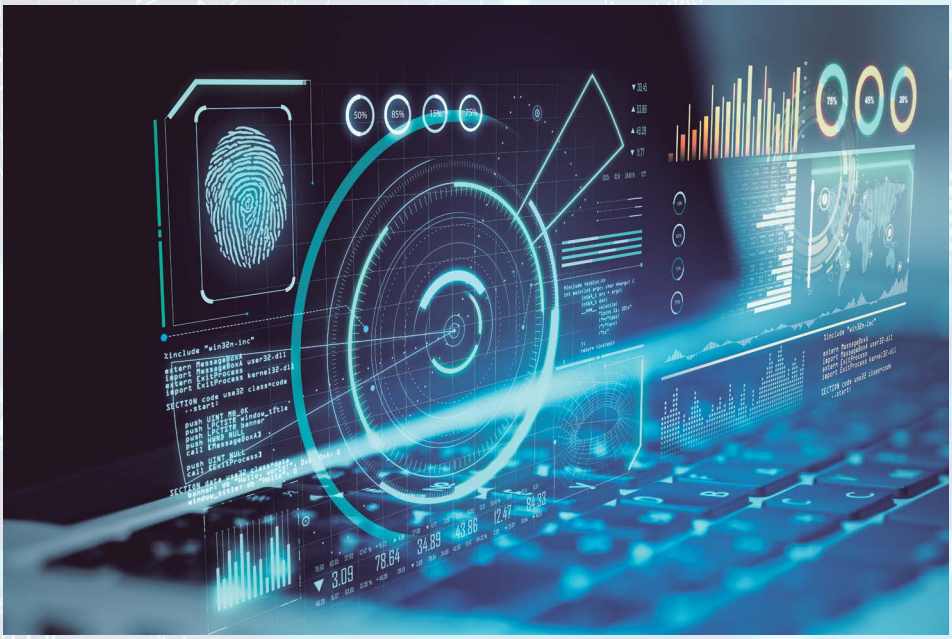
Implicaciones jurídicas en el entorno del big data: el caso del APP Navega Seguro

Cómo citar este artículo [Chicago]: Becerra, Jairo, Bibiana Beatriz Luz Clara, John Grover Dorado, John Velandia, José Araoz Fleming y Marco Emilio Sánchez Acevedo. "Implicaciones jurídicas en el entorno del big data: el caso del APP Navega Seguro". *Novum Jus* 17, núm. 1 (2023): 357-388. https://doi.org/10.14718/NovumJus.2023.17.1.15

Jairo Becerra / Bibiana Beatriz Luz Clara / John Grover Dorado / John Velandia / José Araoz Fleming / Marco Emilio Sánchez Acevedo



Código: 1317954630 • Autor: iStock

https://doi.org/10.14718/NovumJus.2023.17.1.15

Implicaciones jurídicas en el entorno del big data: el caso del APP Navega Seguro*

Jairo Becerra**
John Velandia***
Marco Emilio Sánchez Acevedo****
Universidad Católica de Colombia
Bibiana Beatriz Luz Clara*****
John Grover Dorado******
José Araoz Fleming*******
Universidad Católica de Salta

Recibido: 15 de diciembre de 2022 **| Evaluado:** 15 de enero de 2023 **| Aceptado:** 2 de febrero de 2023

Resumen

El artículo presenta el desarrollo de la aplicación móvil denominada Navega Seguro, la cual ha involucrado herramientas de big data y un marco de referencia del uso de aplicativos que usan datos abiertos públicos frente a temáticas del derecho TIC, como la protección de datos, los términos y condiciones de la aplicación, el acceso a la información y la ciberseguridad, por medio de este estudio de caso. Navega Seguro ha sido desarrollada en el marco de la investigación internacional "Derecho, cambio climático y big data. Fase II", con un enfoque interdisciplinario, que permite observar las fortalezas del trabajo investigativo de áreas como el derecho, la ingeniería, las comunicaciones y el diseño, con el apoyo de organizaciones gubernamentales.

Palabras clave: derecho, cambio climático, protección de datos, acceso a la información, datos abiertos, *software*, toma de decisiones.

* Este artículo es resultado del proyecto de investigación Fase II. Derecho, cambio climático y big data, del grupo de investigación Derecho Público y TIC y del grupo de investigación Software inteligente y convergencia tecnológica.

** Abogado, doctor en Derecho y Ciencia Política. Director del Centro de Investigaciones Sociojurídicas Cisjuc, de la Facultad de Derecho de la Universidad Católica de Colombia. ORCID: https://orcid.org/0000-0001-6694-4950. Correo electrónico: jabecerrao@ucatolica.edu.co

*** Ingeniero de sistemas, doctorando en Learning Analytics. Profesor e investigador de la Facultad de Ingeniería, de la Universidad Católica de Colombia. ORCID: https://orcid.org/0000-0001-9217-4726. Correo electrónico: javelandia@ucatolica.edu.co

**** Abogado, magíster en Ciberseguridad y Ciberdefensa, doctor en Tecnologías y servicios de la sociedad de la información, línea de investigación en derecho y tecnologías. ORCID: https://orcid.org/0000-0002-7745-2182 Correo electrónico: mesanchez@ucatolica.edu.co

***** Abogada, doctora en Derecho Procesal. Docente e investigadora de Universidad Católica de Salta, Universidad FASTA y Universidad CAECE. ORCID: https://orcid.org/0000-0003-4952-5644. Correo electrónico: luzbibianaclara@gmail.com

