LA VERIFICABILIDAD DEL CONSENTIMIENTO EN LAS TRANSACCIONES ELECTRÓNICAS
Recomendaciones valorativas para su abordaje integral en el Derecho argentino

THE VERIFIABILITY OF CONSENT IN ELECTRONIC TRANSACTIONS
Evaluative recommendations for its comprehensive approach in the Argentine legal system

MATÍAS PARMIGIANI*

RESUMEN

¿Qué responsabilidades le caben al operador de una plataforma digital a la hora de verificar el consentimiento de un usuario o cliente que facilita sus datos personales en una transacción electrónica, ya sea a título oneroso o gratuito? El Derecho argentino pretende regular este asunto mediante la Ley de Protección de Datos Personales (Ley 25.326), en la que se constatan algunos artículos no exentos de vaguedad. El objetivo del presente trabajo consistirá en ofrecer una serie de recomendaciones valorativas para una correcta interpretación de esta ley, aunque su alcance podría ser más amplio y general.

Palabras clave: verificación del consentimiento; transacción electrónica; datos personales; Google; Sunstein.

ABSTRACT

What are the responsibilities of a digital platform's operator when it comes to verify the consent of a user or costumer who provides their personal data in an electronic transaction, whether in return for payment or free of charge? The Argentine legal system seeks to regulate this matter through the Personal Data Protection Law (Law 25,326), some of whose articles are not exempt from vagueness. The objective of this paper will be to offer a series of evaluative recommendations for a correct interpretation of this law, although they may have a wider and more general scope.

Key words: verification of consent; electronic transaction; personal data; Google; Sunstein.

*Investigador de CONICET (Centro de Investigaciones Jurídicas y Sociales), Profesor de la Facultad de Derecho y Ciencias Sociales (Universidad Nacional de Córdoba) y Profesor de la Universidad Empresarial Siglo 21, Córdoba (Argentina). E-mail: matias.parmigiani@unc.edu.ar.

El art. 5 de la Ley de Protección de Datos Personales (Ley 25.326) establece en su inciso 1 que "el tratamiento de datos personales ***es ilícito*** cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, ***de acuerdo a las circunstancias***". Al mismo tiempo, el art. 32 de esta ley establece las sanciones administrativas que el organismo de control podrá aplicar, "sin perjuicio de las responsabilidades administrativas que correspondan en los casos de responsables o usuarios de bancos de datos públicos; de la responsabilidad por daños y perjuicios derivados de la inobservancia de la presente ley, y de las sanciones penales que correspondan". Entre las medidas administrativas previstas, se mencionan las siguientes: "***sanciones de apercibimiento, suspensión, multa de mil pesos ($ 1.000.-) a cien mil pesos ($ 100.000.-), clausura o cancelación del archivo, registro o banco de datos***".

Lo primero que llama la atención es la indefinición de esta ley. ¿Cómo debe leerse la última parte del art. 5? Por empezar, considérese un caso como el siguiente: una compañía (C) que ofrece sus servicios a través de un sitio web realiza una transacción comercial con un particular (P), de quien obtiene algunos datos personales vinculados a su cuenta bancaria. Sin embargo, al pasar los días, P se percata de que sus datos han sido manipulados por un tercero. Puesto que no ha sido el titular de la cuenta quien ha prestado su consentimiento, se plantea la pregunta de si a C le cabe alguna clase de sanción por no haberse tomado la molestia de ***verificar*** la identidad de su cliente. Tal como la ley está planteada, los requisitos de verificabilidad del consentimiento se reducen a dos notas disyuntivas: por un lado, a que el mismo se haya manifestado por escrito; o, en su defecto, a que lo haya sido por otro medio equiparable, de acuerdo a las circunstancias. Ahora bien, según nos consta, muchos de los contratos que hoy se celebran en la web, como los contratos «*browsewrap*» o «*clickwrap*», exigen que se completen ciertos formularios, sin que la parte que ofrece el servicio pueda estar al tanto de la verdadera identidad de su firmante.

El problema que quisiera explorar en este trabajo está relacionado con la responsabilidad que les cabe a quienes operan una plataforma digital a la hora de verificar el consentimiento ajeno. La ley no es clara sobre el significado atribuible la expresión "de acuerdo a las circunstancias". En algunos casos, para verificar el consentimiento de una persona, podría bastar con que se completen ciertos formularios. Sin embargo, dado que requisitos así distan de ofrecer una garantía fiable —como nos consta, los formularios digitales y otros procedimientos identificadores suelen prestarse a un nivel de manipulación relativamente elevado—

, se planean interrogantes como los siguientes: ¿qué nivel de responsabilidad cabe atribuirle a un operador digital que ha fallado en comprobar la identidad de su cliente, justamente por haber empleado un procedimiento de bajo nivel de fiabilidad? ¿Acaso no corresponde que, en algunos casos o circunstancias, la responsabilidad sea asumida ni más ni menos que por el presunto dador del consentimiento, por no haber tomado los recaudos para evitar que su identidad fuera adulterada por un tercero? ¿En qué casos o circunstancias correspondería obrar de esta manera? ¿Inciden aquí consideraciones relativas al monto, valor o importancia que la transacción efectuada posee para las partes? Y, de ser así, ¿cómo ha de entenderse esta incidencia? ¿Puede ella moldear la naturaleza de las circunstancias contempladas por la legislación?

A fin de abordar estos interrogantes, en el presente trabajo propondré una interpretación ciertamente amplia del artículo en ciernes. Mi hipótesis es que el consentimiento del titular de datos personales cuya concurrencia la ley estima pertinente para desestimar un comportamiento ***ilícito*** por parte de un operador digital bien puede remitir a una forma meramente ***putativa*** de consentimiento, es decir: a una forma de consentimiento en la que la manifestación de la voluntad ***real*** o ***efectiva*** de una persona simplemente se encuentre ausente. Como sostiene P. Westen, cuando el Derecho le atribuye a un individuo un «consentimiento putativo» [*imputed consent*], y no en cambio un «consentimiento real» [*actual consent*], lo que hace es tratarlo *como si* ese individuo *hubiera consentido*, a pesar de que, en rigor, no alcancen a estar reunidas ninguna de las condiciones definitorias del consentimiento (*cf.* 2004, p. 337). Pues bien, apelando a esta distinción, aquí defenderé una interpretación extensiva de la expresión "de acuerdo a las circunstancias", según la cual la falta de consentimiento sólo comportará ilicitud cuando, por un lado, **(a)** los costos que deba asumir un operador digital en pos de su verificación no sean irrazonablemente elevados; y cuando, por el otro, **(b)** el titular de datos personales cuyo consentimiento ha sido presuntamente manipulado no se haya comportado de manera negligente.

El trabajo se compone de seis secciones. La sec. I procura realizar un repaso muy general por la actualidad del comercio electrónico, con el objetivo de sondear con qué niveles de protección cuentan hoy tanto usuarios como clientes. Dado que muchos sitios web parecen ignorar el consentimiento de los usuarios al tratamiento de sus datos personales, la sec. II pone el foco en un reciente fallo de la Corte Suprema de Justicia de la Nación (CSJN) que se hace eco de este problema, para analizar críticamente los fundamentos esgrimidos por uno de sus miembros, el Dr. C. Rosenkrantz. El objetivo de la sec. III consiste en determinar qué cabe esperar de

una correcta política en materia de protección de datos. Con ese fin, se analizan allí dos enfoques normativos extremos que lidian con esta pregunta, mostrando cuáles son sus alcances y limitaciones. La sec. IV plantea lo que aspira a ser un enfoque o estrategia superadora, fundada en una concepción ética amplia de nuestros derechos personales y, en particular, de la función que cumple el consentimiento. La sec. V, por su parte, sin dudas la más extensa e importante del trabajo, profundiza el contenido de la sección anterior, aunque esta vez intentando derivar de la estrategia allí postulada un criterio evaluativo que sea capaz de precisar *qué puede* y *qué no puede exigirse* de una compañía u operador digital en materia de protección de datos y, por supuesto, de verificación del consentimiento. Y la sec. VI, finalmente, repasa el recorrido efectuado en las secciones previas, buscando deslindar dos órdenes de cuestiones: el orden de lo valorativo y el orden de lo probatorio.

I. El comercio electrónico: ¿Un área de colisión de derechos?

El aumento del tráfico comercial mediado por plataformas electrónicas constituye una realidad innegable, tanto a nivel internacional como a nivel local. Los datos son elocuentes. El último informe confeccionado por la Cámara Argentina de Comercio Electrónico (CACE) da cuenta de una trayectoria en franco ascenso: mientras en el año 2017 la facturación del *e-commerce* había sido de $156.300 millones, el equivalente a un 52% de crecimiento con respecto al año anterior, en el año 2018 la facturación fue de $229.760 millones, lo que arrojó un 47% de crecimiento con respecto al 2017. Pero las cifras son aún más llamativas si tomamos como referencia el año 2019, en el que la facturación fue de $403.278 millones, representando un crecimiento del 76% anual. Además, del total de facturación de las empresas, las ventas realizadas desde *marketplaces* de terceros (plataformas como Mercadolibre, Alamaula, OLX o Linio, entre otras) representaron el 31% en el año 2019 y un 34% en el año 2018, contra el 17% alcanzado en el 2017.

Ante estas cifras, no cabe dudar del comportamiento de los consumidores. Las compras on-line brindan numerosas ventajas: ahorran tiempo, permiten comparar diferentes productos desde la comodidad del hogar y también ofrecen la posibilidad de consultar experiencias de otros consumidores. Como consecuencia de estas y otras características, los hábitos de consumo están experimentando una transformación radical. Hoy, por ejemplo, es cada vez más frecuente que un consumidor, antes de materializar una compra física en un local comercial cualquiera, analice las características del producto accediendo desde su dispositivo móvil a un

Marketplace.[1] Si allí verifica que el producto en cuestión resulta deficitario en algún sentido, o demasiado costoso, o inconveniente en términos comparativos, entonces lo más probable será que desista de la compra o se lo piense dos veces.

Por cierto, nada de esto significa que los hábitos confluyan por igual en todos los estamentos sociales y en todos los grupos etarios. Según algunos estudios cualitativos, tanto la frecuencia de las compras on-line como los tipos de productos adquiridos responden de manera diferencial a la edad del consumidor. CACE, sin ir más lejos, clasifica a los buscadores que tienen entre 45 y 59 años como "de ocasión", pues consultan precios y novedades cada dos o tres meses y se interesan fundamentalmente en productos del hogar, a diferencia de los buscadores "techie", que contempla a aquellas personas de entre 21 y 29 años que semanalmente acceden a Internet buscando información sobre educación, electrónica y elementos recreativos, como consolas o videojuegos. Además, también es cierto que la transformación de los hábitos de consumo encuentra un límite en aquellas regiones en las que el grado de conectividad a Internet es menor, como sucede en algunos países de África o incluso en algunas áreas de la República Argentina de menor densidad poblacional.

