para hacerle frente a los contagios de una pandemia,[62] pero en razón a los avances tecnológicos sobre analítica de datos, procesamiento de la información y masificación del uso de dispositivos móviles, en la actualidad se cuenta con una nueva alternativa que ha sido vista por algunos Estados como facilitadora para controlar la propagación de virus o enfermedades y así ejercer mayor control sanitario.[63] Se trata de las tecnologías de contacto, las cuales tienen el propósito de monitorear a un individuo con el fin de alertar rápidamente si ha estado en proximidad con alguien que ha resultado contagiado, pero si bien es una estrategia que pretende mitigar la propagación, algunos autores manifiestan que el emplear este mecanismo presenta brechas frente a la privacidad, la igualdad y la equidad.[64]

No es la primera vez que se tienen estas discusiones morales, ya que una investigación publicada en la Revista Life Sciences, Society and Policy en 2018, planteó la pregunta sobre si existe el deber de participar en epidemiología digital, en donde se concluyó que en estos aspectos, el consentimiento informado es un requisito central de la ética de la investigación médica. De acuerdo con ello, el derecho a la protección de los datos personales y el reconocimiento de los

[60] MULGAN, Richard. "Accountability": An Ever-Expanding Concept? *Public Administration*. Wiley-Blackwell, Enero 2000, Vol. 78, núm. 3, p. 555–573. DOI 10.1111/1467-9299.00218.p. 571.

[61] RAAD, Charles. The Meaning of 'Accountability' inthe Information Privacy Context. En: *Managing Privacy throughAccountability*. London: Palgrave Macmillan, 2012. ISBN 9781349350452. p. 18.

[62] MUSINGUZI, Geofrey y OPPONG ASAMOAH, Benedict. The Science of Social Distancing and Total Lock Down: Does it Work? Whom does it Benefit? *Electronic Journal of General Medicine*. 2020, Vol. 17, núm. 6. ISBN 2516-3507. p. 2.

[63] CHO, Hyunghoon, IPPOLITO, Daphne y YU, Yun William. *Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs*. Mar. 2020.. Disponible en: http://arxiv.org/abs/2003.11511. Acceso en: 6 jun. 2020.

[64] MORLEY, Jessica, *et al*. Ethical guidelines for COVID-19 tracing apps. Nature Publishing Group, Jun. 2020, Vol. 582, núm. 7810, p. 29–31. DOI 10.1038/d41586-020-01578-0.

derechos humanos, segregan el deber ético de "beneficencia" de contribución a la ciencia médica, pero este argumento admite excepciones, puesto que "[c]uando existe una grave amenaza para la salud de la población, como a la luz de una posible pandemia, las medidas de salud pública infringen los derechos e intereses individuales en aras de los intereses colectivos, es decir, la salud de una población".[65]

De ahí que a lo largo de esta investigación se haga hincapié en el origen de la analítica de datos y las cuestiones éticas, en tanto que esta tecnología se está aplicando para combatir la pandemia alrededor del mundo y hay diferencias sustanciales frente a los sistemas éticos de los hemisferios, considerando los principios del comunitarismo, el imperativo categórico y del utilitarismo.[66] Por tanto, el marco ético en estas herramientas requiere considerar el contexto jurídico y social, en la medida que el cumplimiento del principio de responsabilidad demostrada presenta variaciones de aplicabilidad. Incluso, en América Latina existen países que no cuentan con una normativa de protección de datos, por lo que la implementación de estos mecanismos se ciñe a las cuestiones éticas y el funcionamiento descentralizado con el fin de garantizar mayor trasparencia.[67]

A decir verdad, algunos autores dedicados al área de la filosofía de la informática han manifestado que la recopilación de este tipo de información amenaza la privacidad, la igualdad y la equidad, incluso si el tratamiento de los datos personales se realiza de manera temporal, por lo que contar con mayor supervisión ética es esencial.[68] Sin embargo, como ya se ha mencionado, un modelo de supervisión basado en la ética no se ajusta al ordenamiento jurídico por aplicación del principio de legalidad, de modo tal que la autoridad de datos personales debe ceñirse al principio de responsabilidad demostrada, en donde el responsable o encargado tiene la responsabilidad de demostrar que cumple con los parámetros establecidos en la ley, las interpretaciones jurisprudenciales en la materia y los lineamientos establecidos por las autoridades administrativas.

La primera cuestión que se debe afrontar respecto a la implementación de *contact tracing technology* es la evaluación de necesidad, proporcionalidad

[65] MITTELSTADT, Brent, *et al*. Is there a duty to participate in digital epidemiology? *Life Sciences, Society and Policy* [en línea]. SpringerOpen, Diciembre 2018, Vol. 14, núm. 1, p. 9. DOI 10.1186/s40504-018-0074-1. p. 5.

[66] GORNIAK-KOCIKOWSKA, Krystyna. The computer revolution and the problem of global ethics. *Science and Engineering Ethics*. Opragen Publications, 1996, Vol. 2, núm. 2, p. 177–190. DOI 10.1007/BF02583552. p. 184.

