



Aplicaciones de rastreo y monitoreo: del entusiasmo tecnológico al reconocimiento de la autodeterminación informática

TRACKING AND MONITORING APPLICATIONS: FROM TECHNOLOGICAL ENTHUSIASM TO THE RECOGNITION OF INFORMATIONAL SELF-DETERMINATION

APLICAÇÕES DE RASTREIO E MONITORIZAÇÃO: DO ENTUSIASMO TECNOLÓGICO AO RECONHECIMENTO DA AUTODETERMINAÇÃO INFORMÁTICA

Guillermo Rodrigo Corredor Castellano¹

Resumen

La forma casi obsesiva en que el sistema capitalista tiende a asignar un valor de explotación a todo cuanto puede ser cuantificable, vinculada a las sucesivas evoluciones tecnológicas que han permitido la desmaterialización de los intercambios y la asignación de un valor a bienes intangibles, ha llegado al paroxismo de extrapolar dicha comprensión a los atributos de la personalidad. Este proceso de erosión de la esfera de derechos se da en beneficio de la capacidad monetizadora de un puñado de empresas que ostentan una posición monopólica transnacional. El artículo busca ofrecer respuestas a cuestiones legales que surgen respecto de las actividades de perfilamiento (*web tracking*) de ciudadanos en los contextos públicos y privados. A partir del examen crítico de las normas de protección al consumidor se plantean zonas de incorporación para nuevos conceptos que amplíen la protección de la privacidad.

Palabras clave

Economía digital; derechos intangibles; protección del consumidor; aplicaciones de rastreo; privacidad.

Abstract

The almost obsessive way in which the capitalist system tends to assign an exploitation value to everything that can be quantifiable and its linkage to the successive technological developments that have allowed the dematerialization of exchanges and the assignment of a value with respect to intangible goods has come to the paroxysm of extrapolating this understanding to the very attributes of personality. This process of erosion of the sphere of rights has occurred in favour of the monetizing capacity of a handful of companies that hold a transnational monopoly position. The article seeks to provide answers to legal questions that arise with respect to the web tracking activities of citizens in public and private contexts. Based on a critical examination of consumer protection regulations, areas of incorporation for new concepts that expand privacy protection are proposed.

Keywords

Digital economy; intangible rights; consumer protection; tracking applications; privacy.

Resumo

A forma quase obsessiva como o sistema capitalista tende a atribuir um valor exploratório a tudo o que pode ser quantificado, associada às sucessivas evoluções tecnológicas que permitiram a desmaterialização das trocas e a atribuição de um valor a bens intangíveis, atingiu o paroxismo de extrapolar esse entendimento para

os atributos de personalidade. Esse processo de erosão da esfera dos direitos beneficia a capacidade de monetização de empresas com uma posição de monopólio transnacional. Este artigo procura dar respostas a questões jurídicas que se levantam em relação às atividades de perfilamento dos cidadãos em contextos públicos e privados. Com base em um exame crítico dos regulamentos de proteção do consumidor, são propostas áreas de incorporação de novos conceitos que expandem a proteção da privacidade.

Palavras-chave

Economia digital; direitos intangíveis; proteção do consumidor; aplicações de rastreo; privacidade.

INTRODUCCIÓN

Las numerosas referencias a la economía de los datos o *data driven economy* evocan un clima de nuevos desarrollos tecnológicos que prometen alterar de manera radical los estilos de vida de millones de personas. Sin embargo, las reflexiones en torno a la forma como estas nuevas tecnologías influirán en el alcance de ciertos derechos y garantías fundamentales son menos numerosas o por lo menos, por ahora, un poco menos visibles. En este escenario de transición hacia una sociedad gobernada a través de los datos, la privacidad ha sido, sin lugar a dudas, la puerta de entrada a las discusiones relativas al rol del Estado en la regulación de mercados influenciados por nuevos conceptos, tales como el de economías de escala desde la demanda —o economías de alcance/*scope* (GARCÉS, 2017)—, externalidades de red, economías colaborativas/*gig economy* (LÓPEZ y ARROYO, 2006), prosumidores, mercados de dos caras/*two sided* y desde luego el monitoreo/*web tracking* (ZUBOFF, 2019).

El trasfondo de estas discusiones está relacionado con la forma casi obsesiva en que el sistema capitalista ha asignado un valor de explotación a todo cuanto puede ser cuantificado. Por otra parte, la evolución tecnológica que ha permitido la desmaterialización de los intercambios y la asignación de un valor a bienes intangibles, ha llegado al paroxismo de hacer lo propio con respecto de ciertos atributos de la personalidad. Este proceso de erosión de la esfera de derechos se da en beneficio de la capacidad monetizadora alcanzada por un puñado de poderosas corporaciones tecnológicas. La discusión sobre este tema es ilustrativa de la forma como a lo largo del último siglo se ha ido consolidando un proceso de profundización del capitalismo, el cual solo ahora comienza a parecernos extremo e incómodo en razón de su intrusividad y, en algunos casos, de la irreversibilidad de sus efectos.

El presente artículo aborda desde una perspectiva constructivista una revisión bibliográfica de los aspectos jurídicos subyacentes a la protección de la privacidad y los efectos

actuales del despliegue de herramientas de perfilamiento en línea (*web tracking profiling*). Dentro de esta lógica, en la primera parte se plantea una reflexión crítica en torno a la forma como se ha dado la deconstrucción paulatina de la noción de derechos personalísimos o derechos inherentes a la personalidad y de cómo dicha instrumentalización ha terminado por concretarse en la monetización de la información personal de millones de individuos. En la segunda parte, se avanza en la reflexión tomando partido por los enfoques que privilegian la protección de los derechos del consumidor como medio para lograr la efectiva protección de la privacidad y por esa vía se postula que los actuales niveles de penetración en la esfera privada de los individuos son en parte el resultado de visiones fragmentadas frente a la protección de los derechos de los consumidores. En la tercera parte, el análisis reseña algunos de los programas estatales de vigilancia o *profiling*, tales como el *social rating* en China o el programa de identificación biométrica obligatoria establecido por el gobierno de India. El análisis se extiende al despliegue de herramientas de rastreo durante la crisis sanitaria en países como Israel, Suiza y Francia, así como al alcance de las medidas adoptadas dentro de tales jurisdicciones con el fin de evitar que su uso se convirtiese en un factor potencial de erosión de los derechos y libertades individuales. Desde esta comprensión, el texto aborda la dicotomía entre las nociones de protección del consumidor en el plano del derecho privado y los enfoques de protección a la privacidad planteados en el plano de la información que los particulares ponen a disposición de las autoridades públicas. Como resultado de tales reflexiones, el artículo avizora como solución el desarrollo de la noción de autodeterminación informática como elemento clave para la restauración de la escala de valores universales que al filo de los años logró esbozar una esfera de protección de derechos de los individuos, esa misma que hoy parece erosionada como resultado de un desbordado individualismo hedonista y autodestructivo propiciado en el entorno de las plataformas digitales.