****** Abogado, magíster en Derecho de TIC. Vicedirector del Instituto de Derecho de Nuevas Tecnologías e investigador de la Universidad Católica de Salta. ORCID: https://orcid.org/0000-0003-1160-1285. Correo electrónico: johnidorado@hotmail.com

******* Abogado, especialista en Abogacía del Estado. Director del Instituto de Derecho de las Telecomunicaciones, Informática y nuevas TIC, del Colegio de Abogados y Procuradores de Salta; director del Instituto de Derecho de Nuevas Tecnologías de la Universidad Católica de Salta. ORCID: https://orcid.org/0000-0002-3182-1771. Correo electrónico: jdaraoz@ucasal.edu.ar

https://doi.org/10.14718/NovumJus.2023.17.1.15

Legal Implications in the Context of Big Data: The Case of the Navega Seguro App

Jairo Becerra[**]
John Velandia[***]
Marco Emilio Sánchez Acevedo[****]
Universidad Católica de Colombia
Bibiana Beatriz Luz Clara[*****]
John Grover Dorado[******]
José Araoz Fleming[*******]
Universidad Católica de Salta

Received: December 15, 2022 **| Evaluated:** January 15, 2023 **| Accepted:** February 2, 2023

Abstract

This article presents the development of the Navega Seguro mobile app, which used big data tools and a framework for the use of apps that utilize open data regarding subjects related to information and communication technology (ICT) law such as data protection, application terms and conditions, access to information, and cybersecurity, through this case study. The Navega Seguro has been developed as part of the second phase of the international research program "Law, Climate Change, and Big Data," with a collective and interdisciplinary approach in areas such as law, engineering, communications, and design, with the support of governmental organizations.

Keywords: law, climate change, data protection, information access, open data, software, decision making.

Introducción

La cuarta revolución industrial y la aparición de nuevas tecnologías han traído retos al mundo del derecho, al ampliar la frontera de las relaciones humanas y, por lo tanto, crear situaciones que requieren otros análisis jurídicos y, en algunos casos, otras fuentes de derecho.

Un ejemplo de lo expuesto es el desarrollo y el uso de *software*. Esto es visto como una necesidad en nuestra sociedad, de importancia clave para ejecutar distintas actividades y por eso debe ajustarse plenamente a la normativa vigente, para que no se vulneren los derechos de las personas.

El caso que nos ocupa, el *software* Navega Seguro, se trata de un programa destinado a su uso en algunos de los principales puertos de Colombia, como es el de Cartagena, donde la Dirección Nacional Marítima (Dimar) posee la capacidad de captar datos. Lo novedoso de este sistema es que brinda información a quienes desempeñan actividades náuticas en la zona para que puedan navegar con mayor seguridad, pues les da a conocer las condiciones climáticas existentes y las previstas, mediante la combinación de variables y la utilización de herramientas de inteligencia artificial (IA). Se desarrolló como una aplicación móvil, en el marco de la investigación internacional "Derecho, cambio climático y big data. Fase II", liderada por la Universidad Católica de Colombia, en conjunto con la Dimar, la Universidad de Texas (Estados Unidos), la Universidad Católica de Salta (Argentina) y la Universidad Santo Tomás (Colombia).

En estos tiempos, de alta y continua generación y procesamiento de información por medio de computadoras, dispositivos móviles, servidores, redes, sistemas informáticos y electrónicos, es necesario proteger esos datos. El conjunto de procedimientos y estrategias tendientes a ello es lo que se conoce como ciberseguridad. A su vez, en el proceso con la Dimar, íntimamente ligadas con las nociones de ciberseguridad, se han tenido en cuenta el conjunto de acciones y operaciones activas o pasivas desarrolladas en el ámbito de las redes, sistemas, equipos, enlaces y personal de los recursos informáticos y teleinformáticos de la defensa, a fin de asegurar el cumplimiento de las misiones o los servicios para los que fueran concebidos, concepto más conocido como ciberdefensa.

Así mismo, en el marco de la transparencia, se observa que los datos públicos y abiertos se convierten en una herramienta esencial para adelantar investigaciones y elaborar prototipos que propicien el progreso nacional, cuyo manejo, en un contexto

legal claro, es beneficioso para la sociedad. Veremos cómo se relaciona este tipo de avances con la protección de datos, los términos y las condiciones de la aplicación, el acceso a la información y la ciberseguridad en las nuevas realidades y dinámicas.

El APP Navega Seguro

En el marco del entendimiento de la relación que se presenta entre el derecho y los nuevos desarrollos tecnológicos,[1] la realidad social está formada por un conjunto de factores globales e individuales, por lo que, para entender dicha relación, es necesario abordarlos desde la misma óptica. Áreas como la inteligencia artificial están siendo utilizadas para resolver problemas del orden cuantitativo y cualitativo relativos al derecho,[2] que exigen el desarrollo, por ejemplo, de un lenguaje simple de las herramientas tecnológicas que se usan en ese campo;[3] esto, con el fin de lograr su mejor entendimiento por parte de los usuarios, para aumentar su utilización y efectividad. Ello debe trascender el derecho y el desarrollo de instrumentos jurídicos, como la ley de transparencia, a campos sociales como el periodismo, que son también pilares del desarrollo de la sociedad, y permitirles acceder a datos públicos que, sin estas normas, no serían de fácil acceso.[4] Con estas consideraciones, se estableció la posibilidad de crear una herramienta de *software* que ayudará a la toma de decisiones, en el marco del respeto a la normativa y con el entendimiento de las conjunciones que tienen el derecho y las TIC.