En paralelo a estos datos, lo que los estudios también revelan es el mayor nivel de confianza que exhiben los usuarios con respecto a la seguridad que brindan las plataformas virtuales para concretar con eficiencia un determinado negocio. Sitios y aplicaciones como Amazon o PayPal, por ejemplo, e incluso Google, que en rigor no representa un sitio sino un motor de búsqueda —el mayor motor existente en la actualidad— encabezan las más recientes listas de encuestas de confianza del consumidor.[2] No es ninguna novedad que todas estas compañías procesan una enorme cantidad información, mucha de ella relativa a datos personales de clientes y usuarios. Pero tampoco es ninguna novedad que el valor de mercado de estas compañías no se explicaría con prescindencia de las herramientas informáticas que les permiten procesar esta información y organizarla en tiempo y forma, para ofrecer una experiencia de búsqueda más eficiente.

Técnicamente, los motores de búsqueda funcionan mediante algoritmos, que son "conjuntos de operaciones preestablecidas" que permiten determinar "la relevancia

---

[1] Al respecto, véase el informe anual publicado por The Nielsen Company, accesible desde: https://www.nielsen.com/wp-content/uploads/sites/3/2019/04/december-2018-total-consumer-report.pdf (última fecha de acceso: 22/12/2020).

[2] Al respecto, véase: https://morningconsult.com/most-trusted-brands/ (última fecha de acceso: 22/12/2020).

de cada página en relación con una consulta concreta" (Pazos Castro, 2015: p. 25). Con ayuda de estos algoritmos, los motores ordenan los registros de búsquedas previas de los usuarios, almacenados en *cookies*, y los clasifican en orden de relevancia. De este modo, cada vez que un usuario realiza una nueva búsqueda desde su computadora personal, el motor predeterminará el resultado tomando como referencia su propio historial de búsquedas. Sitios como Amazon, Mercadolibre y otros similares han adquirido la reputación que hoy detentan por haber desarrollado sus propios algoritmos, lo que los ha potenciado para ofrecerle a cada consumidor una experiencia de compra más satisfactoria, al ahorrarle tiempo y también dinero. Desde luego, como señala Pazos Castro, no ha sido menor en este plano el rol jugado por "la publicidad comportamental o *behavioral advertising*", cuyas implicancias en el ámbito económico han sido enormes, pero cuyas implicancias en el ámbito jurídico todavía están por verse (*cf. ibíd*.: p. 8 y sigs.).

Entre los consumidores digitales, es probable que haya muy pocos que hoy no sean conscientes del modo como sus datos personales operan al servicio de estos gigantes de la economía mundial. Según vuelve a recordárnoslo Pazos Castro, "los datos personales son verdaderos activos (*assets*) para las entidades que prestan servicios en Internet" (ibíd.: p. 8). Sin embargo, nada de esto parece haber disuadido a los consumidores de seguir apostando al comercio electrónico, como lo confirman numerosos informes estadísticos (*cf. supra*). Por eso, aun cuando los índices de confianza del consumidor no sirvieran en modo alguno para medir el nivel de protección esperable para nuestros datos personales, todavía podrían ser útiles a fin de señalar el nivel relativamente bajo de preocupación que esta cuestión despierta, en especial si se lo compara con otros considerandos que hoy parecen ganar prevalencia en el imaginario de los internautas (al respecto, véase Thierer, 2013: p. 1072).[3]

¿A dónde nos conduce esto? Y, en particular, ¿qué nos invita a pensar acerca del rol reservado para el consentimiento? Si reparamos en el fenómeno de la publicidad comportamental antes aludido, el rol del consentimiento parece ser inexistente. En efecto, quien accede a un *Marketplace* como Amazon, Mercadolibre o Despegar, o aún quien accede a su propia casilla de mails y, por el sólo hecho de obrar así,

[3] Uno de los considerandos de mayor peso es el relativo al precio de los productos que se ofrecen en la web. Según señala el propio Thierer, hay estudios, como el de Acquisti y Grossklags (2008), que demuestran que los consumidores digitales están dispuestos a renunciar a ciertos resguardos en la medida en que lo que están por consumir sea gratuito. La analogía explicativa que emplea Thierer es digna de mención: "En un sentido, la paradoja de la privacidad existe en la misma medida en que existe la paradoja de la leche: las personas que desean leche se mostrarán dispuestas a adquirirla si se la ofrecen de manera gratuita. El hecho de que deseen menos leche si tienen que pagar por la misma no constituye, por ende, una paradoja" (2013: p. 1082). Sobre esto mismo, véase Berendt, Günther y Spiekerman, 2005.

presencia ante sus ojos molestos carteles de publicidad vinculados a su paso previo por la web, difícilmente haya manifestado conformidad alguna con nada de lo que allí se exhibe. Semejante maniobra publicitaria podría no generar otro perjuicio que una simple molestia visual (*cf. ibíd.*: pp. 1067-8). No obstante, constatar que un acto o preferencia personal se ha prestado a estas formas de manipulación puede llevarnos a sospechar con sobrados fundamentos de lo que podría seguirse de eso. Casos como el de Cambridge Analytica, entre otros ejemplos resonantes, alientan todo tipo de especulaciones: ¿somos realmente dueños de lo que hacemos cuando navegamos por Internet? ¿Hasta dónde llega nuestro grado de control? ¿Qué sucede con las imágenes que le vendemos a un sitio web, por ejemplo? ¿Accedemos a que la misma sea divulgada en otros sitios o buscadores, o a que sea manipulada mediante ciertos programas y aplicaciones de fotomontaje?

II. A propósito de un fallo de la CSJN

Muchas de estas preocupaciones, como la que plantea el último interrogante, ya cuentan con un pronunciamiento firme de la justicia. Un caso paradigmático en este sentido lo constituye el reciente fallo de la Corte Suprema de Justicia de la Nación Argentina en los autos caratulados "Gimbutas, Carolina V. c/Google Inc. s/daños y perjuicios" (*cf.* Fallos: 340:1236, del 12 de septiembre de 2017). Según cabe recordar, la demandante le había exigido a Google una indemnización por daños y perjuicios a raíz de que el buscador habría vinculado su nombre a sitios de contenido pornográfico y prostitución, así como por haber reproducido, difundido y utilizado comercialmente su imagen sin su consentimiento mediante el servicio de búsqueda por imágenes. En ese fallo, según sabemos, se confirmaría el pronunciamiento en contra de la demandante, formulado por la Sala M de la Cámara Nacional de Apelaciones en lo Civil. Pero aquí quisiera que nos detuviéramos en lo que sostuvo el actual Presidente de la Corte, Carlos Rosenkrantz, en la ampliación de sus fundamentos:

> (…) quien consiente mediante una manifestación de voluntad positiva que su imagen sea alojada en una página de internet, tal como lo ha hecho la recurrente (…) y *conoce* que internet funciona con buscadores, tal como ha admitido la recurrente en su demanda (…), consiente también que los buscadores faciliten al público usuario de internet el acceso a su imagen. En suma, de acuerdo a los artículos 31 de la ley 11.723 y 53 del Código Civil y Comercial de la Nación, y en virtud de que el modo de funcionamiento del buscador de la demandada no es *per se* ilegal, la recurrente no puede pretender que Google deje de facilitar a los usuarios de internet el acceso a sus imágenes. Al permitir que dichas imágenes sean allí alojadas, la recurrente ha consentido también que el acceso a sus imágenes sea facilitado por buscadores como el de autos (Fallos: 340:1236: fojas 8 y 9; la cursiva me pertenece).

Este solo pasaje, a mi juicio, ofrece un espacio sumamente sugestivo para la reflexión. Como el mismo Rosenkrantz se encarga de aclarar en un pasaje anterior, el consentimiento otorgado por la demandante no habría sido *tácito*, "pues no depende de una inferencia a partir de un acto distinto al de consentir" (*ibíd*.); tampoco habría sido *contrafáctico* o *hipotético*, al no tratarse de una mera conjetura (*cf. ibíd*.); ni menos habría sido *presumido por la ley*, "dado que no resulta de una directiva impuesta por disposición legal alguna" (*ibíd*.). Sin embargo, aunque Rosenkrantz no lo dice en estos términos, tal vez sí se haya tratado de un acto de consentimiento *implícito*. La explicación es muy sencilla: así como quien consiente 'exponerse a la lluvia', implícitamente consiente 'mojarse', en virtud de que 'la lluvia moja', *mutatis mutandis*, quien accede a que 'su imagen sea alojada en una página web', implícitamente consentiría que 'su imagen sea facilitada al público por ciertos buscadores', en virtud de que 'internet funciona con buscadores' (Rosenkrantz *dixit*).

Adviértase que este razonamiento reviste una importancia crucial a la hora de cubrir dos frentes. El primero de estos frentes constituye el motivo principal de este trabajo, atinente a los requisitos o estándares que deben satisfacerse para dar por verificado el consentimiento de un particular en una transacción digital. En este sentido, si alguien pretende demostrar que no dio su consentimiento, o que su consentimiento no ha sido implícito, como presuntamente debió demostrar la recurrente en el caso analizado; o, puesto a la inversa, si una compañía o cualquier otro operador digital ha de probar que no actuó sin el consentimiento de un usuario o cliente, pues este consentimiento se habría derivado implícitamente de un acto de consentimiento expreso, como presuntamente lo habría probado Google desde la óptica de Rosenkrantz, entonces bastará con explicar de qué modo un hecho se infiere —o no se infiere, según sea el caso— de otro hecho.

En la argumentación del propio Rosenkrantz, parece introducirse un requisito probatorio adicional, de carácter *subjetivo*. En efecto, Rosenkrantz alude a la necesidad de dar por probado el conocimiento de la recurrente acerca de cómo funciona internet, algo para lo que allí habría habido evidencias (*cf. supra*). Sin embargo, no es seguro que este requisito deba estar siempre presente: en algunas circunstancias, porque más que el hecho de si alguien *sabía* ciertas cosas, importa el hecho de si *debía* saberlas; y, en otras, porque el carácter notorio que acompaña a ciertas inferencias empíricas, como en 'si llueve, las calles se mojan', parece tornar innecesaria cualquier obligación probatoria (*cf.* Gascón Abellán, 2010: p. 180 y sigs.). En todo caso, y en relación al litigio en particular que analiza Rosenkrantz, lo

relevante pasa por determinar qué tipo de carácter reviste la inferencia que lo lleva a concluir que el hecho de que una imagen será facilitada al público por ciertos buscadores se deriva del hecho de que la misma imagen haya sido alojada en una página web. ¿Se trata de una inferencia subjetiva, objetiva o notoria? O, para ser más exactos, ¿se trata realmente de una inferencia *deductiva*? Si sólo reparamos en el hecho de que es perfectamente posible que una imagen sea alojada en una página web sin que ningún buscador tenga acceso a la misma, entonces el razonamiento probatorio que emplea Rosenkrantz aparecerá por lo pronto como insuficiente para respaldar su decisión.