I. DE LA INTANGIBILIDAD DE LOS DERECHOS A LA MONETIZACIÓN DE LA INFORMACIÓN PERSONAL

Para abordar la deconstrucción paulatina de la noción de derechos personalísimos y su dinámica actual, tendiente a la excesiva monetización de los datos personales, se propone como punto de partida el análisis planteado por Allaire (2019, p. 35), en relación con el contexto histórico del cual emerge la teoría de los bienes intangibles. En su planteamiento, el autor ubica al Estado de Bienestar como el marco en el cual se dieron los primeros procesos regulatorios de estandarización, que a la postre serán causa eficiente de la dinámica de desmaterialización de las diferentes esferas de derechos.

Aunque su teoría se enfoca hacia los factores que propiciaron la desmaterialización de productos agrícolas y su posterior “comoditización”, es posible encontrar algunos puntos de contacto que resultan extrapolables al estado actual de ciertos derechos “personalísimos” que hoy

en día son objeto del apetito insaciable de los denominados gigantes de la tecnología; la tesis a explorar sugiere:

Intangible property enables the limitation of the abundance of certain things (for example, that of AOC champagne or products of a specific brand) so as to influence prices. But it creates new markets for information contributing to financial capital accumulation: first the development of financial services by the banking system, and then the emergence and development of service industries exploiting numeric and communication technologies and based on intangible assets (audit, design, knowledge production, and so forth) intangible property thus permits the development of new types of services concerning education or social security as new forms of alienation, as revealed by the recurrent criticisms of consumer society and of the mass entertainment industries.

Para los fines de la discusión que se plantea en este artículo, es de especial interés la relación producto-información que el autor identifica en el contexto del derecho privado. En efecto, ciertas categorías de derechos de propiedad intelectual (DPI), específicamente las denominaciones de origen (AOC por su sigla en francés), propician y desarrollan esta relación de causalidad. Es justamente esta preponderancia –la cual, conforme al modelo capitalista, se da a la información ligada a un producto– que ha llegado a permitir la asignación de precios *premium* a un rango de productos en función de la información sobre su origen, procedencia o incluso la técnica de fabricación. Los clásicos ejemplos del vino o del aceite de oliva resultan suficientes para ilustrar cómo, a través de instrumentos de mercadeo, un producto puede ser vinculado a la información de su modo de producción específico, a la proveniencia de un área geográfica o a la intervención de un grupo humano que ha preservado y perfeccionado el proceso de producción. Toda esta información se constituye en factor determinante de la disposición del consumidor a pagar un mayor precio frente a otros vinos o aceites similares.

Pensemos ahora en que la profundización de este discernimiento nos ha conducido al extremo de extrapolar el mismo tipo de análisis de mercadeo al contexto de la valoración de informaciones comercialmente relevantes, pero esta vez vinculadas a los individuos. Tal es el caso de la actividad aseguradora, donde el costo de un individuo asegurable puede determinarse en función de la información a que la aseguradora haya podido acceder respecto del mismo, lo cual puede incluir entre otros: sus hábitos de vida, historia clínica, ubicación geográfica, el tipo de aire que respira, su perfil laboral, sus preferencias sexuales o religiosas, etc. Precisamente, la posibilidad de elaborar perfiles cada vez más detallados sobre los individuos y/o de asociarlos a sistemas de explotación de datos está llamada a generar dramáticos cambios socioeconómicos con efectos potencialmente nocivos en términos de protección de derechos fundamentales. Esta capacidad disruptiva del manejo de los datos es lo que comúnmente identificamos como *data driven economy* o economía basada en los datos (CIURIAK, 2018, p. 12).

Dada la complejidad de los impactos sociales que plantea el desbordado uso del procesamiento algorítmico de información, resulta absolutamente imprescindible volver a las bases del pensamiento filosófico y jurídico que permitieron deducir la existencia de una esfera de derechos intangibles inherente a cada individuo, así como la necesidad de que sea el Estado el encargado de brindar una protección clara y definida de tales derechos.¹

Dicho proceso de evolución de los derechos humanos, así como la idea subyacente de una intangibilidad que los excluye de la lógica de explotación económica —la cual parece hoy fuera de control—, se convierte en un imperativo categórico para poder plantear caminos claros de expansión de la economía digital hacia los espacios cada vez más profundos de una sociedad permanentemente interconectada. En este sentido, la reflexión de J. Habermas, invocada por De Frouville (2004, p. 18), permite un tímido acercamiento a un tema vasto y complejo. El siguiente planteamiento del autor resulta de interés primordial para presentar la discusión:

[...] en efecto, es imposible pensar en la autonomía pública y privada del ciudadano por separado: la institucionalización de los derechos políticos presupone la existencia de derechos que garanticen a todos una cierta libertad privada; pero, a la inversa, es el uso adecuado de la autonomía pública lo que permite una regulación consensuada de la autonomía privada. Los derechos no son, pues, un límite a la soberanía del constituyente, sino una condición de posibilidad del ejercicio del poder constituyente y del derecho en general [...]. Esta percepción de los derechos humanos como fundamento del ordenamiento jurídico se refleja en los ordenamientos internos de los países democráticos —y en particular en Europa— mediante la institución de la protección frente a las infracciones que puedan emanar tanto de los poderes privados como de los públicos. En el derecho privado, la inviolabilidad es, pues, la base de la indisponibilidad, imprescriptibilidad e imposibilidad de renunciar a los llamados “derechos de la personalidad”. Estos derechos, que se definen como derechos inherentes a la persona humana, son considerados por los expertos en derecho civil como derechos extrapatrimoniales, “fuera del comercio”, en el sentido del artículo 1128 del Código Civil. Por tanto, el titular de estos derechos no puede “disponer” de ellos libremente (indisponibilidad), mientras que el paso del tiempo no afecta su validez (imprescriptibilidad). (Traducción libre del autor)

...

1 En materia de intangibilidad de los derechos humanos vale la pena recalcar la naturaleza jurídica de los derechos de autor, en los términos expresados por Plomer (2013, p. 75): “The contrasting undercurrents in eighteenth and nineteenth century philosophies of human rights were reflected in the ideologies that shaped the history of IP law in England, the US, and France. [...] Copyright law in France was grounded in the competing ideology that property rights are ‘pre-political,’ natural rights”.

Consecuente con esta comprensión, la tensión de derechos actual parece ser el resultado del desdibujamiento o erosión de los atributos de lo que en derecho privado se denominaba tradicionalmente como derechos personalísimos —extrapatrimoniales por naturaleza—, los cuales por efecto de la digitalización han dejado su carácter extracomercio para volverse moneda de cambio (*tokens*, dirán algunos) dentro de estas denominadas economías de alcance. En efecto, no es temerario asignar al pensamiento capitalista una tendencia progresiva hacia la monetización de todo cuanto pueda ser aprovechable hasta el punto de llegar a erosionar el carácter intangible de la esfera de derechos de la personalidad, y de convertirlos en simples unidades intercambiables a cambio de prestaciones mercantiles digitalizadas.²

Desde esa perspectiva, la eventualidad de que mediante plataformas como *Study* de Facebook³ se puedan establecer esquemas de remuneración en función de la utilización que se haga de ciertas aplicaciones, no solo resulta extraña desde el punto de vista de la intangibilidad que poseen los derechos a la privacidad, la libertad de expresión o de información, sino que a su vez pone de presente la incompatibilidad de vincular un medio de pago a la disponibilidad de ciertos usuarios para que una misma empresa procese información relacionada con los gustos, preferencias o formas de utilización de dispositivos digitales.⁴ Se abre así una puerta inexplorada y peligrosa para los sistemas democráticos.⁵

De allí que el reconocimiento de la profunda imbricación entre la existencia de garantías públicas como condición de existencia de derechos privados implique que no puede existir

...