Navega Seguro es una aplicación móvil que permite consultar variables asociadas al clima en las costas marítimas colombianas en tiempo cercano al real. El alcance de la primera fase se enfoca en la bahía de Cartagena. Para desarrollarla, se han utilizado las últimas tendencias en tecnología, por ejemplo, despliegue en la nube, lo que garantiza alta disponibilidad, seguridad de la información y escalabilidad; de esta manera, siempre se tendrá la información lista para consultar. Además, se tuvieron en cuenta aspectos tan diversos como el diseño de la aplicación en el contexto de los macrodatos y la influencia del diseño gráfico, desde la perspectiva

1 Germán Silva García, "¿El derecho es puro cuento? Análisis crítico de la sociología jurídica integral", *Novum Jus 16*, núm. 2 (2022): 57, https://doi.org/10.14718/NovumJus.2022.16.2.3

2 Luis Germán Ortega Ruiz y Jairo Becerra, "La inteligencia artificial en la decisión jurídica y política", *Araucaria, Revista Iberoamericana de Filosofía, Política, Humanidades y Relaciones Internacionales*, núm. 49 (2022): 220-221, https://dx.doi.org/10.12795/araucaria.2022.i49.10

3 Paula Pérez et al., "The Colombian Freedom of Information Act Using Media Literacy to Understand and Implement the Law" en *Media Literacy in a Disruptive Media Environment*, ed. William G. Christ y Belinha S. de Abreu (Nueva York: Routledge, 2020), 233.

4 Julián Rodríguez y Andrew M. Clark, "Big data y periodismo: cómo el periodismo estadounidense está adoptando el uso de big data", *Novum Jus 15*, núm. 1 (2021): 76, https://doi.org/10.14718/NovumJus.2021.15.1.4

del replanteamiento de gráficas, así como el entendimiento del cambio que se suscita en su entorno, para poder transmitir de forma correcta los datos adecuados a estas nuevas realidades.[5]

Con respecto al análisis de datos, se utilizan tres aproximaciones: i) analítica descriptiva, para revisar los datos que se generaron en el pasado; ii) analítica prescriptiva, para sugerir algunas decisiones con base en indicadores predefinidos, y iii) analítica predictiva, que utiliza lógica difusa para inferir si los navegantes deberían llevar a cabo actividades náuticas y así prevenir accidentes marítimos.

Los datos usados para alimentar la aplicación móvil se recolectan mediante el Centro Colombiano de Datos Oceanográficos (Cecoldo), institución adscrita a la Dirección General Marítima (Dimar). Estos son recopilados en tiempo real, gracias a la red de monitoreo meteomarino de la Dimar en cada una de las más de cincuenta estaciones entre meteorológicas y mareográficas ubicadas a lo largo de la zona costera y áreas insulares, con el propósito de ayudar a la toma de decisiones informadas por parte de las autoridades, las compañías, los pescadores, investigadores y ciudadanos.

Para aprovechar los datos almacenados, obtenidos con los instrumentos de medición marítimos, se crea una aplicación móvil capaz de admitir e interpretar los valores recibidos y emitir notificaciones. Esto se logra con unas variables de medición y escalas generales, las cuales brindan información descriptiva para los posibles estados en los que puede estar el mar, lo que facilita la toma de decisiones.

[5] Jeice Hernández, "El reto de la cuarta revolución industrial en Colombia: datos, diseño y artes" en *Colombia 4.0: retos y perspectivas sobre el desarrollo de la cuarta revolución industrial*, ed. Eduardo Andrés Perafán del Campo et al. (Bogotá: Tirant lo Blanch, 2020, 163.

Figura 1. Inicio de sesión

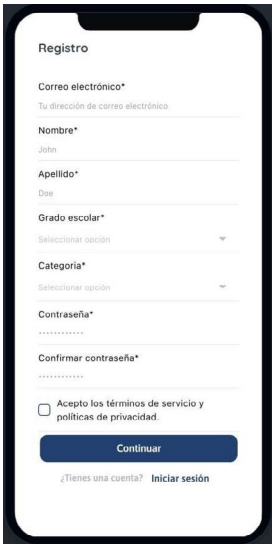
Fuente: elaboración propia

Para registrarse en el APP, se debe hacer clic en Crea una cuenta nueva, ingresar los datos requeridos, aceptar los términos y condiciones y hacer clic en Continuar.