[67] AGUERRE, Carolina. *La delgada y móvil frontera de las corona-apps en América Latina*. Madrid: Analisis Carolina, 2020. ISBN 2695-4362. Disponible en: https://www.fundacioncarolina.es/wp-content/uploads/2020/05/AC-30.-2020.pdf. Acceso en: 13 jun. 2020. pp. 5 y 6.

[68] MORLEY, Jessica, *et al*. Ethical guidelines for COVID-19 tracing apps. Nature Publishing Group, Jun. 2020, Vol. 582, núm. 7810, p. 29–31. DOI 10.1038/d41586-020-01578-0.

y efectividad, en la medida que su uso sea realmente efectivo para mitigar la propagación del virus y el impacto negativo de privacidad sea justificado por la gravedad de las circunstancias, por lo que este análisis de conveniencia se ajusta a la población y jurisdicción específica del territorio en donde se pretende desplegar la tecnología.[69] El Estado debe estar en capacidad de explicar cómo el uso de la tecnología se conjuga con su estrategia de mitigación,[70] de manera que se justifique la vigilancia en aplicaciones de contacto a modo de contraprestación de decisión sobre acciones que mitiguen la problemática. No obstante, el monitoreo y seguimiento se encuentra supeditado a la finalidad de salud pública y se debe respetar la libertad y la autonomía personal, cuyo reconocimiento no es ético, sino jurídico. No se puede olvidar que por ser información de carácter sanitario se clasifica como sensible, y como tal, se somete a un criterio más estricto de privacidad, de ahí que la delimitación y grado de intrusión halle relevancia, en tanto que los distintos modelos de aplicaciones varían entre sí.

Una vez superada esta etapa, el diseño de la plataforma de contacto debe ajustarse al marco regulatorio establecido para la protección de las garantías fundamentales, puesto que si bien la implementación se presenta en medio de un Estado de Emergencia Sanitaria, el respeto por los derechos y las libertades se mantienen vigentes en republicas democráticas.[71] Así pues, la primacía de los principios de protección de datos se mantiene y el tratamiento se sujeta a la manifestación del consentimiento expreso por parte del titular de los datos, a la temporalidad en el almacenamiento y uso de la información, el establecimiento de una finalidad clara y explícita que no debe cambiar sin autorización previa y la garantía del respeto de los derechos de los titulares.

Sobre el consentimiento, hay que aclarar que algunos Estados exceptúan el requerimiento del consentimiento cuando se tratan situaciones de salud pública o se presentan conductas inequívocas del titular. No obstante, la previsión de dichas circunstancias, tal como señala el profesor Nelson Remolina, no exceptúa el cumplimiento de los principios y limitaciones de la Ley, sino que por el contrario, el uso de la información debe ser licito y existir claridad sobre el título habilitante

[69] MORLEY, Jessica, *et al*. Ethical guidelines for COVID-19 tracing apps. Nature Publishing Group, Jun. 2020, Vol. 582, núm. 7810, p. 29–31. DOI 10.1038/d41586-020-01578-0.

[70] ORGANIZACIÓN MUNDIAL DE LA SALUD. *Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing*, 2020. Disponible en : https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1. Acceso en: 8 jul. 2020. p. 2.

[71] CASTAÑO, Daniel. La gobernanza ética de los sistemas de inteligencia artificial y la agencia humana. En: HENAO, Juan Carlos y CASTAÑO, Daniel (ed.), *Transformación digital, disrupción tecnológica y sociedad*. Bogotá : Universidad Externado de Colombia, [s/f].

para realizar el tratamiento.[72] En tal sentido, el titular conserva el derecho a conocer si sus datos son tratados, cuál es el uso que se le están dando y la posibilidad de solicitar la supresión de sus datos.

Así mismo, en el diseño algorítmico y funcional se debe establecer un propósito claro para los datos personales recolectados, y en caso de lanzarse capas adicionales a las previstas inicialmente, se debe notificar y posibilitar su activación manual por parte del usuario. En virtud del principio de trasparencia y en diligencia de la responsabilidad demostrada, se debe realizar un estudio de impacto de privacidad antes del despliegue de cualquier tecnología de seguimiento,[73] así es posible señalar un mayor grado de debida diligencia frente a la autoridad de datos personales en caso de cualquier requerimiento.

El estudio de impacto de privacidad se ha convertido en un estándar obligatorio en Europa, ya que permite identificar los riesgos y minimizarlos lo antes posible,[74] de modo que debe llevarse a cabo antes del tratamiento y sus resultados deben ser considerados para la toma de decisiones en el procesamiento de los datos.[75] El estudio debe realizar una descripción de las operaciones de tratamiento y su finalidad, evaluar la necesidad y proporcionalidad, identificar los riesgos a los derechos y libertades, así como indicar las medidas de seguridad para enfrentar los riesgos.[76] Es básicamente la materialización en el diseño del juicio de conveniencia en necesidad, proporcionalidad y efectividad indicado con anterioridad.