2 En este sentido Aillapán (2016) señala: “Esencial en la teoría de los derechos de la personalidad ha resultado la defensa de su cualidad extrapatrimonial. Guzmán señala que el hecho de ser persona es el título que hace sinónimas las expresiones derechos humanos, de la personalidad y extrapatrimoniales; sin embargo, ‘derechos extrapatrimoniales’ sería la terminología comprensiva de todas las anteriores, y la recomendada, pues resalta la característica más notable de estos derechos: carecer de contenido pecuniario. [...] El mismo autor sentencia que la expresión extrapatrimoniales ‘[s]ignifica desde luego lo que literalmente expresa, es decir, que los derechos en examen están fuera del patrimonio. Se quiere significar además que los mismos son ajenos al comercio y a la circulación. Finalmente, que no se pueden avalar en dinero. En suma, que no son bienes”. En síntesis, reconocerles patrimonialidad, traficabilidad o comerciabilidad a los derechos personalísimos significaría autorizar a las personas para enajenar parte de su personalidad subordinando su propio ser a la voluntad de un tercero.

3 Ver: <https://about.fb.com/news/2019/06/study-from-facebook/>.

4 Al respecto, la prensa reseñó este programa en los siguientes términos: “...le nouveau programme se présentera sous la forme d’une application à télécharger sur son Smartphone [...] Sur son site, Facebook liste plusieurs données qui seront enregistrées et envoyées sur ses serveurs: toutes les applications installées sur el téléphone, leur durée d’utilisation, leur type d’utilisation (sans que cela soit spécifié clairement), la géolocalisation, le type de téléphone et le réseau. Study n’est destinée qu’à des personnes majeures, assure Facebook” (SEYDTAGHIA, 2019).

5 Baste con imaginar los nefastos efectos potenciales que pueden surgir al habilitar el uso de plataformas digitales con fines de establecer remuneraciones en función de las preferencias políticas exhibidas por

autonomía de la voluntad donde no existe Estado de Derecho. Esta deformación de los preceptos legales es abordada con elocuente simplicidad por Margareth Radin, citada por Zuboff (2019, p. 49), quien al referirse a la forma en que las plataformas sugieren —y terminan imponiendo— a los usuarios la aceptación de sus condiciones de utilización, afirma:

Las nociones sagradas de “acuerdo” y “promesa”, intrínsecas a la institución del contrato desde la época romana, se han transformado en simples indicaciones al usuario generando una incautación unilateral de sus derechos sin consentimiento. [...] Estos “contratos” son una “degradación” moral y democrática del Estado de Derecho y de la institución del contrato, una perversión que reestructura los derechos de los usuarios concedidos a través de procesos democráticos, “sustituyéndolos por el sistema que la empresa desea imponer” [...]. Los destinatarios deben entrar en un universo jurídico ideado por la empresa para realizar transacciones con ella. (Traducción libre del autor)

Este razonamiento expone apenas uno de los síntomas de las múltiples alteraciones en materia del ejercicio de los poderes estatales, incluida la regulación, la cual en ciertas ocasiones parece estar supeditada a la influencia del poder económico, haciendo aún más palmario el objetivo que, desde sus inicios, trazaron las empresas tecnológicas de sustituir o anteponer sus esquemas autorregulatorios al ejercicio democráticamente legítimo de las potestades públicas. Desafortunadamente, solo la verificación de las consecuencias actuales ha comenzado a nutrir los debates en torno a la necesidad de preservar los *aquis* de la evolución sociojurídica, en los ámbitos privado y público, como único medio para asegurar una economía digital compatible con el respeto de los derechos fundamentales.

2. ¿CONSUMIDORES ANTES QUE CIUDADANOS O *VICEVERSA*?

La ubicación conceptual de las normas de protección al consumidor dentro del ámbito del derecho privado fue detectada como un tema a solucionar en los albores del despegue del comercio electrónico.⁶ Sin embargo, en el entretiem po, la facilidad con la que los consumidores dieron

...

los ciudadanos en sus perfiles en redes sociales, máxime en países como Colombia, donde prácticas censurables como la “compra de votos” son frecuentes y extendidas, generando efectos nocivos para el ejercicio democrático.

⁶ Para Caycedo (2019, p. 140), “[...] los conceptos jurídicos del consumidor y relación de consumo corresponden al esquema de protección del consumidor que adopte cada sistema jurídico, [los cuales] a su vez lo delimitan”. Dicha flexibilidad conceptual es la que ha servido como causa eficiente a la consolidación de una fragmentación regulatoria global en materia de protección al consumidor, con base en la cual la expansión

por aceptada la idea de la existencia de un registro y análisis permanente de todas sus informaciones, con el propósito de perfeccionar las actividades de mercadeo y publicidad, solo puede ser explicada por los beneficios que muchos de esos consumidores creían obtener de la fluidez de la información y de la mejora en sus experiencias dentro de los espacios virtuales donde concretaban las transacciones en línea.

Ahora bien, la realidad subyacente parece ser un poco más compleja: originalmente, la necesidad de flexibilizar el ejercicio regulatorio y de confiar al sector privado la regulación de sus propias actividades obedeció, de cierta manera, a una errónea concepción de las estrategias de inserción en la economía de los datos, la cual tomó como premisa principal el carácter intensivo en capital y conocimiento de las actividades ligadas al procesamiento algorítmico de información; y, a partir de allí, confirió a la inversión privada —y a su predicada capacidad para apalancar grandes inversiones— un rol dinamizador de la innovación, la transferencia y la asimilación de nuevas tecnologías (GESTRIN, 2018).

Fue esta la alternativa seleccionada por muchos de los países en desarrollo como medio para apalancar su crecimiento económico dentro de la loable idea de incursionar en la economía del conocimiento y alejar sus aparatos productivos de las fluctuaciones de los mercados tradicionales de *commodities*. No obstante, de cara a la digitalización, dicha elección no solo no resultó ser el camino más efectivo hacia la inserción en nuevos y sofisticados mercados, sino que, por el contrario, terminó facilitando la consolidación de mercados monopólicos de carácter transnacional, con muy baja participación de empresas locales dentro de la cadena de valor de los productos y servicios digitales.

En paralelo a esta rápida evolución de los mercados digitales, la capacidad de desplegar análisis con base en grandes volúmenes de información, depositada por los usuarios de internet en calidad de consumidores en línea, recibió un impulso incremental mediante la incorporación de las técnicas que las agencias de seguridad habían venido desarrollando y que fueron puestas en funcionamiento con ocasión de los ataques ocurridos en Estados Unidos en septiembre de 2001. Dicho momento, como se desarrollará posteriormente en la sección 3, marcó un punto de inflexión, a partir del cual múltiples empresas decidieron hacer uso de las herramientas de procesamiento algorítmico de información con fines de mercadeo y comercialización a gran escala (CHERTOFF, 2018, p. 73).