En cuanto al segundo de los frentes mencionados, el mismo remite a una cuestión más general y urticante, que no sólo subyace a la preocupación recién analizada, sino también a otras preocupaciones similares, como las aludidas al final de la sección anterior. Para decirlo de una vez, se trata de la cuestión ético-política relativa a qué nivel de protección ha de brindarse a uno de los aspectos definitorios de nuestra privacidad, como sin dudas lo son nuestros datos personales. Aunque Rosenkrantz no lo dice explícitamente, de sus considerandos parece inferirse con toda naturalidad una auténtica definición en esta materia. Según él, el nivel de protección que sería suficiente vendría representado por el nivel que Google efectivamente alcanzó a brindar, dado el modo como los datos *de hecho* circulan en internet. Si no hay una manera alternativa de hacerlos circular y de esta verdad depende la salud de la circulación —y, en última instancia, la existencia misma de internet—, entonces tal vez no haya demasiado que pueda reprochársele a Rosenkrantz. Pero el desafío justamente pasa por señalar qué elementos probatorios existen para demostrar que efectivamente las cosas funcionan de esta manera. Es en este plano donde el razonamiento de Rosenkrantz resultaría por lo menos apresurado. Google, además, por ser el principal motor de búsqueda existente en la actualidad, parece jugar un papel bastante más activo que aquel que le atribuye Rosenkrantz a la hora de crear y mantener el tráfico y la circulación de datos que objeta la demandante.

III. Dos estrategias tentativas de solución

A fin de abordar el segundo frente abierto en la sección anterior, creo que bien valdría la pena diferenciar entre dos posturas extremas: una, a la que podríamos catalogar de «ingenua o concesiva»; y otra, a la que bien podríamos denominar «alarmista o combativa». Estas posturas, según conviene aclarar, se comportan más como 'tipos ideales' en el sentido weberiano que como reconstrucciones descriptivas de posturas realmente existentes. De todas formas, según creo, ellas capturan mucho de lo que

se ha dicho en la literatura disponible, por lo que serían capaces de brindar un interesante contraste desde el que comenzar a construir una estrategia superadora en torno a lo que cabría esperar de una correcta política en materia de protección de datos personales. Veamos de qué se trata cada postura y cuáles son los problemas que su adopción genera en la práctica.

Para comprender qué tipo de postura adopta alguien en relación al comercio electrónico, así como en relación a otros tipos de transacciones digitales, la clave pasa por determinar si está dispuesto a admitir sin más el *statu quo* imperante, al que podríamos definir en función de dos elementos característicos: objetivos y subjetivos. Los *elementos objetivos* son aquellos que explican el funcionamiento de internet y el modo como operan los usuarios que allí interactúan, valiéndose de la tecnología que encuentren disponible. En cambio, los *elementos subjetivos* hacen referencia a las expectativas, deseos o preferencias de los internautas, es decir: a la forma como las mismas son satisfechas en las experiencias transaccionales de los agentes. Para acotar el problema, aquí consideraré qué implica adoptar una postura de uno u otro tipo en relación al *statu quo* imperante en el comercio electrónico, dejando de lado otras clases de transacciones digitales.

Pues bien, en este ámbito más reducido de análisis, la cuestión puede desglosarse a partir de dos puntos de vista, dependiendo de los *elementos* involucrados. Desde el punto de vista *objetivo*, entonces, cabría decir que alguien adopta una postura *concesiva* o *ingenua* cuando asume que el nivel de protección normativamente exigible para nuestros datos personales no sólo depende de la tecnología existente, sino también de la que se encuentre efectivamente disponible tanto para prestadores y usuarios, como para vendedores y compradores. Por su parte, desde el punto de vista *subjetivo*, diremos que alguien adopta una actitud o postura concesiva cuando asume que ese nivel de protección depende sin más del nivel de satisfacción experimentado por los usuarios o clientes. Por ende, de acuerdo a esta perspectiva, si la realidad se encargase de mostrar que ellos no están preocupados por el modo como sus datos personales son procesados en las plataformas digitales, o que esa preocupación ocupa un lugar menor en relación a otros considerandos, entonces ese dato debería ser clave para confeccionar el estándar evaluativo final. Entre muchos otros, trabajos como los de Posner (2008), Castro y McQuinn (2014), Allen y Berg (2014), Thierer (2013; 2014) o Layton (2018), orientados a prevenir sobre los riesgos de una regulación excesiva en materia de protección de datos, ofrecerían, cada uno a su modo, una demostración bastante aproximada de esta postura concesiva, a la que también se ha catalogado como *conservadora* o *laissez faire*.

Por contrapartida, alguien adopta una postura *alarmista o combativa* en relación al comercio electrónico cuando no se dispone a admitir sin más el *statu quo* imperante, al que volveremos a definir en referencia a las dos clases de elementos mencionados. Según la postura alarmista, el derecho a la privacidad y, junto con él, el nivel de resguardo que debe garantizarse para nuestros datos personales, es innegociable, con total independencia de los elementos objetivos y subjetivos que explican el funcionamiento de internet o el grado de conformidad comprobable entre usuarios y clientes. Por esto mismo, el nivel mínimo de protección exigible a favor de quienes exponen sus datos en internet bien podría establecerse a partir de un determinado umbral fijado *a priori*, incluso admitiendo que ello, a la postre, pudiera poner en peligro la salud del tráfico negocial. Entre muchos otros, trabajos como los de Sachs (2009), Vaidhyanathan (2011), Barocas y Nissenbaum (2014), Susser (2019) o Bietti (2019) constituirían diferentes manifestaciones de este punto de vista, el cual también se refleja en buena parte del Reglamento General de Protección de Datos (RGPD) dictado por el Parlamento Europeo.[4]

Analizadas *grosso modo*, ninguna de estas posturas ofrece a mi entender una comprensión acabada de la problemática en ciernes. La postura concesiva ciertamente no lo hace por varias razones, que podríamos resumir en tres esenciales. La *primera* es que no parece reparar suficientemente en lo que implica la *disponibilidad* de un recurso o herramienta digital. La dificultad, por cierto, excede ampliamente a esta postura, al estar relacionada con el problema filosófico que plantean los términos disposicionales. De cualquier modo, dejando este asunto de lado, aquí la dificultad es más práctica que teórica, pues perfectamente puede suceder que una herramienta técnica esté disponible para un comerciante, aunque ella sea muy costosa desde el punto de vista económico. Pero incluso si se introdujera una salvedad que permitiera sortear esta objeción, la *segunda razón* que desacreditaría a esta postura tiene que ver con el modo en que ella parece validar de por sí las preferencias o preocupaciones de los consumidores, con todo lo manipulables que tanto unas como otras pueden volverse cuando son libradas a los fríos designios del mercado.[5] Por último, la *tercera razón* invalidante es que ella

[4] Hermstrüwer llama a esta postura "el enfoque tradicional sobre la protección de datos" [*traditional data protection approach*], al que contrapone al "enfoque orientado al mercado" [*market-oriented approach*] (*cf.* 2017: p. 10), de características similares a la postura anteriormente descripta.

[5] Las evidencias al respecto son abundantes. En tal sentido, véase el clásico estudio de Hanson y Kysar (1999), destacado en Calo 2014: 995 y sigs. Willis (2014), por su parte, advierte acerca de los efectos formativos que sobre las preferencias ejercen las configuraciones por *default* [*default settings*] que emplean muchos sitios web, aplicaciones y otros tipos de programas. Según Willis, esto ocurre por vía de dos mecanismos diferentes: por un lado, de lo que él llama un "efecto de aprobación" [*endorsement effect*]; y, por el otro, de lo que denomina un "efecto de la experiencia" [*experience effect*]. El primer efecto se produce cada vez que un usuario, pudiendo modificar una configuración por *default*, simplemente

tampoco repararía en los problemas que presenta cualquier concepción agregativa de la sociedad, que es la concepción que vendría implicada en la idea de tomar en cuenta lo que los usuarios y clientes prefieren *en general*, y no lo que cada uno de ellos prefiere o desea en concreto. Para retomar el caso analizado en la sección anterior, imaginemos que el nivel de preocupación general en torno al modo como nuestras imágenes aparecen en internet, vinculadas a sitios de dudosa reputación moral, fuera prácticamente inexistente. Aunque todo el mundo pensara o sintiera de esta manera, ello no tendría por qué impedirle a Gimbutas manifestar un disentimiento explícito sobre el modo como sus datos personales son tratados por Google, aunque luego su demanda no prospere en sede judicial.

En comparación con la postura concesiva, la postura alarmista parece sin dudas mejor acondicionada para brindar un marco protectorio más sólido al derecho a la privacidad. El problema, no obstante, es el extremo opuesto en el que incurre, al desestimar de plano la importancia que los deseos y preferencias *reales* poseen no sólo para explicar nuestros hábitos de consumo, sino también otras decisiones de mayor envergadura moral.[6] Por ejemplo, quien firma un contrato de adhesión tan sólo haciendo "click" en el botón "ok" que figura en una página web, renuncia mediante este acto a muchos derechos de los que antes era titular. El acto encierra una simpleza que bien podría contrastar con la hondura del derecho involucrado, como el de demandar ante ciertas instancias (i.e. un organismo administrativo o un tribunal civil) por los incumplimientos contractuales de los que pudiera ser víctima, pongamos por caso. Pero asumamos que el individuo actúa de esta manera. ¿No constituiría una simplificación sumamente burda presuponer que su conducta tan sólo responde a las tretas manipuladoras del mercado? Por lo pronto, ¿qué hay de sus preferencias *meditadas*, esto es: de aquellas con las cuales haya podido llegar a identificarse a lo largo del tiempo? Cuando ciertos derechos se oponen a su realización, ¿acaso estas preferencias deberían dejar de contar?

Pero hay más. Por varias razones, tradicionalmente se ha dicho que el consentimiento representa la noción ético-política más importante de la Modernidad (*cf.* O'Neill, 2002: p. 224). Sin esta noción, la mayor parte de las instituciones jurídicas que hoy nos rodean ni siquiera existirían, por lo menos no tal como las

---

la acepta, por interpretarla como un "consejo implícito formulado por una parte con mayor conocimiento acerca de lo que la mayoría de las personas preferirían o deberían preferir". Por su parte, el segundo efecto se da cuando el usuario desarrolla una preferencia a favor de la configuración existente por haberse habituado a la misma luego de un tiempo de experimentar con ella (*cf. ibíd.*: pp. 77-78).