La realización del análisis obedece a cada por proyecto individualmente considerado, ya que como señala el profesor Jeffrey P. Kahn, no hay un solo enfoque de diseño para la tecnología de rastreo de contactos digitales y productos sanitarios digitales (DCTT). Por el contrario, las cuestiones sobre estas tecnologías requieren atender las necesidades, preferencias y prioridades locales, de tal suerte que se ajusten a los criterios de protección a la privacidad y la posibilidad del usuario para decidir sobre la información que comparte.[77] No es posible decantar

[72] REMOLINA ANGARITA, Nelson. *Tratamiento de datos personales: Aproximación internacional y comentarios a la ley 1581 de 2012*. Bogotá: Legis, 2013. ISBN 9789587670868. pp. 201 y 202.

[73] VINUESA, Ricardo, THEODOROU, Andreas, BATTAGLINI, Manuela, et al. *A socio-technical framework for digital contact tracing* [en línea]. Mayo 2020. Disponible en : http://arxiv.org/abs/2005.08370. Acceso en: 7 jul. 2020. p. 2.

[74] COIMISIÚN UM CHOSAINT SONRAÍ. *Guidance Note: Guide to Data Protection Impact Assessments (DPIAs)*. [S. l.]:[s. n.], 2019. p. 65.

[75] ARTICLE 29 DATA PROTECTION GROUP. *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679*. 2017. p 16.

[76] ARTICLE 29 DATA PROTECTION GROUP. *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679*. 2017. p. 18.

[77] KAHN, Jeffrey. *Digital Contact Tracing for Pandemic Response*. Baltimore, Md.: Johns Hopkins University Press, 2020. pp. 1 y 2.

un modelo de responsabilidad demostrada preestablecido, en el entendido que los desarrolladores no se han puesto de acuerdo en un enfoque estándar único.[78]

Ahora, el funcionamiento de la aplicación de seguimiento es clave, puesto que es allí en donde se analiza el grado de intrusión y acceso a la información personal. En principio, estas aplicaciones tienen el propósito de presentar una notificación de exposición al usuario,[79] pero se han presentado casos en los cuales las aplicaciones de rastreo además de identificar y notificar, hacen seguimiento a la identidad de los usuarios, su ubicación y su historial de pagos.[80]

Al respecto, la normatividad exige que el tratamiento se ajuste a la finalidad establecida en la política de privacidad, evitando así hallazgos incidentales o políticas de doble uso, en el entendido que podrían darse otros usos potenciales a los datos recolectados.[81] La titularidad de los datos personales corresponde a los usuarios y conservan el derecho que el ordenamiento jurídico les otorga con relación autorizar, rectificar y solicitar la supresión de sus datos personales.

Por tanto, la gobernanza de los datos recopilados adquiere la mayor importancia, puesto que es en esta etapa donde la planeación ética del diseño presenta un punto de encuentro con el ordenamiento jurídico. La doctrina sugiere que debido a que la confianza frente a la administración de los datos por parte del Estado es baja, deben implementarse modelos descentralizados que no hagan uso de servidores de coordinación central y se privilegie la protección del derecho a la privacidad.[82] Igualmente, se propone que para exaltar la transparencia, se presenten políticas claras y disponibles públicamente, en donde el código de programación empleado para esta tecnología sea abierto y acceso libre.[83]

Lo anterior facilita el proceso de auditabilidad del algoritmo que procesa la información de los usuarios, ya que es una de las buenas prácticas que se ha venido decantando en el derecho comparado; ello permite reforzar la confianza,

---

78 HOWELL O'NEILL, Patrick, RYAN-MOSLEY, Tate y JOHNSON, Bobbie. A flood of coronavirus apps are tracking us. Now it's time to keep track of them. *MIT Technology Review*. 7 may. 2020. Disponible en : https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/. Acceso en: 6 jul. 2020.

79 HOWELL O'NEILL, Patrick, RYAN-MOSLEY, Tate y JOHNSON, Bobbie. A flood of coronavirus apps are tracking us. Now it's time to keep track of them. *MIT Technology Review*. 7 may. 2020. Disponible en : https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/. Acceso en: 6 jul. 2020.

80 HOWELL O'NEILL, Patrick, RYAN-MOSLEY, Tate y JOHNSON, Bobbie. A flood of coronavirus apps are tracking us. Now it's time to keep track of them. *MIT Technology Review*. 7 may. 2020. Disponible en : https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/. Acceso en: 6 jul. 2020.

81 VINUESA, Ricardo, *et al. A socio-technical framework for digital contact tracing*. May. 2020. Disponible en : http://arxiv.org/abs/2005.08370. Acceso en: 7 jul. 2020. p. 3.

82 Cfr. MORLEY, Jessica, *et al*. Ethical guidelines for COVID-19 tracing apps. Nature Publishing Group, Jun. 2020, Vol. 582, núm. 7810, p. 29–31. DOI 10.1038/d41586-020-01578-0.