Figura 2. Iniciar sesión > Crear una cuenta

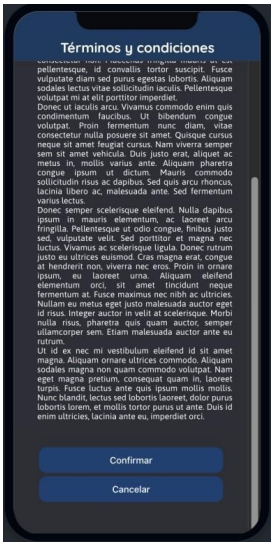
Fuente: elaboración propia

Figura 3. Registro



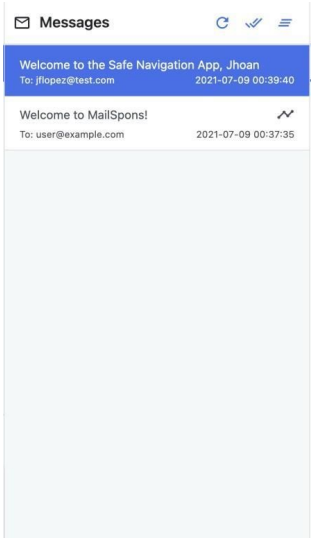
Fuente: elaboración propia

Figura 4. Términos y condiciones



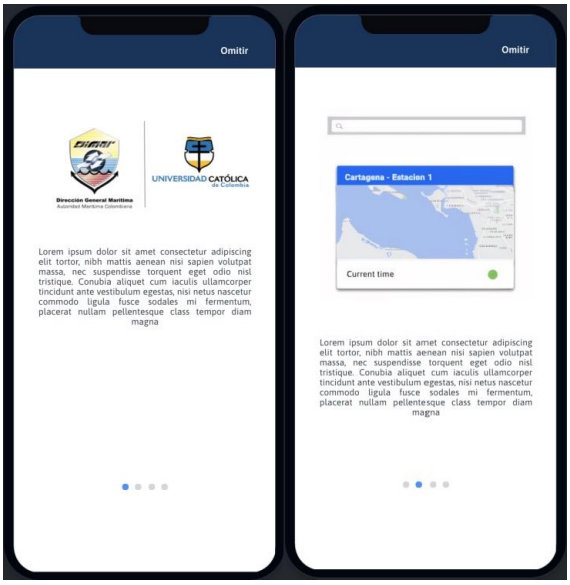
Fuente: elaboración propia

Figura 5. Correo de bienvenida



Fuente: elaboración propia

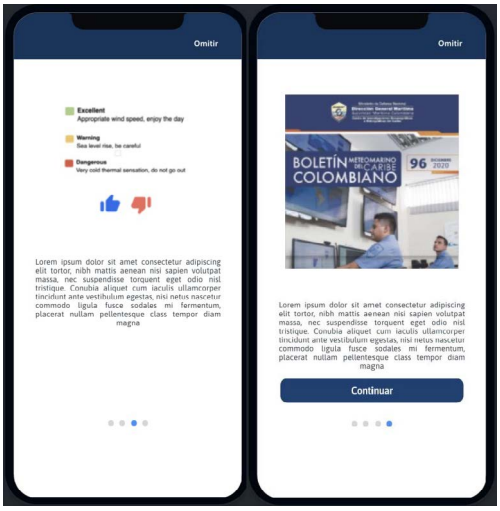
Figura 6. Tutorial pasos 1 y 2



Fuente: elaboración propia

Ya que la cuenta creada es nueva, el APP lo llevará a un corto tutorial, aunque se puede evitar con hacer clic en Omitir.

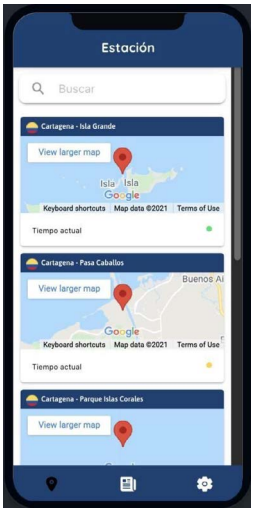
Figura 7. Tutorial pasos 3 y 4



Fuente: elaboración propia

Después de terminar el tutorial o iniciar sesión (para usuarios registrados), el APP se redirige a la pantalla de estaciones, que tienen el respectivo nombre y la ubicación. Si se prefiere, se puede hallar una estación específica mediante el campo de búsqueda.

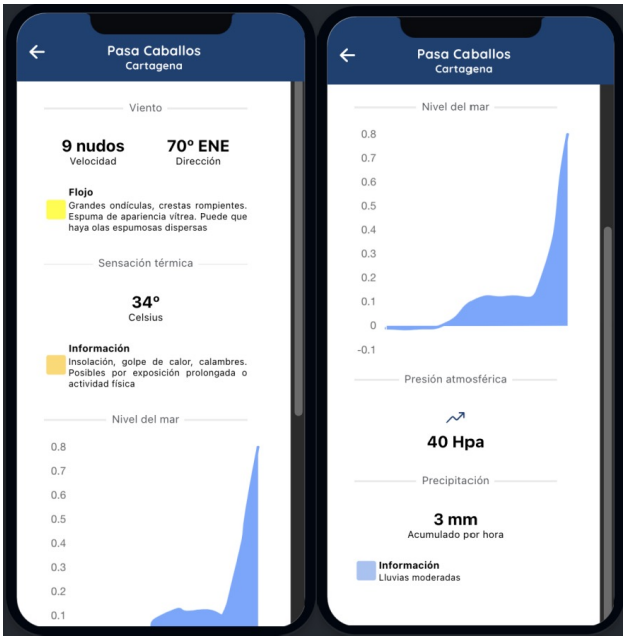
Figura 8. Estaciones



Fuente: elaboración propia

Si se desea ver la información de alguna estación, es posible seleccionarla y se arrojarán los datos más recientes de las variables meteomarinas, con la descripción de alguna de ellas.