[6] Sobre la diferencia entre nuestras preferencias reales e imaginarias (o confesas), véase Berendt, Günther y Spiekerman, 2005 y Norberg, Horne y Horne, 2007. Además, véase Willis, 2014: p. 80, en donde se sugiere que incluso los consumidores que se describen a sí mismos como otorgándole una gran importancia a su privacidad actúan de una manera tal que revela precisamente lo contrario.

conocemos. Como a menudo se sostiene, el consentimiento cumple una función moral *transformadora*, tornando permisibles ciertos actos que, en su ausencia, no lo serían (*cf.* Hurd, 1996; Alexander, 1996). Sin embargo, trabajos como el de Bietti (2019; *cf. supra*) son radicales en su propuesta: puesto que el entorno en el que se desenvuelve la economía digital no garantiza las condiciones marco [*background conditions*] en las que debería ejercerse el consentimiento, el mismo no está capacitado para cumplir en dicho ámbito función moral alguna (*cf. ibíd*.: p. 379 y sigs.). Entre las condiciones marco que menciona la autora, revisten particular importancia las referidas a los desequilibrios de poder [*power imbalances*] que se constatan entre los agentes transaccionales, los que suelen inclinar la balanza en contra de los usuarios y/o clientes (*cf. ibíd*.: p. 315). Por ende, en la medida en que estos desequilibrios no sean corregidos, cualquier esfuerzo que se haga en pos de dotar al consentimiento individual de mayor visibilidad estará condenado a fracasar. Su solución es drástica: asumir una postura paternalista en detrimento del mercado electrónico, tal cual hoy lo conocemos, y en defensa de la dignidad de las personas más débiles del tejido social (*cf. ibíd*.: p. 379).

La preocupación que manifiestan tanto Bietti como otros autores (*cf. supra*) constituye una preocupación genuina y a la que debe darse respuesta. En donde haya desequilibrios manifiestos, oportunamente habrán de introducirse correcciones rectificadoras. No obstante, pretender que el consentimiento de ninguna manera pueda seguir siendo significativo en contextos semejantes supone, a mi modo de ver, una grave distorsión. Si así fuera, entonces nunca podríamos dar por válido ningún acuerdo comercial, sin importar la plataforma en la que se celebre, dado que en general los consumidores suelen posicionarse en una posición de franca desigualdad con respecto a los agentes o instituciones que dirigen el rumbo de la economía. Pero lo más importante que tiende a ocultar una postura así de alarmista es que el consentimiento también representa una herramienta perfectamente apta para comenzar a combatir o, al menos, hacer más tolerables o llevaderas, las condiciones de injusticia socialmente imperantes.

Para ilustrar lo que quiero decir, pensemos en los contratos explotativos, a los que nadie dudaría en considerar injustos. Ellos no sólo constituyen la resultante de una situación de desequilibrio significativo entre las partes, sino que validan un acto a partir del cual la parte dotada de mayor poder negocial se aprovechará de las desventajas de la contraparte para utilizarlas en beneficio propio. Aun así, el hecho de que estos contratos nos parezcan injustos, o incluso inmorales, no constituye *de por sí* una razón suficiente para declararlos *ilícitos*. La aclaración es importante por

la siguiente razón: si la parte fuerte que se beneficia de un acuerdo ha jugado un rol causal en la generación de las desventajas que impulsaron a la parte débil a dar su consentimiento, pues entonces difícilmente este consentimiento podría considerarse moralmente transformador. Pero, en nuestras sociedades reales, signadas por la desigualdad, este dista de ser siempre el caso. Lo que allí sí puede ocurrir, en cambio, es que el contrato explotativo a menudo aparezca como el único remedio que encontró a su disposición el agente desaventajado para tornar menos desventajosa su situación de partida. R. Dworkin solía poner como ejemplo en tal sentido el ejercicio de la pornografía, práctica que nunca osó defender. De todos modos, alentar su prohibición en un contexto general de injusticia distributiva, nos decía, podría generar un efecto aún más grave que el mal que mediante dicha prohibición pretendería evitarse, al obligar a muchas personas vulnerables a subsistir apelando a prácticas aún menos redituables, o no menos reprensibles o humillantes, que el propio ejercicio de esa actividad (*cf.* Dworkin, 2019: p. 282).[7]

De manera similar, en este contexto podríamos argüir que los agentes económicos que contratan con grandes empresas utilizando como medio las plataformas digitales disponibles, y acceden así a que sus datos sean procesados sin que se tomen ciertos recaudos, otorgan una forma de consentimiento que, no por nacer de un contexto general de desigualdad, resulta menos valiosa. Además, Bietti debería ser mucho más específica a la hora de explicar en qué sentido las transacciones digitales entre agentes dotados de diferentes capacidades o recursos necesariamente afectan la dignidad de los agentes menos favorecidos. Una vez más, veamos el caso analizado por la CSJN. A diferencia de lo que piensa Rosenkrantz, es probable que Gimbutas no haya dado su consentimiento a que sus datos personales fueran tratados como finalmente lo fueron. Sin embargo, ¿qué decir de otros casos, como el de muchas estrellas de la industria pornográfica, cuyas imágenes y videos circulan ampliamente por internet? Incluso cuando ellas no sean siquiera conscientes de los sitios y portales que reproducen sus contenidos, algunas no sólo no se oponen a que eso suceda, sino que lo toman con beneplácito, debido al rédito (no *directamente* económico) que obtienen de este modo.[8] Desde luego, si nos remontamos a casos como el de

[7] Escribe Dworkin en concreto, analizando el libro *Only Words*, de C. MacKinnon: "Sería garrafal suponer que las mujeres (o los hombres) que aparecen en películas pornográficas lo hacen involuntariamente. Es verdad que nuestro sistema económico dificulta para muchas de ellas el hallazgo de empleos que resulten satisfactorios o gratificantes, lo que bien puede impulsarlas a aceptar roles en películas pornográficas que de otra manera rechazarían. El sistema, según nota MacKinnon con tristeza, trabaja para el beneficio de los productores pornográficos. Pero también trabaja para el beneficio de muchos otros empleadores —cadenas de comida rápida, por ejemplo— que, de esta manera, obtienen la ventaja de emplear a mujeres por salarios más bajos. Existe una gran injusticia económica en los Estados Unidos, pero esa no es razón para privar a las mujeres pobres de una oportunidad económica que algunas de ellas podrían preferir por encima de las alternativas disponibles" (*ibíd*.).

[8] En palabras de Valentina Nappi, una estrella de la industria porno: "Internet puede haber hundido los márgenes de ganancia de la industria tradicional, pero permite que los actores se den a conocer y hagan

Facebook/Cambridge Analytica, la afectación a la dignidad de los usuarios parece segura, ya que allí se traicionó su confianza. Pero lo que de ninguna manera puede afirmarse es que esto encuentre explicación en el desequilibrio de poder reinante entre los agentes.

IV. ¿Una estrategia auténticamente superadora?

Así como hay mecanismos o herramientas sin los cuales no sería posible que el gas circulara en una red troncal de manera *eficiente*, o que los vehículos a motor hicieran lo propio en las rutas de un territorio, del mismo modo existen mecanismos que son consustanciales al funcionamiento *eficiente* de internet. La eficiencia, por cierto, es un estándar evaluativo, el cual puede ir acompañado de cierta dosis de subjetivismo o arbitrariedad. Sin embargo, no es difícil hallar un marco de condiciones mínimas con el que ponernos de acuerdo. Por ejemplo, a los efectos de garantizar una circulación vehicular que al mismo tiempo sea veloz y prevenga los accidentes, ¿quién se atrevería a poner en duda la mayor eficiencia que detentan las autopistas en comparación con las rutas de doble carril? Por el contrario, si el fin en cuestión se redujera a garantizar un determinado nivel circulación con la menor inversión económica posible, la construcción de una ruta de doble carril quizá aparezca como la alternativa más recomendable. Con internet sucede algo muy parecido, por más que el capital circulante sea la información. Herramientas como las *cookies*, entre otras, se encargan precisamente de aumentar la velocidad de búsqueda de cada usuario, incrementando asimismo el grado de relevancia de los contenidos que se ordenan en nuestras pantallas. Pero las *cookies*, como bien sabemos, comportan una amenaza cierta a la privacidad de las personas, lo que puede llevarnos a evaluar la eficiencia de internet según otros parámetros valorativos. El desafío, en todo caso, queda planteado: ¿qué herramientas tecnológicas resultan indispensables para asegurar una navegación por la web que sea mínimamente satisfactoria?

Para despejar cualquier especulación desde el inicio, aquí deseo aseverar que este tipo de preguntas carecen de respuesta. Las herramientas indispensables no necesariamente se resumen en las herramientas disponibles, y, entre estas últimas, las hay de distintos tipos: factibles y no factibles, o más y menos costosas, tan sólo para enumerar algunos. En materia de circulación vehicular, esto se puede ilustrar mediante un ejemplo sencillo. No hace falta inspirarse en el clásico film futurista de ciencia ficción para saber que hoy es posible la fabricación de pequeñas naves

---

dinero creando sus propios contenidos" (al respecto, véase: https://www.vice.com/en_uk/article/d3amak/how-much-money-porn-stars-make).

programables para volar a cierta altura del suelo, minimizando cualquier riesgo de colisión. Sin embargo, aunque estas naves representaran la única solución tecnológica capaz de garantizar con cierta eficacia una circulación vehicular que fuera todo lo rápida y segura que esperamos, ello no implicaría que inmediatamente debiéramos abandonar los modos de circulación imperantes en la actualidad. Si así fuera, la parálisis social sería absoluta. Salvando las distancias, la misma analogía vale para el mundo de los internautas. Hoy por hoy, los principales motores de búsqueda existentes operan mediante herramientas tecnológicas que permiten rastrear la conducta de los usuarios. Muchos de estos motores fueron diseñados en su momento por personas que no eran ni remotamente conscientes de las amenazas a la privacidad que ellas podrían generar. Y, si bien es verdad que los resguardos tecnológicos introducidos en los últimos años vienen siendo notables, las huellas digitales que se van generando tras nuestro paso por la web son inevitables. Así como no es posible nadar y guardar la ropa, según suele decirse, tampoco es posible navegar por internet sin dejar ningún tipo de rastro.