83 HOWELL O'NEILL, Patrick, RYAN-MOSLEY, Tate y JOHNSON, Bobbie. A flood of coronavirus apps are tracking us. Now it's time to keep track of them. *MIT Technology Review*. 7 may. 2020. Disponible en : https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/. Acceso en: 6 jul. 2020.

asegurar la compatibilidad de la aplicación con los parámetros que se describen al público y verificar que la necesidad para el propósito de diseño inicial se mantiene vigente.[84]

Aunado lo anterior, no se puede olvidar la necesidad de asegurar la privacidad de las bases de datos, producto del funcionamiento de la aplicación de contacto, razón por la cual deben procesarse los datos estrictamente necesarios y preverse un principio de minimización de datos, que realice un almacenamiento local y encriptado de la información.[85] Algunos autores sugieren el modelo descentralizado como protocolo, ya que conlleva a que el rastreo de proximidad se almacene en el dispositivo del usuario y preserva en mayor medida la privacidad.[86] En todo caso, es evidente que existe cierto grado de revelación de información, lo que indica que el tratamiento de los datos se ejerce a suerte de lógica de compensación, respecto del costo privacidad que hay que asumir frente a la propagación del virus.[87]

Hasta este apartado, se ha hecho un mayor énfasis en la tecnología de rastreo de contacto. No obstante, la tendencia frente a la reapertura apunta a la implementación de un gran número de productos sanitarios digitales, los cuales harán uso de imágenes térmicas y otros mecanismos tecnológicos para determinar la temperatura de las personas.[88] En tal sentido, se espera que el tratamiento de información sensible termine en el intercambio generalizado de datos entre agencias gubernamentales y empresas privadas que implementan estas medidas de control.[89] De esta manera, la población enfrenta cierto deber de participar en epidemiología digital generalizada, ya que se involucran nuevas fuentes de datos diferentes a los de salud y se registraría toda clase de comportamientos a través de la interacción con plataformas, servicios y dispositivos en línea.[90]

De acuerdo a lo indicado en este marco ético-legal, la tecnología de rastreo de contactos digitales y productos sanitarios digitales requiere de

[84] MORLEY, Jessica, *et al*. Ethical guidelines for COVID-19 tracing apps. Nature Publishing Group, Jun. 2020, Vol. 582, núm. 7810, p. 29–31. DOI 10.1038/d41586-020-01578-0.

[85] Cfr. VINUESA, Ricardo, *et al. A socio-technical framework for digital contact tracing*. May. 2020. Disponible en : http://arxiv.org/abs/2005.08370. Acceso en: 7 jul. 2020.

[86] VINUESA, Ricardo, *et al. A socio-technical framework for digital contact tracing*. May. 2020. Disponible en : http://arxiv.org/abs/2005.08370. Acceso en: 7 jul. 2020. p. 2.

[87] SCHNEIER, Bruce. "Security Trade-Offs Are Subjective" and 'Technology Creates Security Imbalances". En: JOHNSON, Deborah (ed.), *Technology and Society: Building our Sociotechnical Future*. Masachusets: The MIT Press, 2008. ISBN 9780262600736. p. 545.

[88] COSGROVE, Cathy. Privacy questions for COVID-19 testing and health monitoring. IAPP. 13 may. 2020.. Disponible en: https://iapp.org/news/a/privacy-questions-for-covid-19-testing-and-health-monitoring/. Acceso en: 7 jul. 2020. p. 2.

[89] COSGROVE, Cathy. Privacy questions for COVID-19 testing and health monitoring. IAPP. 13 may. 2020.. Disponible en: https://iapp.org/news/a/privacy-questions-for-covid-19-testing-and-health-monitoring/. Acceso en: 7 jul. 2020. p. 2.

[90] MITTELSTADT, Brent, *et al*. Is there a duty to participate in digital epidemiology? *Life Sciences, Society and Policy*. Springer, Dic. 2018, Vol. 14, núm. 1, p. 9. DOI 10.1186/s40504-018-0074-1.

fases de implementación para una implementación viable de conformidad con el ordenamiento jurídico, pero pese a todos los esfuerzos, es posible que se presenten brechas a la seguridad o al cumplimiento responsable de los protocolos de tratamiento de datos personales, razón por la cual, se debe prever una estrategia de mitigación de daños, todavía más, cuando los usuarios no tienen la oportunidad de consentir el tratamiento por cuestiones de salud pública.[91]

Al final, la Organización Mundial de la Salud (OMS) indica que la utilización de esta tecnología se resume en la efectividad de su propósito, por lo que si no existe confianza y fiabilidad para tener resultados eficientes en la toma de decisiones de salud pública, la tecnología debe ser eliminada.[92] También, se sugiere considerar como estándar ético el establecimiento de limitación de tiempo en el tratamiento de los datos, la realización de pruebas y evaluaciones previo al uso masivo, realizar el procesamiento de forma proporcional con el propósito, minimizar los datos requeridos y preservar la privacidad en el almacenamiento.

En tal sentido, es primordial dar prevalencia a una gobernanza de los datos con debida diligencia, en donde se apliquen procesos de anonimización de datos y se establezcan modelos para que el acceso a los datos sea restringido y el tratamiento de esta información personal no termine en procesos de segmentación y discriminación.