Figura 9. Información estación 1 y estación 2



Fuente: elaboración propia

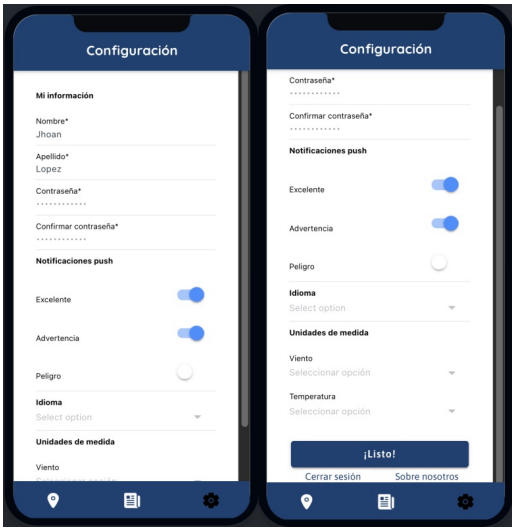
La herramienta cuenta con un boletín informativo del Pacífico colombiano, que puede ser consultado mes a mes. Esta opción se encuentra en el ícono central del menú inferior.

Figura 10. Estaciones

Fuente: elaboración propia

Si se desea actualizar datos de la cuenta, configurar el lenguaje del APP, actualizar las unidades de medida o las notificaciones, se debe seleccionar el ícono de rueda dentada en el menú inferior.

Figura 11. Configuraciones 1 y 2



Fuente: elaboración propia

Por último, podemos establecer que la aplicación capta datos abiertos y datos públicos, en términos generales, lo que conlleva a la formulación de preguntas relativas a la legalidad de su recolección y se crea, a su vez, la necesidad de ser analizadas desde varias perspectivas, para entender la oportunidad de nuevas relaciones y marcos jurídicos o su interpretación.

Los datos abiertos, la transparencia y el acceso a la información pública

El primer análisis surge desde la perspectiva de los datos abiertos y la transparencia, en busca de identificar si este tipo de datos es captado por la aplicación y su posterior manejo, de acuerdo con el marco legislativo actual en Colombia. Entre los datos recolectados no identificamos alguna restricción, ya sea en razón a la reserva por un daño a un interés colectivo (defensa nacional) o por un daño a un derecho personal (derecho a la intimidad).[6] Dichos datos son abiertos, clasificados como información pública porque son recolectados por un sujeto obligado por la Ley de transparencia (en este caso, Dimar).[7]

El alcance del procesamiento de los datos abiertos (aquellos que son primarios) y su posterior tratamiento pueden constituir un nuevo conjunto de estos, que podrían ingresar a la esfera de los datos clasificados o, incluso, reservados. Ejemplo de ello es que, a partir del número de consultas de un usuario sobre una zona determinada, cruzados con el nivel del mar, la emisión de rayos UV y la hora de consulta de la aplicación, se podría determinar la ubicación aproximada de un sujeto, lo cual pasaría a ser asunto privado, en los términos de la Ley de protección de datos de Colombia.

¿Cómo proceder, entonces, en este contexto? El marco legal no es claro sobre la generación de datos indirectos que afecten derechos; por consiguiente, es posible abstenerse de cualquier consideración o medida legal. No obstante, la realidad exige un marco que contemple la emisión de alertas a los usuarios acerca de las consecuencias del uso de ese tipo de aplicaciones. Esto, desde una perspectiva moral y ética amplia que involucra una filosofía más personal que legal, acorde con fenómenos disruptivos

6 Jairo Becerra et al., *La responsabilidad del Estado por la utilización de las tecnologías de la información y la comunicación (TIC)* (Bogotá: Universidad Católica de Colombia, 2015), 8.

7 Colombia, Congreso de la República, *Ley 1712 de 2014*, "Por medio de la cual se crea la Ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones" (Bogotá: *Diario Oficial* núm. 49 084, 6 de marzo de 2014).

que, por ser nuevos, son poco entendidos y precisan constante evolución política, social y legal.

Los datos, los macrodatos y sus implicancias jurídicas

El *software* que estamos analizando, como todo programa, requiere que le sean cargados distintos tipos de datos. El dato es la más pequeña unidad de información que se utiliza y se clasifica en público y privado. Los públicos son aquellos de fácil obtención, a los que cualquiera puede acceder, mientras que los privados los indica el titular cuando le son solicitados para adelantar trámites de su interés.

Entre estos últimos existen los sensibles, que son aquellos que corresponden a la intimidad de la persona y solo se pueden dar a conocer con el consentimiento expreso de su titular, ya que pueden provocar discriminación; por el mismo motivo, no pueden cargarse en bases de datos, salvo con la debida autorización de su dueño. Son los relativos a raza, religión, cuestiones de salud, genéticos, ideas políticas, etc.

Hay información que es requerida para cumplir una función social, como prevenir accidentes o enfermedades, entre otros. Navega Seguro se encuentra en esta categoría, pues permite que las personas conozcan las condiciones climáticas y del mar antes de decidir si salen a navegar o no, en el caso de que las condiciones fueran adversas o peligrosas. Los datos que la aplicación solicita son públicos, salvo el correo electrónico, usado para hacerle saber novedades.

Un producto de nuestro tiempo y de la dinámica de las nuevas tecnologías es la posibilidad de obtener y manejar los grandes volúmenes de datos: macrodatos.[8] Esta información se procesa muy velozmente, en tiempo real. Siempre fue importante contar con información adecuada y de calidad y, tenerla en grandes cantidades es un agregado muy importante.