Ligado al necesario uso de herramientas tecnológicas —algoritmos— para contrarrestar el riesgo de nuevos actos terroristas, se configuró un ecosistema de libre flujo de información, que a su vez requería la desregulación como factor habilitante para el monitoreo de millones de personas. Fue en tal momento que muchas empresas descubrieron la ausencia

...

de la relativización de la importancia de aspectos vinculados, como la privacidad, se ha ido dando como condición necesaria para el funcionamiento de las economías en red.

o insuficiencia de regulaciones que los disciplinaran, en la esfera mercantil, respecto del despliegue de estrategias invasivas de la privacidad de los consumidores. En tal sentido no resulta temerario afirmar que los vacíos en materia de protección al consumidor en general —y del consumidor digital en particular— han operado como un elemento bisagra que ha facilitado a muchas de las empresas tecnológicas desplegar sus estrategias por fuera de las consideraciones sociojurídicas sobre las cuales tradicionalmente se había entablado la comprensión de la dimensión del consumidor (CAYCEDO, 2019, p. 159).⁷

3. LA ERA DEL *PROFILING*: DEL *SOCIAL RATING* EN CHINA A LA IDENTIFICACIÓN BIOMÉTRICA OBLIGATORIA *AADHAAR* EN INDIA

El tránsito desde la elaboración de simples repertorios biográficos de consumidores, como actividad inherente y necesaria para el comercio digital, hacia la profundización de las actividades de perfilamiento de los ciudadanos (*profiling*) ha sido un proceso paulatino coadyuvado por coyunturas políticas, vertiginosos cambios tecnológicos, pero sobre todo vacíos en el ámbito del derecho privado. Dicho de manera más directa, la posición de dominio que los gigantes tecnológicos ostentan actualmente no hubiera podido consumarse de manera tan satisfactoria, de haber mediado una comprensión técnico-jurídica y un consenso político más claros en torno a los nefastos efectos económicos —y para completar antidemocráticos— que surgirían de la desprotección de los derechos de los consumidores (GONZÁLEZ, 2018, p. 213).

La cuestión se torna, entonces, aún más interesante cuando se descubre que los modelos de predicción que han revolucionado la prestación de servicios en línea, son el resultado de la monetización de una parte de nuestra realidad que, como quedó sentado en la sección anterior, hasta el momento había estado protegida en el marco de la economía de mercado, mediante normas estatutarias de protección a los derechos a la privacidad, la imagen, la información, y normas de derecho privado que establecían un carácter extracomercio.

En efecto, un repaso a la forma como se ha dado la penetración de internet en países en desarrollo deja al descubierto la intención de ofrecer soluciones y experiencias a sectores de la población con capacidad de consumir bienes a través de intercambios *P2P*. Esta propuesta de internet, en principio elitista, se vio rápidamente superada por la oportunidad real de crear

...

⁷ De acuerdo con Caycedo (2019, p. 156), la normativa mercantil desechó el criterio subjetivo —el comerciante— como mecanismo definitorio de su ámbito de aplicación. Son los criterios objetivos—los actos de comercio y de la empresa—los que definen el ámbito de aplicación de la ley comercial. En el código de comercio se prevé igualmente que no tiene carácter mercantil la “adquisición de bienes con destino al consumo doméstico o uso del adquirente”, pero, aunque parece excluir al acto de consumo del ámbito de aplicación de la ley mercantil, simultáneamente, bajo la regla de atracción del acto mixto, dispone que esas transacciones se regirán por la ley comercial cuando son actos de comercio para quien suministra o enajena dichos bienes”.

nuevos y masivos mercados basados en la conectividad intensiva que conocemos actualmente, que ha dado lugar incluso a su categorización como derecho fundamental. Sin embargo, en la actualidad, y una vez escrutada la complejidad técnica, la aparente magia de la predicción de las preferencias se ha revelado como el resultado del despliegue de actividades de seguimiento (*web tracking*) que son, en última instancia, las que permiten determinar o inferir, a partir de informaciones colectadas, los gustos, preferencias o predilecciones por las que nos inclinaremos bajo ciertas circunstancias. Siguiendo a Röttgen (2018, p. 73):

Web tracking enables recording and analysis of user behaviour and comes along in various manifestations. The use of cookies and social-plugins on websites, for instance, allows identifying how often a user visits a concrete website and which content he or she is interested in. Through this, companies “decode” the user behind its data and are able to provide targeted advertising [...]. Through the establishment of smartphones and tablets web tracking achieved a new level of user analysis. *App Tracking* allows a cross-application identification of the user. Depending both on the apps that are installed as well as how (or not) the user configured his smartphone, location data, surfing behaviour and other information is recorded. Those apps, which record location data and allow extensive analysis, are, regardless of the service offered, often for free. There are considerable doubts that these apps are for free, actually [...] the user “pays” by the disclosure of his data.

Ahora bien, devolver el péndulo hacia una protección de la privacidad en cabeza de entes gubernamentales parecería la salida lógica y la reacción apropiada de cara a los comprobados o potenciales efectos nocivos que surgen, o podrían surgir, de la descontrolada monetización de la información. Sin embargo, y por ahora, la incursión de las administraciones públicas en el tratamiento algorítmico de información no parece ser la vía ideal para restablecer el equilibrio descompuesto en materia de garantías y derechos fundamentales que hoy tenemos como consecuencia de la disrupción digital.

3.1. DE LA LUCHA CONTRATERRORISTA A LA BATALLA EPIDEMIOLÓGICA

El apetito por los datos que caracteriza el momento actual de la economía digital no es nuevo. Desde los albores del desarrollo de internet, la idea de coleccionar y organizar grandes volúmenes de información estuvo presente y fue en sí misma el aliciente para que muchas empresas buscaran convertir la red en el medio eficiente para la expansión de novedosos y prometedores servicios. Desde otra perspectiva, este mismo dinamismo de la digitalización ha generado nuevos riesgos para las empresas, los individuos y los Estados. Es así como en menos de dos décadas el fenómeno del ciberterrorismo ha pasado de ser parte del imaginario de las películas de ficción a constituir todo un nuevo escenario de acción y de contención en la esfera de las relaciones internacionales entre Estados (RIORDAN, 2019, p. 80).

Esta curiosa relación entre proliferación de los efectos en red, disponibilidad de información en línea, consentimiento para conectarse y necesidad de marcos regulatorios no es resultado del azar. Por el contrario, la consolidación de los mencionados efectos de las economías en red es la consecuencia de una instrumentalización progresiva de los datos, desplegada por empresas del sector privado y en algunos casos con participación de las administraciones públicas. Algunos autores señalan acertadamente el tránsito desde la simple disponibilidad de información (*sharing of information*) a una etapa avanzada de vigilancia permanente (*permanent surveillance*). Puntualmente, Chertoff (2019, p. 71) lo ilustra en los siguientes términos:

The notable changes in surveillance and security requirements came in the wake of the traumatic attacks suffered on September 11, 2001 [...] new demands transformed intelligence gathering from traditional espionage targeting foreign leaders and officials to the more difficult effort to find a terrorist needle in the haystack of a civil population.