Tal como lo señala Jake Goldenfein, Ben Green y Salomé Viljoen, el análisis de impacto de privacidad entre el control epidemiológico del virus y la puesta en riesgo de los datos personales de los ciudadanos parece indicar "una falsa compensación", porque la implementación puede convertirse en una excusa para crear infraestructuras de vigilancia sobre la población civil y no se estaría cumpliendo el propósito.[93] Desde esta perspectiva, la implementación en América Latina no arroja datos precisos todavía, por lo que por ahora, es menester priorizar un modelo de gobernanza que resguarde el derecho a la privacidad y evaluar la conveniencia del uso de esta tecnología mediante el contraste de los datos conforme transcurre la implementación.

---

[91] Cfr. MITTELSTADT, Brent, *et al*. Is there a duty to participate in digital epidemiology? *Life Sciences, Society and Policy*. Springer, Dic. 2018, Vol. 14, núm. 1, p. 9. DOI 10.1186/s40504-018-0074-1. p. 15.

[92] ORGANIZACIÓN MUNDIAL DE LA SALUD. *Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing*, 2020. Disponible en: https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1. Acceso en: 8 jul. 2020. p. 2.

[93] GOLDENFEIN, Jake; GREEN, Ben; VILJOEN, Salomé. Privacy Versus Health Is a False Trade-Off. *Jacobin*, abr. 2020. Disponible en : https://jacobinmag.com/2020/04/privacy-health-surveillance-coronavirus-pandemic-technology. Acceso en: 9 jul 2020.

V Conclusiones

En concordancia con lo expuesto, el diseño de esta tecnología es éticamente justificable solo si logra un equilibrio razonable frente a una respuesta efectiva de salud pública, la protección de la privacidad, la prevención de daños y la correcta distribución equitativa de los beneficios y afectación de derechos individuales.[94] La realidad demuestra que el principal reto que presenta la escalabilidad de estas iniciativas es lograr obtener la confianza de los usuarios, ya que por tratarse de una situación de emergencia en donde el consentimiento y la auditabilidad se pasa por alto, la balanza se puede inclinar al autoritarismo y el perfilamiento de los ciudadanos.

Ahora, hay que precisar que el carácter ético de la tecnología de contacto se presenta en el diseño técnico de la misma, porque cuando se pone en marcha el proyecto y se recopilan datos personales empieza a tener aplicación las normativas de protección de datos personales, y por ende, los principios que le rigen. En particular, el principio de responsabilidad demostrada exige comprobar una debida diligencia y el efectivo cumplimiento de los protocolos de seguridad y uso responsable de la información. No se puede olvidar que hay una diferencia clara entre moral y derecho, pero en algunas ocasiones, una norma moral se convierte en norma jurídica por considerar su previsión en el derecho positivo.

Es el caso de la aplicación de buenas prácticas, en donde se expuso que el cumplimiento de la responsabilidad demostrada puede materializarse en un modelo de gobernanza de datos, cuyo pilar se exponga en la política de privacidad de la tecnología de contacto. La rendición de cuentas adquiere entonces un rol preponderando de cara a la autoridad de datos personales, pero también respecto de los usuarios, ya que plantea cierto control ético que recibe una sanción social efectiva prevista en el ordenamiento jurídico.[95] Si bien la ética digital se ha tornado como una disciplina propia, en el entendido que la política pública no es suficiente para enfrentar la evolución tecnológica, nuestro ordenamiento jurídico se ciñe al principio de legalidad.[96]

La investigación sugiere abordar una hoja de ruta que combine la ética digital en el componente técnico y los aspectos jurídicos en la puesta en marcha. De ahí que se proponga evaluar el marco de implementación y diseño, para luego aplicar

[94] KAHN, Jeffrey. *Digital Contact Tracing for Pandemic Response*. Baltimore, Md.: Johns Hopkins University Press, 2020. p. 44.

[95] WIENER, Norbert. *The human use of beings*. Vol. 140, 1965. ISBN 1853430757. DOI 10.1097/00005053-196501000-00001. p. 105.

[96] MANER, Walter. Unique ethical problems in information technology. *Science and Engineering Ethics* [en línea]. Opragen Publications, 1996, Vol. 2, núm. 2, p. 137–154. DOI 10.1007/BF02583549. p. 66.

los principios en el funcionamiento y seguimiento de la aplicación. Así mismo, es de gran importancia reforzar la confianza con procesos de auditabilidad y la adopción de mecanismos de seguridad que garanticen la seguridad los datos.

Así pues, si bien la tecnología ha resultado beneficiosa en muchos aspectos de la vida, ello no obsta para que sea la respuesta a todos los problemas.[97] Se requiere fomentar buenas prácticas y la realización de análisis de impacto de privacidad que permitan modelar un modelo ético-legal para la gobernanza de los datos, aún más cuando se trata de la recopilación y monitoreo de datos en cuestiones de salud pública.

The dichotomy of ethics and legality of personal data in contact apps

Abstract: The contact tracing technology and digital health products has become one of the mechanisms to monitor individuals and alert if they have been in proximity to someone who has been infected with a virus. The text presents an analysis of the aspects related to the right to privacy and the conflict that arises from the principle of legality, in order to propose a data governance model based on an ethical-legal framework of reference, which conforms to the accountability in the implementation and operation of technological tools.

Keywords: data protection, digital ethics, privacy, health technology, governance, principle of legality.