[8] La inteligencia de datos o big data es un "término que comúnmente es utilizado para para identificar una fórmula o conjunto de éstas que surge dada la imposibilidad de analizar inconmensurables cantidades de información a través de las formas tradicionales de tratamiento de datos". Nayibe Chacón Gómez, "Las tecnologías disruptivas: los retos a la protección de datos" en *Memórias do XXIII Congreso Ibero-americano de Direito e Informática 2019*, org. Fiadi y Luiz Fernando Martins Castro (Timburi: Cia do eBook, 2019), 446.

El uso de macrodatos está cambiando el mundo empresarial porque facilita la toma de decisiones, lo que implica enormes ventajas sobre quienes no lo hacen, pues permite conocer las necesidades del momento y adelantarse frente a los competidores.

Es importante que dichos datos sean de calidad, es decir, que sean exactos, actuales y veraces, que se puedan medir y representar de manera comprensible, con la finalidad de encontrar patrones. La información errónea, antigua e incompleta puede causar serios daños, máxime cuando se procede al cruce de diferentes fuentes que llevarían a determinar perfiles de usuarios, sus gustos y sus tendencias, entre otras cosas.

Su conocimiento y manipulación por terceras personas puede afectar seriamente el derecho a la privacidad; por eso, su resguardo ha dado lugar a lo que se conoce como derechos ARCO, que son aquellos que permiten a su titular solicitar, a los sujetos que estén en posesión de sus datos, el acceso, la rectificación, la cancelación o la oposición respecto al tratamiento de estos.

Las ventajas de tal uso llegan a todos los campos y se encuentran en constante evolución, por lo que esta práctica seguirá incrementándose en los próximos años, haciendo que sean minimizados los riesgos asociados que pudieran acontecer, dado que es posible ofrecer una visión cada vez más aproximada de los distintos tipos de recursos y posibilidades y sus implicancias, permitiendo que sean prestados nuevos servicios antes impensados al obtener nuevos conocimientos.

No obstante, si la información no es administrada por profesionales competentes y comprometidos, que trabajan con transparencia, responsabilidad y confidencialidad, pueden surgir riesgos asociados. Entre ellos podríamos mencionar: sacar conclusiones erróneas, caer en sesgos cognitivos e invadir la privacidad de las personas, pues se podría individualizarlas aun cuando la información proporcionada fuera de datos anónimos.

Puede ocurrir que algunos de los programas que utilizamos a diario no sean del todo correctos o registren fallas, que lleven a obtener resultados defectuosos y, por lo tanto, que se vuelvan inseguros en su aplicación. En tales casos, el proveedor de estos servicios informáticos deberá responder por los daños que pudiera haber causado. El responsable de recopilar los datos y guardarlos en sus bases también está sujeto a la aplicación y al resguardo de los principios de protección del dato personal y el Reglamento de protección de datos de la Unión Europea.

La seguridad informática resulta ser el mayor reto, ya que, por su vulnerabilidad, los programas suelen ser objeto de ciberataques, pues necesitan recopilar información de muchas fuentes, que debe validarse.

El riesgo de almacenamiento inseguro es otro punto a tener en cuenta, puesto que los datos pueden ser accedidos por terceros no autorizados. Por ello, la información debe almacenarse encriptada. Se debe procurar que, si existen datos sensibles, se guarden cifrados para que no pueda accederse a ellos sin autorización y que se requiera validación de los usuarios para la realización de consultas y análisis.

Hoy en día, muchos sistemas incorporan IA, con la finalidad de automatizar diversas funciones. Esta práctica constituye el mayor cambio disruptivo de los últimos tiempos, pues lleva a la transformación de las costumbres y de la forma de hacer las cosas; además, se encuentra en avance, porque se incluyen algoritmos de machine learning y forecasting behaviour,[9] propios de la cuarta revolución industrial en la cual nos encontramos inmersos, con todos sus dispositivos electrónicos conectados a Internet. Es por ello que en el campo de la navegación se hace necesario aprovechar las posibilidades que la tecnología pone a disposición de la gente de mar, para viajar seguros y en las mejores condiciones, como se pretende con el *software* que aquí se presenta.

Dado el desarrollo sin pausa de la tecnología, se hace necesario contar con normas claras que indiquen hasta qué punto aquella que utiliza IA para obtener e inferir datos puede volverse intrusiva y lesionar derechos, y cómo protegerse, ya que, aun cuando se indique que no se solicita información privada, el *software* puede tomarla por defecto.

Los países se encuentran abocados al estudio de esta temática, con la finalidad de dictar normas regionales o por bloques. En mayo de 2019, la OCDE aprobó la Recomendación sobre inteligencia artificial, basada en valores centrados en el ser humano y en el desarrollo inclusivo y sostenible, la robustez y la seguridad de los sistemas. Luego, también en 2019, los países del G20, reunidos en Japón, firmaron la Declaración sobre comercio y economía digital, resaltaron el carácter humanista que debe reconocer la IA y ratificaron los principios expuestos por la OCDE.[10] En

[9] Aprendizaje automático y predicción.