La sofisticación de las actividades de perfilamiento es en última instancia el resultado del carácter esencial para la lucha contra flagelos transnacionales. Este cambio tácito ha logrado actualmente que “[...] aproximadamente la mitad de los adultos estadounidenses – la gran mayoría no delincuentes– tengan imágenes de su rostro almacenadas en bases de datos accesibles al FBI [...]” (THE ECONOMIST, 2018), lo cual, como es bien sabido, ha dado lugar a suspicacias en torno a la posibilidad de que las autoridades avancen sus líneas rojas y “entrenen” sus algoritmos de predicción de delitos de manera intencional para perseguir determinadas comunidades o identidades culturales.

3.2. ESFERAS DE RASTREO

Casos relevantes, que dan cuenta del uso del tratamiento algorítmico por parte de entes estatales, son el sistema de *Social Credit* que viene funcionando en países como China o de manera más indirecta el programa de identificación biométrica *Aadhaar* en India. Ambos sistemas se declaran concebidos para lograr una asignación más eficiente de los recursos públicos que se destinan a programas sociales o a recompensar o castigar comportamientos reprochables por la sociedad. Como puede intuirse, la línea difusa que se plantea entre los fines de mejoramiento de la gestión y la intrusión en la esfera privada de los individuos es un tema inexplorado y, por lo tanto, la precaución frente al uso de estas tecnologías debería ser la premisa que oriente su aplicación, pues tal como se ha expresado:

The crux of the problem when it comes to social credit is the way it ascribes moral value to certain behaviours, introducing an all-encompassing, quasi-religious aspect to the political system. It’s the nail in the coffin for a dictatorial government, solidifying its hold on the population. [...] For example, points can be given for “good” behaviour

such as doing charity work or helping family member, or deducted for jaywalking, spending too long playing video games or wasting money on “trivial purchases”. (PERRYER, 2019)

Es claro que la necesidad de ejercer control por parte de las autoridades, la cual tiende a ser más rigurosa en regímenes totalitarios, ha encontrado en el *big data* una herramienta propicia para consolidar la aplicación de castigos y recompensas en función de la adhesión a los postulados oficiales. Esta coerción de las libertades individuales tiende a ser aceptada como una fatalidad, pues a través de ella los ciudadanos, en su faceta de consumidores, se aseguran la posibilidad de acceder a los beneficios de la economía de plataformas. En este punto, resulta curioso apreciar la forma en que los postulados económicos, que fundamentan las economías de alcance (*scope*), terminan inspirando y justificando la sumisión ciudadana a la experiencia de un gobierno digital omnipresente y de contera omnipotente.

De manera análoga, la promesa de irradiar la prosperidad económica y social a través del control de la información biométrica ha encontrado eco en el contexto de iniciativas como *Aadhaar*. Esta “manera de pensar” la gestión pública, a través de la creación de bienes públicos (bases de datos), plantea retos en cuanto a la habilidad de los ciudadanos para distinguir los escenarios y discernir los efectos que surgen de la puesta a disposición de datos sensibles (RAMNATH y ASSISI, 2019, p. 240), condensando esta problemática dentro del concepto de plataforma social:

A Societal Platform is built on the premise that the most precious commodity in the world today is data. So far, data is owned by government or the business that collects it. In the framework of Societal Platforms, though, the underlying premise is that data belongs to the individual. An individual may consent to share it with regulatory authorities to comply with norms or private entities if he or she thinks it appropriate.

Justamente, las barreras en materia de información son relevantes en el momento de negociar el acceso a información personal, y es desde esta perspectiva que la existencia de estándares de protección, decantados a partir de la práctica privada y/o incorporados en las relaciones con la administración, puede resultar determinante para orientar la decisión informada de los ciudadanos de hacer disponibles sus informaciones personales, y aún más importante de hacerlo basado en elecciones racionales, tal como se concibe dentro de la noción de autodeterminación informática, la cual será objeto de algunos comentarios en la parte final del artículo.⁸

...

8 Con relación a este concepto, Thouvenin (2021, p. 248) afirma: “La idea y el concepto de autodeterminación informática se refieren al derecho y la oportunidad de cada persona de determinar qué informa-

3.3. DESPLIEGUE DE LAS APLICACIONES DE *TRACKING*

El advenimiento de la crisis provocada por el Covid-19 es particularmente interesante de cara al momento de transformación tecnológica que ya experimentaba la sociedad global de la información. En efecto, con antelación a la crisis sanitaria, los esfuerzos de muchos empresarios y académicos estaban centrados en encontrar un lugar propicio para los nuevos desarrollos tecnológicos, categorizados dentro de la denominada cuarta revolución industrial (4RI). La deriva tecnológica permitía intuir un nuevo rol aumentado para muchas de las aplicaciones y sobre todo para las actividades de minería de datos que surgen como resultado de la configuración normal de grandes volúmenes de información y que, como bien los describimos anteriormente, se venían probando como beneficiosas en contextos tales como el de la lucha anti-terrorista, el lavado de activos o la lucha contra el crimen transnacional. Ante el arribo de un nuevo y ubicuo enemigo global, la información y la capacidad de interpretación de los datos aparecieron rápidamente dentro del radar de los gigantes tecnológicos quienes, en el marco de la economía desregulada de Estados Unidos, no vacilaron en aumentar sus apuestas por una solución tecnológica. De acuerdo con Al Dahdah y Javed (2020), al inicio de la crisis:

Neither the US nor the European Union have adopted a digitally-based tracing policy so far. In the United States, there is no contact tracing system at federal level, the US government adopting a liberal and market based approach, the development of such digital contact-tracing systems was mostly taken up by tech companies. Apple and Google are collaborating for an application programming interface (APIs) using Bluetooth Low Energy (BLE) principles that will be rolled out for iOS and Android in May. Apple and Google say that proximity tracking will be built-in feature for upcoming operating systems to help ensure broad adoption.

De esta manera se fue construyendo el núcleo (*core*) de lo que han sido la mayoría de las respuestas tecnológicas a la crisis sanitaria, las cuales deben ser apreciadas como lo que realmente son: una oportunidad de capturar valor a partir de la explotación de los datos que masivamente los ciudadanos están dispuestos a compartir con miras a solucionar un problema común que afecta el funcionamiento normal de muchas de sus actividades (THE ECONOMIST, 2020).

...

ción sobre sí misma se revela a otros y para qué fines puede utilizarse esa información. [...] El término y la idea han tenido una exitosa carrera en el pensamiento jurídico y en el debate público, al menos en Europa, donde el derecho a la autodeterminación informática se ha convertido en uno de los fundamentos conceptuales del derecho a la protección de datos personales consagrado en el artículo 8 de la Carta de los Derechos Fundamentales de la Carta de Derechos Fundamentales de la Unión Europea”.

Surge, por lo tanto, la necesidad de balancear no sólo la efectividad de las soluciones técnicas propuestas, sino su oportunismo frente a la posibilidad ampliada de acceder a un mayor espectro de información. A priori, se podría afirmar que la actividad regulatoria debería ponderar este momento particular antes de proceder a autorizar el despliegue de aplicaciones con capacidad de derivar en fallos sistémicos que afecten derechos fundamentales de gran alcance, como lo son la salud, la educación, el trabajo y, desde luego, la privacidad.