A dicotomia da ética e a legalidade dos dados pessoais em aplicações de contato

Resumo: A tecnologia de rastreamento de contatos e de produtos de saúde digitais converteu-se em um dos mecanismos para monitorar os indivíduos e alertar rapidamente se estiveram em proximidade com alguém que foi contagiado por um vírus. O texto apresenta uma análise dos aspectos relacionados ao direito à privacidade e o conflito que surge face ao princípio da legalidade, para assim propor um modelo de governança dos dados baseado em um marco ético-legal de referência, o qual se ajuste ao princípio da responsabilidade demonstrada na implementação e funcionamento de ferramentas tecnológicas.

Palavras-chave: proteção de dados, ética digital, privacidade, tecnologia de saúde, governança, princípio da legalidade.

[97] COECKELBERGH, Mark. Corona app: Ethical, legal, and societal issues. Derstandard, 19 may. 2020. Disponible en: https://www.derstandard.at/story/2000117457461/corona-app-ethical-legal-and-societal-issues. Acceso en 7 jul. 2020.

Referencias

AGUERRE, Carolina. Estrategias nacionales de IA y gobernanza de datos en la región. En: AGUERRE, Carolina (Ed.), Inteligencia Artificial en América Latina y el Caribe. *Ética, Gobernanza y Políticas*. Buenos Aires: CETyS Universidad de San Andrés., 2020.

AGUERRE, Carolina. *La delgada y móvil frontera de las corona-apps en América Latina*. Madrid: Analisis Carolina, 2020. ISBN 2695-4362. Disponible en: https://www.fundacioncarolina.es/wp-content/uploads/2020/05/AC-30.-2020.pdf. Acceso en: 13 jun. 2020.

ARTICLE 29 DATA PROTECTION GROUP. *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679*. 2017.

ARTICLE 29 DATA PROTECTION GROUP. *Opinion 3/2010 on the principle of accountability*, 2010. Disponible en: https://www.dataprotection.ro/servlet/ViewDocument?id=654. Acceso en 13 jun. 2020.

BLOUSTEIN, Edward J. Privacy as an aspect of human dignity: an answer to Dean Prosser. En : *Philosophical Dimensions of Privacy*. London: Cambridge University Press. p. 156–202. DOI 10.1017/cbo9780511625138.007.

BUENADICHA SÁNCHEZ, César; GALDON, Gemma; HERMOSILLA, María; LOEWE, Daniel; POMBO, Cristina. *La gestión ética de los datos*. Washington D.C.: Banco Interamericano de Desarrollo, marzo 2019. DOI 10.18235/0001623.

BYNUM, Terrell Ward. Computer ethics: Its birth and its future. *Ethics and Information Technology*. Kluwer Academic Publishers, 2001, Vol. 3, núm. 2, p. 109–112. DOI 10.1023/A:1011893925319.

CASTAÑO, Daniel. La gobernanza de la Inteligencia Artificial en América Latina: entre la regulación estatal, la privacidad y la ética digital. En: AGUERRE, Carolina (ed.), *Inteligencia Artificial en América Latina y el Caribe. Ética, Gobernanza y Políticas*. Buenos Aires: CETyS Universidad de San Andrés, 2020.

CASTAÑO, Daniel. *GovTech: Legalidad, Privacidad y Ética Digital*. Bogotá: Alcaldía Mayor de Bogotá, 2019. ISBN 9789585251618.

CASTAÑO, Daniel. La gobernanza ética de los sistemas de inteligencia artificial y la agencia humana. En: HENAO, Juan Carlos; CASTAÑO, Daniel (ed.), *Transformación digital, disrupción tecnológica y sociedad*. Bogotá: Universidad Externado de Colombia, [s/f].

CASTAÑO, Daniel. Nudge + código. Una arquitectura digital para el precedente judicial. En : RINCÓN CÓRDOBA, Jorge (Ed.), *Las trasformaciones de la administración pública y del derecho administrativo*. Bogotá: Universidad Externado de Colombia, 2019.

CENTRE FOR INFORMATION POLICY LEADERSHIP AT SECRETARIAT TO THE GALWAY PROJECT. *Data Protection Accountability: The Essential Elements A Document for Discussion*. [S. l.]: [s. n.], 2009.

CHO, Hyunghoon; IPPOLITO, Daphne; YU, Yun William. *Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs*. Marzo 2020. Disponible en : http://arxiv.org/abs/2003.11511. Acceo en: 6 jun. 2020.

COECKELBERGH, Mark. Corona app: Ethical, legal, and societal issues. Derstandard, 19 may. 2020. Disponible en: https://www.derstandard.at/story/2000117457461/corona-app-ethical-legal-and-societal-issues. Acceso en 7 jul. 2020.

COIMISIÚN UM CHOSAINT SONRAÍ. *Guidance Note: Guide to Data Protection Impact Assessments (DPIAs)*. [S. l.]: [s. n.], 2019.

COSGROVE, Cathy. Privacy questions for COVID-19 testing and health monitoring. IAPP, 13 may. 2020. Disponible en : https://iapp.org/news/a/privacy-questions-for-covid-19-testing-and-health-monitoring/. Acceso en: 7 jul. 2020.