Por todo esto, simplemente resultaría irrisorio plantear el desafío en aquellos términos. Cuando nos enfrentamos al dilema de qué hacer para garantizar una experiencia satisfactoria en la web que al mismo tiempo brinde un determinado nivel de resguardo a la privacidad (o al patrimonio) de los usuarios, la solución sólo podrá provenir de un enfoque que sea realista y, a la vez, multidimensional. Por lo primero, entiendo un enfoque que, sin dejar de visualizar las posibilidades tecnológicas presentes o futuras, reconozca las limitaciones tecnológicas actualmente imperantes y actúe con cierta deferencia hacia quienes operan en este contexto para llevar a término un determinado negocio. Pero también lo entiendo como un enfoque preocupado por no desalentar la innovación humana, aunque la misma pudiera entrar en tensión con el estatuto jurídico del que gozan ciertas prácticas o valores. En este sentido, la invención de aplicaciones como Uber, que sin dudas han venido a desafiar al servicio tradicional de taxis, o la creación de herramientas financieras como las billeteras virtuales, que hoy brindan un área de cobertura a la que los bancos no tienen acceso, ofrecen indicios ciertos de lo que quiero decir.

Ahora bien, a fin de precisar hasta dónde puede llegar la innovación, lo que se requiere es una mirada ética amplia, es decir: una mirada que sea capaz de sopesar en su justo término cuáles son los valores que promovería la innovación tecnológica y cuáles son aquellos otros que protegería la regulación jurídica. A esto es a lo que llamo un enfoque multidimensional. En ocasiones, no habrá necesidad de efectuar balance alguno, como cuando la innovación tecnológica apunta precisamente a

brindar respuesta a un reclamo jurídico. Tal es lo que sucede, por ejemplo, con *Privacy Sandbox*, un proyecto anunciado por Google mediante el cual se busca eliminar el soporte para *cookies* de seguimiento de terceros en Chrome. No obstante, habrá otras ocasiones en las que esta confluencia valorativa se mostrará problemática. Google mismo, tal como hoy funciona, no permite que los usuarios bloqueen las *cookies* de terceros. Sin embargo, para compensar este defecto, existe una política de privacidad que el propio buscador publica en la parte inferior de su página, en la que se dan a conocer todos los riesgos que se siguen de operar con sus servicios. Quien accede a Google, pues, no puede desconocer esta política, con lo que parecería estar otorgando una forma de consentimiento a cargar con ciertos costos.

En un universo de constantes innovaciones tecnológicas puestas al servicio de un acceso a la información más amplio, sencillo y fluido, casos como el recién aludido tienden a ser la regla más que la excepción. Tanto la Convención Interamericana como la Corte Europea de Derechos Humanos sostienen que el derecho de acceso a la información constituye uno de los pilares que contribuyen a la maximización de nuestra autonomía personal (*cf.* Abramovich y Courtis, 2000). Pero también es cierto que el ejercicio de este derecho encuentra límites evidentes, como cuando la información solicitada infringe el derecho a la privacidad de otra persona, que también constituye otro de los pilares fundamentales de la autonomía personal. ¿Qué sucede, de todas formas, cuando no es la privacidad ajena la que está en juego, sino la propia? ¿Qué sucede cuando, a fin de acceder a cierta información, la cual probablemente contribuya a ampliar mi autonomía, debo sacrificar un aspecto de mi esfera privada? ¿Acaso no es evidente que todos deberíamos contar con la potestad de tomar este tipo de decisiones?

Algunos planteos, como muchos de los agrupados bajo la postura *alarmista* antes analizada (*cf. supra*), parecen entender el derecho a la privacidad y, junto con él, el valor de la autonomía, desde un punto de vista estático y monolítico. Según ellos, la privacidad se trataría de un objetivo social a ser promovido desde el Estado, que es la agencia que debería bregar para que cualquier otra agencia o institución, tanto pública como privada, cumpla con una serie de requisitos definidos de antemano por medio de ciertas regulaciones. De este modo, si se trata de una agencia como Google, por ejemplo, su política de privacidad no puede ser distinta de las políticas de privacidad de otras agencias o empresas que ofrecen sus servicios en la web. Por eso mismo, si un Estado, por medio de su aparato regulatorio, estimara insuficiente la política de cookies implementada por la empresa, aunque un usuario decidiera

aceptar los términos y condiciones que dan cuenta de esta política, cargando con los costos de contar con un menor nivel de protección para sus datos personales, ello no bastaría para eximir a Google de ciertas responsabilidades. De acuerdo a tales planteos, la máxima "*volenti non fit iniuria*" resultaría infundada en este contexto.

A mi juicio, el error en el que incurren algunas versiones de la postura alarmista se debe a que toman en cuenta el valor de la autonomía personal sólo en su faz estática, la cual contempla aquellos derechos de los que nadie podría ser privado so pena de experimentar un detrimento *significativo* en su capacidad de actuar como agente moral. Pero el derecho a la privacidad, como muchos otros derechos que tienen como correlato una prohibición —a saber: la prohibición de tratarnos de cierta manera que recae sobre terceros—, sólo puede interpretarse como una restricción a actuar de tal o cual forma *sin nuestro consentimiento*. Y es perfectamente lógico que así sea. De lo contrario, aunque todos fuéramos autónomos, cada uno lo sería en la misma medida y en el mismo sentido que el resto de las personas que nos rodean. ¿Pero para qué querríamos contar con autonomía, sino para perseguir de la manera más efectiva posible nuestra propia concepción particular del bien? ¿Para qué querríamos ser autónomos sino para llevar a la práctica los proyectos de vida que, según entendemos, podrían redundar en nuestra propia realización personal?

En contraposición a este enfoque estático, un enfoque dinámico concibe el derecho a la privacidad como una de las tantas condiciones que podrían requerirse a la hora de ejercer la autonomía y, de este modo, perseguir la realización personal o simplemente satisfacer una preferencia. Según este enfoque, la privacidad es un valor importante, consagrado en un derecho, pero el mismo podría ser mucho menos importante que otros valores alternativos. En determinadas circunstancias, justamente el acceso a la información (o un mayor acceso a la información) podría representar uno de estos valores en pugna. En la medida en que la prosecución de este valor demandara que abandonemos cierto resguardo a nuestra privacidad, ¿por qué no habríamos de hacerlo? La autonomía personal, en cualquier caso, puede ejercerse de múltiples formas, dependiendo de cuáles sean las razones personales que nos muevan a actuar.

El consentimiento, según sabemos, constituye la herramienta comunicativa fundamental para renunciar a ciertas pretensiones o derechos y validar así un acuerdo o transacción. C. S. Nino supo poner esta herramienta en correlación con el "principio de dignidad de la persona humana", subyacente a la *dinámica* de nuestros derechos, es decir: a la posibilidad que todos tenemos de "operar" con los mismos,

renunciando a algunas ventajas a las que estábamos jurídicamente facultados a cambio de otras ventajas en persecución de nuestros "distintos fines" (Nino, 2007: p. 293). El consentimiento, según él, es el que permite esta operatividad. El problema surge cuando llega el momento de precisar qué formalidades han de rodear a semejante acto comunicativo. Con esto no me refiero aquí a los vicios que afectan la voluntariedad del acto o la equivalencia de poder negocial entre las partes, dos cuestiones usualmente aludidas por los contractualistas. En este lugar, asumo que no hay nada como lo primero y que lo segundo, en un punto, es inevitable (*cf. supra*). Más bien me refiero a las solemnidades que deben satisfacerse para dar por acreditada la identidad de quien consiente. Porque, como dice Mik, aunque "los problemas de identificación surgen en todas las transacciones que se realizan por primera vez entre extraños, las transacciones digitales [*e-commerce transactions*] parecen exacerbar estos problemas" (2012: p. 397). En su opinión, además —que comparto—, un análisis de lo que aquí está en juego podría resultar sumamente iluminador para analizar el problema más general de cómo calificar jurídicamente a un acuerdo en el que una de las partes no es quien aduce ser.

V. Identidad, consentimiento y culpabilidad

En el año 2018, Elena Paoloni, una ciudadana de la localidad bonaerense de Lanús, denunció la extracción de 6.000 pesos de su cuenta bancaria mediante la utilización de Todo Pago, una billetera virtual.[9] La maniobra se habría orquestado por medio de los siguientes pasos. Por empezar, una persona (¿el empleado de un bar?) habría obtenido una foto de la tarjeta de débito de Paoloni. Con los datos de esta tarjeta y la creación de una cuenta falsa de e-mail a su nombre, esta persona descargó la aplicación de Todo Pago a su dispositivo digital y se adhirió a la misma actuando en representación de la afectada. Siempre que esto sucede, lo que automáticamente hace la billetera es vincularse a la cuenta bancaria que respalda la tarjeta, permitiendo operar con ella. Ahora bien, Todo Pago, al igual que otras billeteras virtuales, brindan la posibilidad de transferir pequeñas sumas de dinero a otras personas sin que sea necesario revelar la identidad de las mismas. Para ello, la aplicación habilita la creación de PINs, mediante los cuales cualquier persona, disponga o no de cuenta bancaria, queda inmediatamente habilitada para extraer dinero de un cajero electrónico. La persona que estafó a Paoloni, pues, habría realizado un total de doce extracciones de 500 pesos mediante la creación sucesiva

[9] Al respecto, véase: https://www.lanacion.com.ar/economia/se-viralizo-en-twitter-una-estafa-con-una-billetera-virtual-nid2101206/ (última fecha de acceso: 22/12/2020). Además, https://www.unosantafe.com.ar/santa-fe/billetera-virtual-recomendaciones-un-caso-estafa-que-tomo-estado-publico-n2120238.html (última fecha de acceso: 22/12/2020).

de PINs. ¿Qué responsabilidad le cabe a Todo Pago por no haber apelado a un procedimiento identificador que le asegurara que la responsable de manipular su aplicación no era la propia Paoloni? ¿Cabe considerar ilícito a su comportamiento y, por ende, susceptible de una sanción?

En este caso, lo que se comprueba es que los recaudos tendientes a verificar el consentimiento ajeno no fueron suficientes. Pero lo que también se comprueba allí es que la compañía interviniente habría actuado sin dolo, es decir: sin intención aparente de defraudar a nadie. La reglamentación del art. 31 de la Ley 25.326 establece que las sanciones administrativas a ser aplicadas a los responsables de procesar un dato personal sin el consentimiento de su titular habrán de graduarse en función de varios factores, entre los que justamente se destaca el grado de intencionalidad de la conducta. Si no hay intención, entonces tal vez nos encontremos en estos casos con una atenuante. Pero la reglamentación también cita entre los factores aludidos cualquier otra circunstancia que sea relevante "para determinar el grado de antijuricidad y de culpabilidad presentes en la concreta actuación infractora". En consecuencia, todavía resta analizar si aquella insuficiencia verificadora que se detecta en esta clase de comportamiento empresarial constituye una omisión *culpable*. Al abordaje de esta cuestión están destinadas las siguientes reflexiones.