3.3.1. DIFERENTES APROXIMACIONES

- *Israel: HaMagen 2.0 “a small step for the citizen, a giant step for the state”*

El despliegue de esta aplicación resulta especialmente ilustrativo en la medida en que la población del Estado de Israel es ampliamente reconocida por compartir una percepción del riesgo bastante rígida como resultado de las constantes presiones que suscita el conflicto político y territorial. En estas circunstancias, el punto de partida de la autoridad sanitaria se apoyó en una profundización de la percepción de seguridad, la cual frente a la situación sanitaria imponía nuevos parámetros de acción.

La utilización de dos plataformas paralelas: *HaMagen*, de carácter civil y construida dentro de una lógica *opt in*, compite con una aproximación más restrictiva embebida en la aplicación *Shin Bet*, la cual es la base del sistema de vigilancia estatal, apoyada en los desarrollos de los sistemas GPS que permiten desplegar una trazabilidad inversa para ubicar la fuente de un contagio a partir del análisis de los datos captados por los dispositivos móviles. Esta oferta dual abrió la posibilidad a posiciones matizadas, como la expuesta por Toi Staff (2020):

Many Israelis have criticized the Shin Bet program, both due to civil rights concerns and because a growing number of people have said that they were being forced to stay home by mistake, likely due in part to technology that fails to discern whether two people were actually within six feet of each other, close enough to transmit the virus. Additionally, people said calls to the Health Ministry routinely go unanswered as officials say the system has been overwhelmed.

Este ecosistema digital dual parece hacer compatibles dos visiones diferentes compartidas por los ciudadanos y, por ende, su funcionamiento se ha planeado dentro de una lógica de arenera regulatoria (*sandbox*) en virtud de la cual las dos aproximaciones compiten por mostrar su efectividad e inocuidad en materia de afectación de los derechos civiles.

- *Suiza: SwissCovid y el “traçage de proximité”*

La iniciativa del Gobierno Suizo consistió en promover el uso de una aplicación estatal que hace uso de la interfaz *Bluetooth Low Energy* (BLE), incorporada en los teléfonos inteligentes, la cual permitía configurar un sistema de alertas al suscriptor, creando la posibilidad de notificarlo

en el caso de haber estado en proximidad con potenciales personas infectadas (MONTAVON, 2021, p. 595).

Actualmente, el uso de este sistema es completamente facultativo y permite a los dispositivos generar IDs aleatorios en función de la proximidad y el tiempo entre dos dispositivos. Estos contactos generados son almacenados en cada dispositivo por periodos de catorce (14) días y solo se comunican en caso de que uno de los usuarios reporte haber estado contagiado, generando automáticamente el aviso a los demás dispositivos para que la alerta sea transmitida y los usuarios involucrados tomen las medidas necesarias para cortar la cadena de transmisión del virus.

La percepción del riesgo ha jugado un papel crucial y, a diferencia del caso de Israel, la preeminencia de una visión que privilegia el respeto por las libertades individuales ha generado resistencia en una porción importante de la población; a noviembre de 2020, solamente 1.84 millones de personas habían activado y reportaban el uso de la aplicación, razón por la cual el Gobierno Federal ha tenido que insistir en la importancia de generar efectos en red respecto de la descarga y uso de la aplicación.

- *Francia y la UE: prevalencia del control epidemiológico*

A pesar de los esfuerzos preliminares por sustraer el monitoreo de la pandemia de los estándares puestos a disposición por los gigantes tecnológicos, tanto Francia como Alemania terminaron por abandonar el denominado *Pan-European Privacy-Preserving Proximity Tracing* (PEPP-PT) y acordaron la adopción de sistemas descentralizados basados en la interfaz *Bluetooth Low Energy* (BLE), la cual permite, como en el caso de Suiza, garantizar una localización temporal en cada dispositivo y en condiciones de anonimización suficientes para los fines de control epidemiológico. Es de resaltar que la decisión asumida por la UE reflejó en su momento, una clara apuesta por el pragmatismo, dando prevalencia a la evaluación del estado de la técnica, enfocada en que la implementación de mecanismos de trazabilidad no implique más esfuerzos que los necesarios para garantizar el uso adecuado y proporcional de las tecnologías disponibles.

Habiendo dejado claro el panorama en que se desenvuelven las discusiones sobre el uso de las tecnologías de rastreo y de sus fronteras con el respeto por los derechos y garantías fundamentales, queda pendiente la discusión en torno al carácter facultativo del uso de estas aplicaciones. Tal y como ya se ha evocado en el desarrollo de esta discusión, el valor de las aplicaciones de rastreo está en la capacidad de generar efectos en red y de vincular los mismos a la “creación de valor”, que en el caso apremiante de la Covid-19 es el de permitir reconfigurar la normalidad trastocada, lo que en definitiva puede ser considerado como el restablecimiento de la confianza, la libre circulación y la movilidad como bienes públicos.

Desde dicha perspectiva, cada uno de los enfoques presentados tuvo que asumir el costo social que generaba la desconfianza en las tecnologías y la opacidad denunciada por organizaciones de la sociedad civil en relación con la utilización de la información que se puede

colectar con el despliegue de aplicaciones que, aunque dicen rastrear la ocurrencia de contagios, pueden terminar por proveer información sobre otros aspectos íntimos de la vida e intereses de los ciudadanos. En los tres casos analizados, la herramienta propuesta por las autoridades sanitarias para lograr influenciar la aceptación y uso de las aplicaciones de rastreo es la anonimización, respecto de la cual existen recurrentes dudas, por la manera en que el perfeccionamiento de la criptografía inherente a dicho proceso dejaría abiertas las puertas a modelos matemáticos que permiten de una forma u otra la regresión al origen del emisor de un mensaje.

4. LAS DISCUSIONES EN TORNO A LA AUTODETERMINACIÓN INFORMÁTICA

A lo largo de la presente discusión teórica se ha señalado un panorama de instrumentalización de la economía digital en general y de los datos en particular, que tiene como telón de fondo una intensa actividad de procesamiento algorítmico adelantada indistintamente por empresas privadas y al mismo tiempo, y progresivamente, por entidades públicas. En efecto, la profundización de las relaciones mercado-entornos digitales ha contribuido a fortalecer sectores específicos abriendo oportunidades de creación de valor frente a temas que otrora eran exclusivos del resorte de las agencias de inteligencia de los Estados. Este dinamismo actual del mercado de soluciones en materia de seguridad tecnológica y ciberseguridad es abordado por Zuboff (2019, p. 172) en los siguientes términos:

[...] la vigilancia en el interés de la captación y venta de excedentes de comportamiento se ha convertido en un servicio por derecho propio. Estas empresas suelen denominarse “software-as-a-service” o SaaS, pero es más preciso denominarlas “vigilancia como servicio” o “SVaaS”. Por ejemplo, un nuevo enfoque basado en una aplicación para la concesión de préstamos establece instantáneamente la solvencia crediticia basándose en la minería detallada del Smartphone de un individuo y otros comportamientos en línea, incluyendo textos y correos electrónicos, coordenadas GPS, publicaciones en redes sociales, perfiles de Facebook, transacciones minoristas y patrones de comunicación [...] el método cuantifica aspectos ricos del comportamiento típicamente considerados como información “blanda”, haciéndola legible para las instituciones formales.