[10] Lucana María Estévez Mendoza, "Regulación de la inteligencia artificial y la protección de los derechos fundamentales en la cuarta revolución industrial" en *Memórias do XXIII Congreso Ibero-americano de Direito e Informática 2019*, org. Fiadi y Luiz Fernando Martins Castro (Timburi: Cia do eBook, 2019), 271.

el caso de la Unión Europea, se ha elaborado el *Libro blanco sobre la inteligencia artificial*,[11] que pone el énfasis en la transparencia, la excelencia y la confianza —para evitar la existencia de "cajas negras"— y en el comportamiento basado en la ética, conscientes de que la tecnología adquiere cada día mayor preponderancia en nuestra vida y actividades, con miras al desarrollo y al crecimiento sostenibles y al avance social permanente. Como vemos, todos coinciden en que debe ser posible la convivencia de los derechos fundamentales consagrados junto a los novedosos desarrollos de la IA, aunque en la práctica no sea fácil de lograr.

Otro concepto en expansión y que hoy se analiza es el de "privacidad por diseño",[12] que se refiere a que la privacidad está compuesta por una filosofía y un diseño tecnológico, lo que constituye una arquitectura de sistema de información y, al mismo tiempo, un modelo de negocios. En esencia, se pretende mantener las garantías de seguridad en la privacidad de los datos frente a las tecnologías disruptivas en evolución. Asociado aparece el concepto de "privacidad por defecto", que implica la obligación de que el titular de los datos preste su consentimiento para poder compartir sus datos, es decir, que todo sistema se estructure de tal modo que no permita compartir su información, salvo que lo consienta su titular.

Ciberseguridad y ciberdefensa

En estos tiempos de continua generación y procesamiento de información mediante dispositivos informáticos y electrónicos, y la consiguiente necesidad de protegerla (ciberserguridad), es preciso asegurar el uso de las redes propias y negarlo a terceros por medio de un conjunto de acciones preventivas. En este caso vamos a emplear estos conceptos en el *software* Navega Seguro.

Tanto en el ámbito gubernamental como en el empresarial —privado—, la necesidad de tener un sistema de gestión de seguridad de la información es cada vez mayor. La gestión de los riesgos por medio de un sistema de gestión de seguridad de la información nos va a permitir preservar la confidencialidad, la integridad y la disponibilidad de esta en la empresa, ante los clientes y ante las partes interesadas en el negocio. En ese sentido, la Recomendación UIT-T X.1205 contiene la siguiente definición:

[11] Comisión Europea, *Libro blanco sobre la inteligencia artificial. Un enfoque europeo orientado a la excelencia y la confianza. COM(2020) 65 final* (Bruselas, 19 de febrero de 2020).

[12] Privacy by design es un concepto postulado por Ann Cavoukian, comisionada de Información y Privacidad de Ontario (Canadá), a fines de la década del noventa.

> […] la ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: • disponibilidad; • integridad, que puede incluir la autenticidad y el no repudio; • confidencialidad.[13]

Tal definición será la adoptada a los efectos del presente trabajo.

Tenemos, entonces, acciones de defensa activas, pasivas, proactivas, preventivas y reactivas, para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras inteligencias en oposición, en cumplimiento de misiones o servicios propios.

Como normativa a seguir tenemos el Estándar Británico BS 7799, que se publicó en 1995 y dio origen a la serie ISO 27000. El BS 7799-2 es adoptado por la ISO, que recibió la numeración 27000 y dio inicio a la serie dirigida a la estandarización de normas para el segmento de seguridad de la información, lanzado como norma ISO/IEC 27001.

La norma ISO 27000 fue publicada en octubre de 2005 por la Organización Internacional de Estandarización y por la Comisión Electrónica Internacional. Es un conjunto de estándares internacionales sobre la seguridad de la información. La familia ISO 27000 contiene un conjunto de buenas prácticas para el establecimiento, la implementación, el mantenimiento y la mejora de sistemas de gestión de la seguridad de la información.

El International Register of Certificated Auditors (IRCA) es el mayor organismo mundial de certificación de auditores de sistemas de gestión y asimismo certifica la norma ISO 27000.

[13] Unión Internacional de Telecomunicaciones, *Resolución 181*, "Definiciones y terminología relativas a la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación" (Guadalajara, 4-22 de octubre de 2010), 5.

La ISO 27001:2013 es la norma internacional que proporciona un marco de trabajo para los sistemas de gestión de seguridad de la información (SGSI), con el fin de proporcionar confidencialidad, integridad y disponibilidad continuada de la información, así como cumplimiento legal. Es una regulación internacional que permite el aseguramiento, la confidencialidad y la integridad de los datos y de la información, así como de los sistemas que los procesan. El empleo de ISO-27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización.

La ISO 27001 es una norma de la International Organization for Standardization (ISO) que define buenas prácticas asociadas a la seguridad de la información. Su objetivo principal es defender, proteger y gestionar la información como uno de los activos más importantes de la empresa. Ayuda a establecer formas de coordinación y comunicación entre todas las secciones de una organización, a generar una cultura de seguridad y a mejorar la responsabilidad de la gestión; además, impulsa la evaluación y la mejora por medio de auditorías internas, acciones correctivas y preventivas, e instituye buenas prácticas para implementar un sistema de gestión de seguridad de la información. Hacerlo no solo conduce a proteger los datos de la organización, que son el activo más importante, sino también a incrementar la confianza entre clientes, proveedores y empleados.