DE HERT, Paul. Accountability and SystemResponsibility: New Concepts in Data Protection Law andHuman Rights Law. En: *Managing Privacy throughAccountability*. London: Palgrave Macmillan, 2012.

DEMETZOU, Katerina. GDPR and the concept of risk: The role of risk, the scope of risk and the technology involved. En: *IFIP Advances in Information and Communication Technology*. Vol. 547. Nw York: Springer, 2019, p. 137–154. ISBN 9783030167431. DOI 10.1007/978-3-030-16744-8_10.

ENCK, William; GILBERT, Peter; CHUN, Byunggon; COX, Landon P.; JUNG, Jaeyeon; MCDANIEL, Patrick; SHETH, Anmol. TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones. *OSDI'10: Proceedings of the 9th USENIX conference on Operating systems design and implementation,*. 2010. p. 393–407. DOI 10.5555/1924943.

FLORIDI, Luciano. *Philosophy and computing: an introduction*. London: Routledge, 1999. ISBN 0415 180244.

FULLER L., Lon. *La moral del derecho*. Ciudad de México: Editorial F. Trillas, 1964.

GOLDENFEIN, Jake; GREEN, Ben; VILJOEN, Salomé. Privacy Versus Health Is a False Trade-Off. J*acobin*, abr. 2020. Disponible en : https://jacobinmag.com/2020/04/privacy-health-surveillance-coronavirus-pandemic-technology. Acceso en: 9 jul 2020.

GORNIAK-KOCIKOWSKA, Krystyna. The computer revolution and the problem of global ethics. *Science and Engineering Ethics*. Opragen Publications, 1996, Vol. 2, núm. 2, p. 177–190. DOI 10.1007/BF02583552.

GUAGNIN, Daniel; HEMPEL, Leon; ILTEN, Carla; KROENER, Inga; NEYLAND, Daniel; POSTIGO, Hector. Introduction. En: *Managing Privacy through Accountability*. London: Palgrave Macmillan, 2012. ISBN 9781349350452.

HALD, Anders. *A history of probability and statistics and their applications before 1750*. Hoboken N.J: Wiley, 2003. ISBN 9780471471295.

HANS, Kelsen. *Teoría pura del derecho*. Buenos Aires: Editorial Eudeba, 2015. ISBN 9789502308869.

HINESTROSA, Fernando. *Tratado de las obligaciones II: de las fuentes de las obligaciones : negocio jurídico*. Bogotá: Universidad Externado de Colombia, 2015.

HOWELL O'NEILL, Patrick; RYAN-MOSLEY, Tate; JOHNSON, Bobbie. A flood of coronavirus apps are tracking us. Now it's time to keep track of them. *MIT Technology Review*, 7 may. 2020. Disponible en: https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker. Acceso en: 6 jul. 2020.

JOHNSON, Deborah. Computer ethics. En: FLORIDI, Luciano (ed.), *The Blackwell Guide to the Philosophy of Computing and Information*. Nueva Jersey: Blackwell Publishing Ltd, 2004.

KAHN, Jeffrey. *Digital Contact Tracing for Pandemic Response*. Baltimore, Md.: Johns Hopkins University Press, 2020.

KELLEHER, John D.; TIERNEY, Brendan. *Data science*. Cambridge, MA: The MIT Press, 2018. ISBN 9780262347020.

LI, Jing; ZHANG, Xinwei; WANG, Keqin; ZHENG, Chen; TONG, Shurong; EYNARD, Benoit. A personalized requirement identifying model for design improvement based on user profiling. *Artificial Intelligence for Engineering Design, Analysis and Manufacturing*. Cambridge University Press (CUP), Febrero 2020, Vol. 34, núm. 1, p. 55–67. DOI 10.1017/s0890060419000301.

MANER, Walter. Unique ethical problems in information technology. *Science and Engineering Ethics*. Opragen Publications, 1996, Vol. 2, núm. 2, p. 137–154. DOI 10.1007/BF02583549.

MITTELSTADT, Brent; BENZLER, Justus; ENGELMANN, Lukas; PRAINSACK, Barbara; VAYENA, Effy. Is there a duty to participate in digital epidemiology? *Life Sciences, Society and Policy*, Dic. 2018, Vol. 14, núm. 1. DOI 10.1186/s40504-018-0074-1.

MOOR, James. Whats is computer ethics? *Metaphilosophy* [en línea]. John Wiley & Sons, Ltd, Octubre 1985, Vol. 16, núm. 4, p. 266–275. DOI 10.1111/j.1467-9973.1985.tb00173.x.

MORLEY, Jessica; COWLS, Josh; TADDEO, Mariarosaria; FLORIDI, Luciano. Ethical guidelines for COVID-19 tracing apps. Nature Publishing Group, Jun. 2020, Vol. 582, núm. 7810, p. 29–31. DOI 10.1038/d41586-020-01578-0.

MULGAN, Richard. "Accountability": An Ever-Expanding Concept? *Public Administration* [en línea]. Wiley-Blackwell, Enero 2000, Vol. 78, núm. 3, p. 555–573. DOI 10.1111/1467-9299.00218.