Conforme con esta comprensión, el flujo creciente de datos en los mercados digitales hace indispensable la distinción entre el procesamiento de datos efectuado por autoridades públicas de aquel que se realiza por parte de empresas del sector privado. Esta distinción, a primera vista trivial, resulta relevante en la medida en que el desarrollo actual de la noción de “autodeterminación informática” se encuentra circunscrito a la facultad de los particulares de oponerse a los poderes públicos con el fin de proteger las informaciones personales.

Ahora bien, el hecho de que la misma facultad de determinar la disponibilidad de información personal frente a una empresa privada no dependa exclusivamente del consentimiento del titular de los datos, sino del denominado “interés legítimo del controlador” (LYPALO, 2021, p. 170), pone de presente un elemento que ha sido transversal a todo el desarrollo de internet que es el de privilegiar la innovación permanente de productos y servicios digitales aun en desmedro de la intangibilidad de los derechos personalísimos.

Esta confusa comprensión de la dinámica de los mercados digitales parece estar fragilizando aún más la posibilidad de que los entes reguladores puedan configurar entornos regulatorios lo suficientemente robustos para facilitar la innovación en estos nuevos mercados y asegurar la transparencia a los usuarios respecto de la intangibilidad de los derechos fundamentales, que como en el caso de la privacidad, aparecen altamente comprometidos a través de la interacción con estas tecnologías. Por otro lado, los efectos desproporcionados de la crisis sanitaria, en términos de afectación a los derechos a la autodeterminación informática, plantean la urgente necesidad de que el Estado haga uso de novedosos instrumentos de construcción de marcos regulatorios que permitan procesos continuos de prueba y error, sin tener que incurrir en los costos de legitimidad que implica la inflación normativa frente a los nuevos fenómenos tecnológicos y sus efectos sociales. Subyacente a esas preocupaciones, surge la necesidad de preservar la intangibilidad del derecho a la privacidad en momentos en que la conjunción entre la ampliada capacidad tecnológica y necesidad de controlar un evento pandémico parecen haberse unido para crear una nueva realidad con prescindencia de ciertos derechos fundamentales. Oponerse a la tiranía de los datos debería dar lugar a crear posibilidades técnicas para que los individuos puedan decidir libremente sustraerse de la obligación de instalar en sus dispositivos mecanismos de rastreo que puedan eventualmente devolverse contra sí mismos en la forma de perfiles elaborados por organismos de seguridad estatales o por empresas privadas con fines publicitarios o comerciales. Uno de los elementos de base dentro de la discusión para habilitar este tipo de excepciones lo constituye el carácter intangible que globalmente se reconoce a la protección de la personalidad y, en general, a los derechos humanos.⁹ En tal sentido, es pertinente retomar la reflexión que De Frouville (2004, p. 519) hace sobre el pensamiento de Habermas, y su alcance en el contexto de la interdependencia generada por la globalización, al afirmar:

...

⁹ Un primer paso en esta dirección lo constituye la reciente decisión de uno de los gigantes tecnológicos de modificar la capacidad de los anunciantes para entregar publicidad dirigida. Dicha decisión ha causado revuelo en la industria de marketing digital, pues se teme que si las personas pueden no aceptar el rastreo, disminuirán considerablemente los datos que permiten los perfilamientos. Al respecto ver: <https://www.cnbc.com/2020/12/15/apples-seismic-change-to-the-mobile-ad-industry-draws-near.html>.

Habermas llega a la conclusión de que es necesario y suficiente, para hacer frente a los desafíos de la interdependencia y la globalización, crear las condiciones en las que se pueda desarrollar una política interna global. En esta etapa, su concepción democrática del derecho, basada en una ética de la discusión, exige la construcción de un espacio público transnacional [...]. Los Estados deben por lo tanto colocarse en una posición de duplicación funcional. Los Estados solo adoptan esta posición cuando los intereses mundiales que están llamados a defender no contradicen sus intereses nacionales.

Esta proposición parece cobrar un sentido especial en el contexto de los desafíos que plantean simultáneamente la crisis sanitaria y la penetración abusiva de la economía digital en la esfera de los derechos fundamentales. La construcción del espacio público transnacional evocada por Habermas es pues la tarea pendiente que permitirá a los Estados afrontar en igualdad de condiciones a las empresas transnacionales que amenazan con su ejercicio oligopólico las condiciones mismas de la sociedad global a la que creíamos haber arribado.

CONCLUSIÓN

La asignación de valor a los bienes intangibles o inmateriales está en el centro de los fenómenos socioeconómicos que han permitido el despliegue omnímodo del capitalismo tal como lo experimentamos en los entornos digitales. La importancia de la noción de autodeterminación informática radica en que pone de presente el vínculo que se crea entre la información y su titular. Esta particularidad es especialmente importante de cara a las posibilidades de explotación que surgen en contextos caracterizados por complejos flujos de información y permanente tratamiento algorítmico. El *web tracking* pone de manifiesto, como ninguna otra actividad ligada al comercio electrónico, la conjunción o incluso simultaneidad de actividades de minería de datos por parte de agentes públicos y privados. La fragmentación regulatoria en materia de derechos del consumidor, que ha operado como un factor distorsionante en la aplicación del concepto de autodeterminación informática, es un tema urgente dentro de las agendas regulatorias, que, de ser solucionado, permitiría definir las esferas de control que buscan ejercer algunas plataformas digitales, las cuales ostentan en la actualidad un significativo poder de mercado.

En un plano más filosófico, es necesario reconocer que el carácter intangible propio de la información ha venido evolucionando de manera vertiginosa, entre muchas razones, debido al perfeccionamiento de la capacidad de generar valor a partir del análisis e interpretación de los datos (*data analytics*). Las reflexiones en torno al valor que asumen bienes intangibles, tales como la información que se genera sobre las actividades de personas, comunidades o grupos específicos deberían orientarse a atribuir una valoración más allá de la simple explotación comercial que puede suscitarse a partir del uso de esta nueva materia prima. Una postura coherente frente a la propuesta actual, de esquemas de remuneración basados

en plataformas, debe reconocer los riesgos en materia de erosión de la esfera de derechos y, por ende, de la banalización de los procesos históricos que han permitido la evolución de instituciones universales de protección de los derechos humanos. Es claro que ante la evidencia de la realidad tecnológica que nos arrolla, hoy más que nunca se hace urgente y necesario retomar los principios del pensamiento jurídico y filosófico de manera que nos permitan comprender y oponernos con mayores posibilidades de éxito a la excesiva monetización de la información personal.

REFERÊNCIAS

AILLAPÁN, Jorge Eduardo. El derecho a la propia imagen: ¿Derecho personalísimo?, ¿Derecho fundamental? Precisiones terminológicas para el caso chileno. *Revista Chilena de Derecho*, Santiago, v. 43, n. 2, p. 433-459, 2016.

AL DAHDAH, Marine; JAVED ALAM, Mohammad. Tracing Apps to Fight Covid-19. Are Surveillance Technologies Effective? *Books, and Ideas*, Paris, 18 may. 2020. Disponible en: <https://booksandideas.net/Tracing-Apps-to-Fight-Covid-19.html>. Consultado el 5 de noviembre de 2020.

ALLAIRE, Gilles. The Ambivalence of Agriculture Capitalist Socialization. In: ALLAIRE, Gilles; DAVIRON, Benoit. *Ecology, Capitalism and the New Agricultural Economy: The Second Great Transformation*. New York: Routledge, 2019.