V.I. Del consentimiento presunto a la auto-puesta en peligro de la víctima: dos casos claros de responsabilidad del usuario

El caso de Paoloni, como decenas de casos similares que podrían citarse, reúne aproximadamente los elementos distintivos que capturara el ejemplo inicial con el que abriera este trabajo: una compañía (C) realiza una transacción con alguien (Q) que simula ser cierta persona (en este caso, P), para lo cual se apropia de los datos personales de esta última, como los números de su tarjeta de crédito. C aduce haber actuado con el consentimiento de P, pero la realidad es que P no ha otorgado nada semejante. Tal como está construido, el ejemplo imaginario no sugiere ninguna hipótesis acerca de la identidad de Q. Pero ahora intentemos compensar este silencio. Supongamos que Q se trata de un menor de edad a cargo de P. ¿Qué relevancia tendría este dato para responsabilizar a C por la pérdida de P si P decidiera radicar una denuncia ante la Agencia de Acceso a la Información Pública (AAIP)? O imaginemos que P fuera víctima de lo que actualmente se conoce como "*phishing*". Haciéndose pasar por una compañía X, E, el estafador, le envía un correo a P

solicitándole sus datos personales, algo a lo que este accede. ¿No sería ciertamente irrisorio que la AAIP le exija a C que se responsabilice por la pérdida de P?

Ejemplos de este tipo, por cierto, abundan. De lo que se trata, en cualquier caso, es de delimitar las áreas de competencia entre los agentes intervinientes en cada situación. La razón es obvia: sin una delimitación semejante, no habrá asignación de culpabilidad posible. En este sentido, parece haber al menos dos factores que jugarían aquí un rol determinante. El primero de ellos remite a algo que capturan los ejemplos precedentes y que bien podríamos resumir en la siguiente pregunta: ¿qué obligaciones o deberes de cuidado recaen sobre los usuarios y/o clientes? A lo que la respuesta no se hace esperar: ninguna obligación o deber que no sea razonable cumplir, ya sea por no haber surgido de una decisión voluntaria, ya sea por los elevados costos que acarrearía dicho cumplimiento. Por su parte, el segundo de ellos remite sin lugar a dudas a la razonabilidad de los costos que debería afrontar una compañía o agente comercial a la hora de implementar mecanismos más o menos confiables para la identificación de sus usuarios o clientes. En ambos casos, la delimitación de competencias parece requerir como condición un análisis de costo-beneficio, algo a lo que ya llegaremos en unos instantes. Por ahora, sin embargo, propongo que nos detengamos en lo que podría deducirse del contenido explícito de nuestra legislación de fondo.

Con respecto al primer factor, el ejemplo del menor de edad hablaría por sí mismo. Recordemos en este sentido que el artículo 684 del Código Civil y Comercial ya prevé una respuesta para este tipo de casos, al menos en lo atinente a los contratos de escasa cuantía que celebran los menores. Como sabemos, lo que el Código estipula es que estos contratos "se presumen realizados con la conformidad de los progenitores", una solución que, según asumen los doctrinarios, descansaría en una doble *ratio*: por una parte, en la necesidad de operar mediante un criterio *práctico o realista* que no derive en "un inconveniente obstáculo para el tráfico negocial" (Lorenzetti, 2015: p. 497); y, por la otra, en la convicción de que nada de esto resultaría posible si cada padre no se vinculara al mismo tiempo con un "deber de vigilancia" sobre el menor a su cargo (*cf.* Ignacio y Cerra, 2014: p. 604). De modo que, si ahora procedemos a analizar nuestro ejemplo en este contexto legislativo, puesto que P ha incurrido voluntariamente en una obligación, C quedaría exento de toda clase responsabilidad. Desde luego, todavía restaría considerar el monto o valor de la transacción realizada, pero asumamos por el momento que todo se acomoda a la disposición del Código. Tal como está dado el escenario, la ley presume el

consentimiento de P en la maniobra que lo ha perjudicado, lo que en la práctica equivale a eximir a C de cualquier medida sancionatoria.

En cuanto al interrogante que plantea el otro ejemplo, aquí la respuesta parece descansar en la posibilidad de exigirle al usuario que esté al tanto de cierto contexto social, en el que por cierto se cometen maniobras delictivas como el *hacking* o el *phishing* del que precisamente ha sido víctima. ¿Podría decirse, pues, que P debe cargar con el costo de no haber verificado que estaba entregando sus datos a un posible estafador? Nuevamente, la decisión de P en este caso parece tanto o más voluntaria que la decisión de quien ha accedido a cuidar del menor. Además, los costos tampoco serían demasiado significativos. Para no ser víctimas de semejante tipo de maniobras, a veces basta con ignorar ciertos correos electrónicos, o con investigar superficialmente en la web acerca de las modalidades de estafa actualmente imperantes. Si todo esto parece razonable, entonces también lo será la decisión de eximir a C de cualquier clase de responsabilidad.

Sin embargo, llegados a esta altura, no debemos olvidar el segundo de los factores mencionados, relativo a lo que puede hacer el operador de una plataforma digital para verificar la identidad de sus usuarios. Supongamos que los recaudos que toma al respecto son mínimos o prácticamente inconducentes, como verificar que el nombre del correo electrónico del usuario coincida con su nombre real. En ese caso, es posible que el operador deba afrontar alguna clase de sanción por parte del organismo aplicador. Por lo pronto, el organismo podría forzar al operador a desarrollar un procedimiento identificador más eficiente o seguro, suspendiendo mientras tanto algunos de los servicios provistos que dependen de este procedimiento. Lo que no parece plausible es la aplicación de una medida tendiente a compensar a P por la pérdida ocasionada, ya que P, obrando como obró, parece haberse expuesto voluntariamente al resultado finalmente acaecido.

V.II. Todo Pago y los límites de la responsabilidad extracontractual

En cierto modo, el caso de Todo Pago se parece al segundo de los ejemplos analizados en el apartado anterior. Al igual que C, la compañía que realiza la transacción con E, el estafador, fingiendo ser P, Todo Pago opera con alguien que se hace pasar por Paoloni. Sin embargo, a diferencia de P, que habría incurrido en una suerte de negligencia o descuido, Paoloni no parece haber hecho nada de lo que tenga que arrepentirse. Desde ya, lo que puede haber sucedido es que, al momento de pagar en un comercio, Paoloni perdiera de vista su tarjeta de débito por algunos minutos,

precisamente los necesarios para que alguien obtuviera una fotografía de la misma y luego la usara para crear la billetera virtual. Pero este acto también podría haberse gestado de muchas maneras distintas, en las que el dominio del hecho por parte de la víctima fuera casi nulo.[10] Suponiendo que esto haya sido efectivamente así, ¿no cabría responsabilizar a Todo Pago por la pérdida de Paoloni?

La pregunta reviste un carácter meramente hipotético debido a que, en los hechos, fue la propia empresa la que se responsabilizó de manera voluntaria frente a la pérdida. Y no sólo eso: Todo Pago también se comprometió públicamente a introducir una serie de mejoras en su servicio, tendientes a garantizar un mayor nivel de seguridad tanto para sus clientes como para cualquier otro titular de una cuenta bancaria. Esta decisión, por cierto, se habría visto motivada por el estado público que tomó el hecho. Sabido es que ninguna empresa desea cargar en su historial con un antecedente de esta naturaleza. Aunque las consecuencias legales fueran nulas, las pérdidas materiales podrían ser cuantiosas. En tales casos, no es difícil corroborar en el mercado un mecanismo corrector más eficiente que el propio Derecho, una evidencia que ciertas posturas conservadoras o *laissez faire* suelen esgrimir en contra de la regulación estatal (*cf. supra*, sec. 3). Pero también debe decirse que ello funciona así en la medida en que un hecho adquiera cierta envergadura. Y, si bien resulta innegable que en un mundo digitalizado como el nuestro las posibilidades de hacer públicos ciertos conflictos particulares son cada vez más sencillas, esto no tiene por qué minimizar la necesidad de una respuesta jurídica. Después de todo, perfectamente podría suceder que el particular afectado no se mostrara conforme con la solución *no jurídica* que se le ofrece.

A esta altura, sin embargo, el problema surge cuando es la misma ley la que no ofrece una respuesta inconfundible. Con el artículo 5 de la ley 25.326 sucede precisamente esto. Tal como está redactado, resulta sumamente difícil determinar si Todo Pago ha incurrido en una conducta *ilícita*. Que la empresa no fue la responsable de adulterar el consentimiento de Paoloni es algo de lo que no cabría dudar. Pero todavía podría tratarse de un ilícito culposo, es decir: de una omisión de un deber de cuidado por parte de la empresa. Ahora bien, ¿cómo se determina un deber semejante? Llegados aquí, no parece quedar otro remedio que apelar al análisis de costo-beneficio. A continuación, intentaré explicar por qué un análisis de esta naturaleza, aunque diste de resultar enteramente satisfactorio, no sólo no puede

[10] Por ejemplo, supongamos que Paoloni se dispusiera a pagar la cuenta de un bar mediante su tarjeta de débito. El mozo concurre a su mesa con el posnet móvil y, justo cuando ella se dispone a realizar el pago, la persona que manipula la cámara de seguridad del local amplifica la imagen de su mesa y obtiene una fotografía muy nítida de la tarjeta que acaba de extraer de su billetera.

estar ausente en la aplicación de la ley que lleva a cabo el organismo que tiene a su cargo velar por su cumplimiento, sino tampoco en la interpretación que hagan de la misma los tribunales. Para ello, acudiré a la obra de C. Sunstein, una autoridad indiscutible en la materia.

Documenta Sunstein en *Riesgo y razón* el modo en que los tribunales de los Estados Unidos, como asimismo muchos organismos administrativos de control, tal el caso del Ente de Protección Ambiental (EPA) que regula los contaminantes del aire, aplican desde hace tiempo los estatutos dictados por el Congreso no sin antes presuponer la validez de una serie de principios interpretativos que bien cabría denominar "de costo-beneficio" (*cf.* 2006: p. 264 y sigs.). Más específicamente, Sunstein los llama "principios de costo-beneficio por default" [*cost-benefit default principles*], por tratarse de principios sin cuya supuesta operatividad no sería posible interpretar una ley o estatuto evitando desafiar el "sentido común" (ibíd.: p. 268). Entre otras cosas, estos principios estipulan que los organismos "estarán facultados para efectuar excepciones *de minimis* a los requisitos estatutarios, exceptuando a los riesgos *pequeños* de los controles regulatorios", o "para dejar de regular una vez pasado el punto en que la regulación fuese económica o tecnológicamente *factible*", "salvo que el Congreso lo haya explicitado claramente de otra manera" (*ibíd*.: p. 164). ¿Qué constituye, no obstante, un riesgo *pequeño* en materia de salud, por ejemplo? ¿O qué implica la *factibilidad* económica (o tecnológica) de una medida regulatoria? Responder estas preguntas no es tarea sencilla. Sin ir más lejos, repárese en la segunda. Tentativamente podría decirse que "una regulación se torna *no factible* si da como resultado trastornos significativos en la industria, bajo la forma de grandes cantidades de quiebras comerciales, pérdidas sustanciales de empleos o sus equivalentes" (*ibíd.*: pp. 295-6). Sin embargo, tal como advierte Sunstein, respuestas de este talante conllevan el empleo de criterios cualitativos, más que cuantitativos, por lo que su implementación podría dejar "un alto grado de arbitrio a los organismos" (*ibíd*.: p. 296).