MUSINGUZI, Geofrey; OPPONG ASAMOAH, Benedict. The Science of Social Distancing and Total Lock Down: Does it Work? Whom does it Benefit? *Electronic Journal of General Medicine*. 2020, Vol. 17, núm. 6. ISBN 2516-3507.

NIEVES SALDAÑA, María. El derecho a la privacidad en los Estados Unidos: aproximación diacrónica a los intereses constitucionales en juego. *Teoría y Realidad Constitucional*. UNED - Universidad Nacional de Educacion a Distancia, Jun. 2011, Vol. 0, núm. 28, p. 279. DOI 10.5944/trc.28.2011.6960.

ORGANIZACIÓN MUNDIAL DE LA SALUD. *Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing* [en línea]. [S. l.] : [s. n.], 2020. Disponible en : https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1. Acceso en: 8 jul. 2020.

PARLAMENTO EUROPEO; CONSEJO DE EUROPA. *Directiva 95/46/CE* . OPOCE, 1995.

PARLAMENTO EUROPEO ; CONSEJO DE EUROPA. *Reglamento General de Protección de Datos Europeo. Reglamento (UE) 2016/679*. Disponible en : https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES. Acceso en: 28 abril 2020.

PERILLA, Mario; RAMÍREZ, Daniel. *Guía para la implementación del principio de responsabilidad demostrada en el tratamiento de datos personales*. [S. l.]: Deloitte, 2015.

RAAD, Charles. The Meaning of 'Accountability' inthe Information Privacy Context. En : *Managing Privacy throughAccountability*. London: Palgrave Macmillan, 2012. ISBN 9781349350452.

RAMÍREZ CLEVES, Gonzalo. Teoría de la constitución, constitución y poder constituyente. En: CORREA HENAO, Magdalena; OSUNA PATIÑO, Néstor; RAMÍREZ CLEVES, Gonzalo (ed.), *Lecciones de derecho constitucional*. Bogotá: Universidad Externamdo de Colombia, 2017.

RED IBEROAMERICANA DE PROTECCIÓN DE DATOS. *Reglamneto de la RIPD*, 2003.

REMOLINA ANGARITA, Nelson. *Tratamiento de datos personales: Aproximación internacional y comentarios a la ley 1581 de 2012*. Bogotá: Legis, 2013. ISBN 9789587670868.

RICHARDSON, Janice. *Law and the Philosophy of Privacy*. New York: Routledge, 2017. ISBN 978113 8081116.

RODOTÀ, Stefano. Data Protection as a Fundamental Right. En: GUTWIRTH S.; POULLET, Y.; DE HERT, P.; DE TERWANGNE, C.; NOUWT S. (Ed.). *Reinventing Data Protection?* Netherlands: Springer, 2009, p. 77–82. DOI 10.1007/978-1-4020-9498-9_3.

RODRÍGUEZ, Libardo. *Derecho administrativo: general y colombiano*. Bogotá: Editorial Temis, 2017. ISBN 9789583511486.

RUMOLD, Mark. *Evaluación de la legalidad y proporcionalidad de la vigilancia de las comunicaciones en la legislación de Estados Unidos*. [S. l.] : [s. n.], 2016.

SCHNEIER, Bruce. "Security Trade-Offs Are Subjective" and "Technology Creates Security Imbalances'. En : JOHNSON, Deborah (ed.), *Technology and Society: Building our Sociotechnical Future*. Massachusetts: The MIT Press, 2008. ISBN 9780262600736.

SCHOEMAN, Ferdinand. Privacy and intimate information. En : SCHOEMAN, Ferdinand (ed.), *Philosophical Dimensions of Privacy*. Cambridge: Cambridge University Press, feb. 2010, p. 403–418. DOI 10.1017/cbo9780511625138.018

SCOGLIO, Stefano. *Transforming privacy: a transpersonal philosophy of rights*. Westport: Praeger, 1998. ISBN 9780275956073.

SOLOVE, Daniel. Conceptualizing Privacy. *California Law Review*. 2008, Vol. 90, núm. 2002.

VINUESA, Ricardo; THEODOROU, Andreas; BATTAGLINI, Manuela; DIGNUM, Virginia. *A socio-technical framework for digital contact tracing*. May. 2020. Disponible en: http://arxiv.org/abs/2005.08370. Acceso en: 7 jul. 2020.

WHITMAN, James Q. The Two Western Cultures of Privacy: Dignity versus Liberty. *Yale Law Journal*. 2004, Vol. 113. DOI 10.2139/ssrn.476041.

WIENER, Norbert. *The human use of beings*. Vol. 140. [S. l.]: [s. n.], 1965. ISBN 1853430757. DOI 10.1097/00005053-196501000-00001.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

VARGAS OSORNO, Teresa; CABALLERO MARTÍNEZ, Jhon. La dicotomía de la ética y la legalidad de los datos personales en aplicaciones de contacto. *Direitos Fundamentais & Justiça,* Belo Horizonte, ano 14, p. 17-41, nov. 2020. Número especial.

Recebido em: 12.07.2020
Aprovado em: 14.09.2020
Cota Convite