BIG Tech Faces Competition and Privacy Concerns in Brussels. *The Economist*, London, 23 mar. 2019. Disponible en: <https://www.economist.com/briefing/2019/03/23/big-tech-faces-competition-and-privacy-concerns-in-brussels>.

CAYCEDO, Carlos. Protección constitucional al consumidor en Colombia. *Serie de Derecho Económico*, Bogotá D.C., Universidad Externado de Colombia, n. 4, p. 131-178, 2019.

CHERTOFF, Michael. *Exploiting Data, Reclaiming our Cyber Security in the Digital Age*. London: Grove Press, 2018.

CIURIK, Dan. The Economics of Data: Implications for the Data-Driven Economy. *Data Governance in the Digital Age*, Centre for International Governance Innovation, Ontario, p. 236, 2018.

DE FROUVILLE, Olivier. Don't Rely on Contact-Tracing apps. *The Economist*, London, 16 may. 2020. Disponible en: <https://www.economist.com/leaders/2020/05/16/dont-rely-on-contact-tracing-apps>.

DE FROUVILLE, Olivier. *L'Intangibilité des droits de l'homme en droit international, regimen conventionnel des droits d'homme et droits des traites*. Paris: Pedone, 2004.

GARCÉS, Eliana. The Dynamics of Platform Business Value Creation. *CPI: Competition Policy International*, Chicago, 14 ago. 2017. Disponible en: <https://www.competitionpolicyinternational.com/the-dynamics-of-platform-business-value-creation/>. Consultado el 09 de agosto de 2020.

GONZÁLEZ, Laura Daniela. Germany Switches to Google and Apple on Virus Tracing App over Privacy Concerns. *The Local*, Berlin, 27 abr. 2020. Disponible en: <https://www.thelocal.de/20200427/germany-switches-to-google-and-apple-on-coronavirus-tracing-app-over-privacy-concerns>. Consultado el 10 de diciembre de 2020.

GONZÁLEZ, Laura Daniela. Control de nuestros datos personales en la era del *big data*: El caso del rastreo web de terceros. *Revista Estudios Socio-Jurídicos*, Universidad del Rosario, Bogotá, v. 21, n. 1, p. 209-244, 2018.

GESTRIN, Michael; STAUDT, Julia. The Digital Economy, Multinational Enterprises and International Investment Policy. *OECD*, Paris, 2018. Disponible en: www.oecd.org/investment/the-digital-economy-mnes-and-international-investment-policy.htm. Consultado el 06 de mayo de 2020.

GRAHAM, Megan. Apple's Seismic Change to the Mobile Ad Industry Is Drawing Near, and It's Rocking the Ecosystem. *CNBC*, London, 15 dic. 2020. Disponible en: <https://www.cnbc.com/2020/12/15/apples-seismic-change-to-the-mobile-ad-industry-draws-near.html>. Consultado el 17 de diciembre de 2020.

HELLER, Nathan. Is the GIG Economy Working? *The New Yorker*, New York, 15 may. 2017. Disponible en: <https://www.newyorker.com/magazine/2017/05/15/is-the-gig-economy-working>. Consultado el 15 de agosto de 2020.

LÓPEZ, José Ignacio; ARROYO, José Luis. Externalidades de Red en la Economía Digital: Una Revisión Teórica. *Revista de Economía Industrial*, Madrid, n. 361, p. 21-32, 2006. Disponible en: <https://eco.mdp.edu.ar/cendocu/repositorio/01017.pdf>. Consultado el 17 de junio de 2020.

LYPALO, Dzhuliia. Can Competition Protect Privacy? An Analysis Based on the German Facebook Case. *World Competition, Law and Economics Review*, Wolters Kluwer, Alphen aan den Rijn, v. 44, n. 2, p. 169-198, 2021.

MONTAVON, Michael. *Cyberadministration et Protection des Données*. Zürich: Schulthess Verlag, 2021.

PERRYER, Sophie. China's Social Credit System Awards Points to Citizens Who Conform. *The New Economy*, London, 22 may. 2019. Disponible en: <https://www.theneweconomy.com/strategy/116498>. Consultado el 01 de septiembre de 2019.

PLOMER, Aurora. The Human Rights Paradox: Intellectual Property Rights and Rights of Access to Science. *Human Rights Quarterly*, v. 35, n. 1, p. 143-175, 2013. doi: 10.1353/hrq.2013.0015

RAMNATH, N. S.; ASSISI, Charles. *Aadhaar Effect: Why the World's Largest Identity Project Matters*. New Delhi: Oxford University Press, 2018.

RIORDAN, Shaun. *Cyberdiplomacy*. London: Polity, 2019.

RÖTTGEN, Charlotte. Like or Dislike – Web Tracking. In: HOEREN, Thomas; KOLANY-RAISER, Barbara. *Big Data in Context: Legal social and technological Insights*. Berlin: Springer, 2018.

SEYDTAGHIA, Anouch. Facebook paiera pour devenir voyeur. *Le Temps*, Ginebra, 14 jun. 2019. Disponible en: <https://www.letemps.ch/economie/facebook-paiera-devenir-voyeur>.

SOKOL, Sam. Health Ministry Launches Revamped COVID-19 Tracking App. *The Times of Israel*, 27 jul. 2020, Disponible en: <https://www.timesofisrael.com/health-ministry-launches-revamped-covid-19-tracking-app/>. Consultado el 20 de agosto de 2020.

STAFF, Toi. Lawmakers Extend Shin Bet Phone Tracking by 10 Days, But Voice Reservations. *The Times of Israel*, 06 sep. 2020. Disponible en: <https://www.timesofisrael.com/lawmakers-extend-shin-bet-phone-tracking-by-10-days-but-voice-reservations/>. Consultado el 15 de diciembre de 2020.

SWISSCOVID, 2020. Disponible en: <https://www.covidtracker.ch/en/>. Consultado el 09 de octubre de 2020.

SWISSCOVID, 2020. Disponible en: <https://www.epfl.ch/campus/security-safety/en/health/coronavirus-covid19/swisscovid/>. Consultado el 09 de octubre de 2020.

THOUVENIN, Florent. Informational Self-Determination: A Convincing Rationale for Data Protection Law? *JIPITEC: Journal of Intellectual Property, Information Technology and E-Commerce Law*, v. 12, n. 4, 2021. Disponible en: https://www.jipitec.eu/issues/jipitec-12-4-2021/5409/thouvenin_pdf.pdf. Consultado el 10 de diciembre de 2021.

ZUBOFF, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books, 2019.

CÓMO CITAR ESTE ARTÍCULO:

CORREDOR-CASTELLANOS,
Guillermo Rodrigo. Aplicaciones de
rastreo y monitoreo: del entusiasmo
tecnológico al reconocimiento de la
autodeterminación informática.
Revista Direito GV, São Paulo, v. 18, n. 2,
maio/ago. 2022, e2225. [https://doi.org/
10.1590/2317-6172202225](https://doi.org/10.1590/2317-6172202225)

Guillermo Rodrigo Corredor Castellanos

DOCENTE INVESTIGADOR, DEPARTAMENTO DE DERECHO
ECONÓMICO DE LA UNIVERSIDAD EXTERNADO DE COLOMBIA.

rodrigo.corredor@uexternado.edu.co