Sobre la base de esta propuesta, intentemos reconstruir el deber de cuidado que podría imperar sobre una empresa como Todo Pago. Dos órdenes de cuestiones confluyen paralelamente. El primer orden tiene que ver, por cierto, con lo que cabe esperar de cierto tipo de empresas en materia de protección de datos personales, derechos patrimoniales y, por supuesto, verificación del consentimiento. Las empresas que hoy se conocen como "fintech", tal el caso de Todo Pago, operan en el mundo digital con determinados niveles de resguardo. Muchos de estos resguardos son económica y tecnológicamente factibles para ellas, tanto por no implicar

cuantiosas inversiones de recursos como por depender de mecanismos de fácil implementación. Pero muchos de estos resguardos pueden resultar insuficientes para evitar la filtración de datos o la manipulación de una aplicación por parte de un tercero. En este sentido, entonces, se impone una pregunta: ¿qué ha de considerarse un nivel de protección mínimamente factible? Autores como el propio Sunstein, La Pierre (1977) o McGarity (1994) han llamado la atención sobre lo que sucede cuando las regulaciones "fuerzan la tecnología, en el sentido de que exigen de las empresas (…) que hagan más de lo que la tecnología del momento permite" (Sunstein, 2006: p. 275). En ocasiones, proceder así puede resultar justificable. No obstante, ello a menudo conduce a que las empresas abandonen ciertos proyectos por no poder estar a la altura del desafío que se les impone (*cf. ibíd*.).

Justamente por esta razón, el segundo orden de cuestiones que corre en paralelo al anterior tiene que ver con lo que cabe esperar de tales empresas en materia de innovación tecnológica. En un contexto como el argentino, de alta informalidad económica y bajo nivel de bancarización, desarrollos como el implementado por Todo Pago vendrían a ofrecer una solución nada despreciable. Gracias a su sistema de PINs, personas que, de otro modo, no podrían recibir ciertas sumas de dinero, de repente encuentran una herramienta sencilla para hacerlo. Como ya se viera, lo que diría al respecto una postura *laissez faire* es predecible. Sin embargo, puesto que lo que se requiere es una respuesta jurídica, el problema permanece en pie. Una alternativa, compatible con la postura alarmista antes descripta, consiste en ser taxativos con ciertos desarrollos empresariales, sancionándolos severamente o exigiendo su suspensión. Supongamos entonces que tal es la alternativa por la que se inclina el organismo de control que atiende en el caso de Todo Pago. Si no hubiera ninguna otra empresa capaz de proveer un servicio similar con un mayor nivel de resguardo personal, ¿semejante decisión no sería ciertamente apresurada?

En el medio, además, parece haber otras opciones menos restrictivas. Imaginemos por lo pronto una disposición general como la siguiente:

> **(D1)** Cada vez que se extrae dinero de la cuenta bancaria de una persona utilizando el Servicio de Extracción de Dinero Sin Tarjeta de Débito ofrecido por una billetera virtual, una simple declaración jurada del titular de dicha cuenta afirmando que no ha operado el servicio será suficiente para que la empresa restituya el dinero extraído, lo que deberá acontecer en un plazo máximo de 72 horas de formulada la declaración. Una vez producida la restitución, la empresa dispone de 10 días para presentar su descargo ante la Administración, el cual deberá ir acompañado de las medidas de prueba correspondientes. Transcurrido ese plazo, la decisión se considerará irrecurrible.

Esta disposición puede resultar demasiado drástica para las empresas, por invertir la carga de la prueba a favor de los usuarios o clientes. En un caso como el de Todo Pago, si la empresa tuviera la sospecha de que ha sido la propia denunciante la que gestó la maniobra, justamente con el objeto de volver a cobrar el dinero que ella ya había extraído de su cuenta, diez días quizá resulten insuficientes para reunir las medidas de prueba correspondientes. De cualquier modo, incluso en ese caso, una disposición así resultaría mucho menos restrictiva que una disposición que simplemente obligue a la empresa a retirar su producto del mercado. Y, lo que reviste aquí mayor interés: a diferencia de la respuesta prohibicionista, lo que hace esta respuesta es tomar en cuenta la importancia de la innovación tecnológica en ciertos contextos sociales, como aquellos dominados por una gran informalidad económica y un bajo nivel de bancarización.

Al evaluar cualquier alternativa de solución, desde la prohibicionista a una menos restrictiva, el análisis de costo-beneficio parece volverse imprescindible en algún punto. Este punto, como bien nota Sunstein, tiene que ver con aquellas circunstancias en las que el silencio legislativo parece insuperable; o en las que, para repetir una idea de *Riesgo y razón*, aplicar la ley con un determinado significado desafíe el sentido común (*cf. supra*). Una vez situados allí, el orden de consideraciones que se impone es doble: por una parte, están aquellas que remiten a lo que resulta económica y tecnológicamente factible para una empresa; y, por otra parte, están aquellas que procuran determinar lo deseable en términos sociales. Entre estos dos órdenes de consideraciones bien puede que no exista un punto arquimediano de equilibrio. De cualquier modo, esto no tiene por qué ser un defecto. Si la ley es poco clara, vaga o ambigua, ¿qué más podría pedirse?

V.III. Del consentimiento efectivo al consentimiento putativo o presunto y lo que esto significa en la práctica

Tanto en Derecho Civil como en Derecho Penal suele aceptarse que el consentimiento del damnificado exime de responsabilidad al presunto agresor. Si ahora repasamos los dos apartados precedentes, comprobaremos que la primera parte del apartado V.I estuvo destinada a mostrar en qué circunstancias, y por qué, la ley presume el consentimiento de los padres en cierto tipo de transacciones, siendo justamente este consentimiento el que libera de responsabilidad a las empresas a la hora de tratar ciertos datos o adquirir nuevos derechos patrimoniales. En rigor, sin embargo, debe notarse que este consentimiento *presunto* al que alude la ley no es más que un

derivado del deber de cuidado que detentan los padres sobre los menores a su cargo. Por eso, bien podría decirse que, a efectos puramente procesales, bastará con que se pruebe este vínculo para que de allí se siga un juicio exculpatorio. Ahora bien, dado que esto es así, ¿existe alguna diferencia entre un caso como este, basado en el consentimiento presunto, y cualquiera de los casos tratados en la segunda parte del apartado V.I y en el apartado V.II?

Como ya se viera, la resolución de estos casos depende de que se delimiten como corresponde los deberes de cuidado exigibles a los agentes intervinientes. Tratándose en particular de una empresa como Todo Pago, que opera en una plataforma digital, también aquí se ha comprobado que el modo más factible de obtener una resolución administrativa o judicial que resulte favorable a la misma consiste en reconstruir su deber de cuidado con cierta laxitud o contemplación. Por lo general, esto podrá hacerse a partir de una evaluación deferente de la actuación empresarial que considere las siguientes clases de factores: por una parte, los relativos al grado de innovación tecnológica que podría demandar un determinado entorno social; y, por otra parte, los relativos a los costos financieros y tecnológicos que razonablemente podría afrontar la empresa. Del otro lado, por cierto, están los deberes de cuidado imponibles a los usuarios y/o clientes, así como al ciudadano común que sufre un perjuicio sin desempeñarse en ninguno de estos roles. En tal sentido, una resolución resultará favorable a una ciudadana como Paoloni, que precisamente sufrió un perjuicio sin ser cliente de la empresa que lo hizo posible, en la medida en que también se evalúe de manera contemplativa el deber de cuidado que le era exigible a la hora de operar con sus credenciales bancarias.

En la primera parte de este trabajo sostuve que cuando el Derecho le atribuye a un individuo un «consentimiento putativo» [*imputed consent*], y no en cambio un «consentimiento real» [*actual consent*], lo que hace es tratarlo *como si* ese individuo *hubiera consentido*, a pesar de que, en rigor, no alcancen a estar reunidas ninguna de las condiciones definitorias del consentimiento (*cf. supra*). Ahora bien, ¿en qué casos resulta apropiado apelar a esta noción? Puesto que el consentimiento, bajo cualquier modalidad expresiva, principalmente cumple la función de eximir a su destinatario de la responsabilidad que le cabría por realizar un acto o producir un estado de cosas para los que no está autorizado (Hurd, 1996; McConnell, 2018), resultará apropiado apelar a esta noción cada vez que nuestra intención sea la de eximir al operador de una plataforma digital de toda responsabilidad civil o penal por haber tratado ciertos datos personales sin el consentimiento *real* de su titular. El requisito, desde luego, es que *siempre* se satisfagan las dos condiciones ya aludidas:

en primer lugar, que el operador haya hecho todo lo que le era *razonablemente* exigible para verificar que el consentimiento del titular de los datos personales estaba presente (**a**); y, en segundo lugar, que el titular de estos datos no se haya comportado de manera *negligente* para propiciar su facilitación (**b**). Cuando ambas condiciones logren reunirse, mas sólo cuando este sea el caso, podrá afirmarse con plena justicia que una persona prestó su consentimiento (putativo o presunto), lo que en los hechos significa liberar al operador digital de cualquier responsabilidad civil o penal. En cambio, cuando concurra una de ellas, mas falte la otra, lo razonable será que las cartas se inviertan a favor del usuario. A propósito del caso que ha servido de guía a lo largo de esta sección, lo más probable es que se haya satisfecho la primera condición. Sin embargo, justamente porque no se satisfizo la segunda es que cualquier persona en la posición de Paoloni debería merecer una protección jurídica especial.

VI. Palabras finales: deslindando lo valorativo de lo probatorio

Iniciaba el presente trabajo citando el art. 5 de la Ley de Protección de Datos Personales (Ley 25.326). Según una interpretación bastante literal de este artículo, podría decirse que todo operador de una plataforma digital se hallaría bajo la obligación de procurar el consentimiento de sus usuarios o clientes cada vez que sus datos personales se encuentren en juego. Pero esta obligación, como fácilmente se infiere, conlleva una obligación subsidiaria, a la que intuitivamente podríamos adjudicarle una naturaleza probatoria: la obligación de velar por que este consentimiento se verifique en cada transacción que ocurra en su plataforma. Tal cual intenté mostrarlo desde un principio, el problema se produce al intentar definir los límites de esta obligación.

A los efectos de idear una solución, propuse trabajar sobre la base de un caso imaginario. ¿Qué responsabilidad le cabría al agente comercial C por almacenar en su sitio web una serie de datos personales del usuario P, cuando existen evidencias contundentes que demuestran que P no consintió ese almacenamiento? Si todo lo que aquí estuviera en juego se redujera a probar que P *no otorgó su consentimiento*, entonces la solución consistiría en cargar a C con todas las responsabilidades del caso. No obstante, luego del largo rodeo efectuado, creo que no sólo se ha hecho evidente que contamos con razones utilitarias que desaconsejan un tratamiento semejante en perjuicio de C (*cf. supra*, sec. 5.2), sino que un tratamiento de esta naturaleza tampoco dejaría mejor parados a los usuarios que, más allá de P,

quisieran beneficiarse de lo que en términos personales implica la expansión del comercio electrónico y el universo informativo y transaccional propiciado por internet (*cf. supra*, sec. 4).

Como alternativa frente a lo que denominé un enfoque alarmista, por un lado, y un enfoque concesivo, por el otro (*cf. supra*, sec. 3), en este trabajo propuse un enfoque superador, al que denominé realista y multidimensional (*cf. supra*, sec. 4). Procura ser un enfoque realista, en primer término, porque contempla las limitaciones tecnológicas actualmente imperantes como un hecho a veces decisivo para adoptar una mirada deferente hacia quienes ofrecen sus servicios en el universo digital. Y procura ser un enfoque multidimensional, en segundo término, porque nos insta a brindar un marco protectorio para nuestro derecho a la privacidad, e incluso para algunos de nuestros derechos patrimoniales (por ejemplo, los vinculados a bienes de escasa cuantía), que no oblitere la posibilidad de que sus titulares renuncien a los mismos en procura de ejercitar su propia autonomía. Precisamente cuando existen factores estructurales que tornan técnica o económicamente inviable que nos beneficiemos de los servicios que ofrece una plataforma virtual sin renunciar a algunos resguardos, ciertas formas de consentimiento parecerán aceptables, aunque las mismas no sean capaces de brindar demasiadas certezas sobre la identidad de sus dadores.

De modo general, podría decirse que todos los casos en los que el operador de una plataforma virtual falla en verificar fehacientemente la identidad de sus clientes o usuarios suscitan un problema probatorio. Sin embargo, ¿cuál es el objeto o materia a probar? Intuitivamente podría pensarse que se trata del consentimiento del usuario P al procesamiento de sus datos personales, así como a cierta disposición sobre su patrimonio, dependiendo el tipo de transacción que se constate entre él y el operador C. Ahora bien, en el presente trabajo he sostenido una idea diferente. Dado que bien puede suceder que todos los indicios apoyen la hipótesis de que P no ha consentido lo que se le imputa, pero que esto sea insuficiente para cargar a C con alguna clase de responsabilidad penal o civil, el objeto de la prueba ya no puede ser la falta de consentimiento de P, sino los pasos razonables que haya dado C para evitar cierto tipo de maniobras fraudulentas en perjuicio de P.

Como no podría ser de otra manera, este objeto o materia probatoria plantea sus propias dificultades, comenzando por la de reconstruir con el mayor rigor posible hasta dónde han de llegar las obligaciones verificadoras de los operadores digitales. A lo largo del presente trabajo, tal ha sido la dificultad de la que me he ocupado con

mayor detenimiento. Por cierto, debido a que ella constituye un asunto netamente valorativo que, en rigor, antecede a lo que debe probarse, mal haríamos aquí en considerarla una dificultad estrictamente probatoria. Pero puesto que ella demanda una respuesta, el Derecho probatorio tampoco puede ignorarla. Las recomendaciones valorativas que he formulado a lo largo de este trabajo tan sólo deben leerse como una humilde contribución en esta materia, aunque la terea que todavía queda pendiente sea ciertamente muy grande.

REFERENCIAS

ABRAMOVICH, Víctor y COURTIS, Christian (2000). El acceso a la información como derecho. *Anuario de Derecho a la Comunicación,* 1 (1), Buenos Aires, Argentina: Editorial Siglo XXI.

ACQUISTI, Alessandro y GROSSKLAGS, Jens (2008). What Can Behavioral Economics Teach Us About Privacy? En A. Acquisti *et al* (editores), *Digital Privacy: Theory, Technologies and Practices* (pp. 363-380). Florida, Estados Unidos: Taylor and Francis Group.

ALEXANDER, Larry (1996). The Moral Magic of Consent (II). *Legal Theory*, 2 (3), 165-174. URL: https://doi.org/10.1017/S1352325200000471.

ALLEN, Darcy y BERG, Chris (2014). The Sharing Economy. How Over-Regulation Could Destroy an Economic Revolution. *Institute of Public Affairs*, 1-39. URL: https://darcyallen.net/2014/12/31/the-sharing-economy-how-over-regulation-could-destroy-an-economic-revoltion/.

BAROCAS, Solon y NISSENBAUM, Helen (2014). Big Data's End Run around Anonymity and Consent. En J. Lane, V. Stodden, S. Bender y H. Nissenbaum (editores), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (pp. 44-75). Cambridge, Reino Unido: Cambridge University Press.

BERENDT, Bettina, GÜNTHER, Oliver y SPIEKERMAN, Sarah (2005). Privacy in E-Commerce: States Preferences vs. Actual Behavior. *Communications of the ACM*, 48, 101-106.

BIETTI, Elettra (2019). Consent as a Free Pass: Platform Power and the Limits of the Informational Turn. *Pace Law Review*, 40 (1), 310-398.

CALO, Ryan (2014). Digital Market Manipulation". *The George Washington Law Review*, 82 (4), 995-151.

CASTRO, Daniel y McQUINN, Alan (2014), The Economic Costs of the European Union's Cookie Notification Policy. *The Information Technology and Innovation*

Foundation, 1-11. URL: http://www2.itif.org/2014-economic-costs-eu-cookie.pdf.

DWORKIN, Ronald (2019). *El derecho de las libertades*. Lima, Perú: Palestra Editores.

GASCÓN ABELLÁN, Marina (2010). *Los hechos en el derecho. Bases argumentales de la prueba*. Madrid, España: Marcial Pons.

HANSON, Jon D. y KYSAR, Douglas A. (1999). Taking Behavioralism Seriously: Some Evidence of Market Manipulation*. Harvard Law Review*, 112, 1420-1569.

HERMSTRÜWER, Yoan (2017). Contracting Around Privacy. The (Behavioral) Law and Economics of Consent and Big Data. *JIPITEC*, 8, 9-26.

HURD, Heidi (1996). The Moral Magic of Consent. *Legal Theory*, 2 (2), 121-146. URL: https://doi.org/10.1017/S1352325200000434.

IGNACIO, Graciela Cristina y CERRA, Silvina (2014). Representación, Disposición y Administración de los Bienes del Hijo Menor de Edad" (Capítulo 8). En Julio César Rivera y Graciela Medina (directores), *Código Civil y Comercial de la Nación Comentado,* Tomo II, Arts. 401 a 723 (pp. 591-617). Buenos Aires, Argentina: Thomson Reuters/La Ley.

LA PIERRE, Bruce (1977). Technology-Forcing and Federal Environmental Protection Statutes. *Iowa Law Review*, 62, 771-811.

LAYTON, Roslyn (2018). Statement before the Federal Trade Commission. *The American Enterprise Institute.* URL: https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0051-d-0021-152000.pdf.

LORENZETTI, Ricardo Luis (2015). *Código Civil y Comercial de la Nación Comentado*, Tomo IV, Arts. 594 a 723. Santa Fé, Argentina: Rubinzal-Culzoni Editores.

McCONNELL (2018). When Is Consent Required? En A. Müller y P. Schaber (editores), *The Routledge Handbook of the Ethics of Consent* (pp. 75-84). Abingdon, Reino Unido: Routledge.

McGARITY, Thomas O. (1994). Radical Technology-Forcing in Environmental Regulation. *Loyola of Los Angeles Law Review*, 943, 943-958.

MIK, Eliza (2012). Mistaken Identity, Identity Theft and Problems of Remote Authentication in E-Commerce. *Computer Law and Security Review*, 28: 396-402. URL: https://www.sciencedirect.com/science/article/pii/S0267364912000611?via%3Dihub.

NINO, Carlos S. (2007). *Ética y derechos humanos.* Buenos Aires, Argentina: Astrea.

NORBERG, Patricia A., HORNE, Daniel R. y HORNE, David A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *The*

Journal of Comsumer Affairs, 41 (1), 100-126. URL: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1745-6606.2006.00070.x.

O'NEILL, Onora (2002). *Autonomy and Trust in Bioethics.* Cambridge, Reino Unido: Cambridge University Press.

PAZOS CASTRO, Ricardo (2015). El funcionamiento de los motores de búsqueda en Internet y la política de protección de datos personales, ¿una relación imposible? *InDret. Revista para el análisis del derecho,* 1, 1-50.

POSNER, Richard (2008). Privacy, Surveillance, and Law. *University of Chicago Law Review*, 245, 245-260.

SACHS, Benjamin (2009). Consumerism and Information Privacy: How Upton Sinclair Can Again Save Us from Ourselves. *Virginia Law Review*, 95, 205-252. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1373123.

SUNSTEIN, Cass (2006). *Riesgo y razón. Seguridad, ley y medioambiente.* Buenos Aires, Argentina: Katz.

SUSSER, Daniel (2019). Notice After Notice-And-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't. *Journal of Information Policy*, 9, 37-62. URL: https://pennstate.pure.elsevier.com/en/publications/notice-after-notice-and-consent-why-privacy-disclosures-are-valua.

THIERER, Adam (2013). A Framework for Benefit-Cost Analysis in Digital Privacy Debates. *George Mason Law Review*, 20 (4), 1055-1105. URL: https://www.mercatus.org/publications/technology-and-innovation/framework-benefit-cost-analysis-digital-privacy-debates.

——— (2014). *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom*, Virginia, Estados Unidos: Mercatus Center at George Mason University.

VAIDHYANATHAN, Siva (2011). *The Googlization of Everything: (And Why We Should Worry*). California, Estados Unidos: University of California Press.

WESTEN, Peter (2004). Some Common Confusions About Consent in Rape Cases. *Ohio State Journal of Criminal Law*, 2 (1), 333-359. URL: https://kb.osu.edu/handle/1811/72856.

WILLIS, Lauren E. (2014). Why Not Privacy by Default? *Berkeley Technology Law Journal*, 29 (1), 61-133. URL: https://www.jstor.org/stable/24119938?seq=1.