De vuelta al tema de la ciberdefensa, Fonseca y otros autores nos dicen:

> Una guerra no deja de ser tal porque se libre en el ciberespacio en vez de los ambientes tradicionales de tierra, agua y contemporáneo del aire. Si consideramos al ciberespacio como un escenario más en el cual los Estados a través de sus Ejércitos participarían en guerras cibernéticas, cabe investigar si es posible aplicar el "ius ad bellum" (o el derecho que regula el recurso de la fuerza por parte de los Estados) y el "ius in bello" (derecho de la guerra o derecho internacional humanitario, que regula el comportamiento durante el uso de la fuerza en un conflicto armado) a dicho contexto, siendo este uno de los mayores desafíos para los hombres del derecho.[14]

Hay diversas posturas jurídicas al respecto. Algunos autores dicen que se necesitaría un marco legal específico, mientras que otros opinan que todas las normas del DIH

[14] Claudia Elizabeth Fonseca et al., "El Manual de Tallin y la aplicabilidad del derecho internacional de la ciberguerra", *La Revista de la Escuela Superior de Guerra*, núm. 588 (2014): 135, http://www.cefadigital.edu.ar/bitstream/1847939/993/1/Revista%20ESG%20no.588-2014_Fonseca_172.pdf (acceso diciembre 20, 2021).

que rigen la conducción de las hostilidades serían adaptables y aplicables durante un conflicto armado cibernético, ya que, en definitiva, las normas a las que nos referimos tienen por objetivo proteger a la población y los bienes civiles contra los efectos de las agresiones bélicas; por ello podemos incluir a los ataques cibernéticos.

Lo cierto es que expertos en la materia han confeccionado una especie de corpus normativo, el *Tallinn Manual on the International Law Applicable to Cyber Warfare*, denominado comúnmente *Manual de Tallin*, nombre de la capital de Estonia. Fue publicado en abril de 2013 y expone el primer ataque cibernético de un país a otro. Si bien no se trata de una publicación oficial, se creó a pedido del Centro de Excelencia en la Defensa Cooperativa Cibernética de la OTAN y es una guía para situaciones que se puedan plantear en el ciberespacio.

Entre las normas que referencia están la Declaración de San Petersburgo, de 1868, y las Convenciones de Ginebra, de 1949, y las adapta al ciberespacio. El Manual es el resultado de un trabajo de tres años de análisis de las normas internacionales que pueden emplearse para combatir los ataques de la guerra cibernética, elaborado por un grupo de expertos independientes que emiten opiniones bajo su absoluta responsabilidad, pero crea el primer cuerpo de ideas sobre la materia.

Marco Roscini, profesor de derecho internacional en la Universidad de Westminster, en Londres, dijo que el Manual es el primer intento de mostrar que las leyes de guerra, algunas de las cuales datan del siglo XIX, son lo suficientemente flexibles para aceptar las nuevas realidades de los conflictos en el espacio cibernético.

Allí se indica, por primera vez, el procedimiento a seguir por parte de los Estados y las alianzas militares, en caso de ciberataques masivos. En cierta medida, el objetivo de la publicación es evaluar si las actuales normas legales internacionales (sobre todo en derecho internacional humanitario) son útiles también en el ciberespacio. Según el Manual, los ciberataques cometidos en ausencia de acciones militares pertenecen a la categoría de las "acciones en contra de la ley", por lo que la reacción ante estos puede llevar al agresor a ámbitos penales o a tomar "contramedidas proporcionales", lo cual depende de la envergadura del ciberataque y sus consecuencias (muertes, daños o destrucción de edificios). Así, un ciberataque en tiempos de paz podría ser equivalente al "uso de la fuerza" o a un "ataque armado" y el Estado agredido tendría derecho a defenderse, entre otras cosas, con armamento tradicional.

Michael D. Schmitt, uno de los principales autores del Manual y profesor de la Escuela de Guerra Naval de Newport (Estados Unidos), indicó que el ataque de virus Stuxnet, perpetrado contra las infraestructuras críticas de Irán, en 2009, constituye en sí mismo un "acto de fuerza".

Como vemos, tanto la ciberseguridad como la ciberdefensa son temas ineludibles, tanto desde los convenios interestatales como desde la normativa de cada país, y bien sea en su fase preventiva como en la reparativa. Desconocer el tema es desconocer la realidad de los tiempos que corren.

Términos y condiciones de uso de aplicaciones móviles: importancia, cláusulas habituales y políticas de privacidad

En el presente proyecto, la regulación de uso debe materializarse con un contrato denominado Términos o condiciones de uso o del servicio, vocablos que utilizaremos de manera indistinta en esta obra. Dicho contrato es de fundamental importancia para determinar el alcance de los derechos y las obligaciones de las partes involucradas en la relación jurídica que se crea entre quien otorga y quien recibe su licencia de uso.

Por lo general, en este tipo de acuerdos se incluyen cláusulas de propiedad intelectual, de uso del contenido provisto por el proveedor del APP, de seguridad informática, de resolución de conflictos, de limitación de responsabilidad del proveedor, de competencia y legislación aplicable, entre otras que analizaremos a continuación. Se destacan también, como párrafo aparte y especial, aquellas cláusulas de privacidad y uso de datos personales llamadas políticas de privacidad, que pueden estar incluidas o separadas de los términos y condiciones.

Términos y condiciones. Importancia desde la óptica contractual

En el último tiempo, la contratación electrónica mediante aplicaciones móviles parece ser la forma elegida por los usuarios de tecnologías de información y comunicación (TIC) para adquirir bienes y servicios.[15] Si bien esta tendencia resulta obvia para el

[15] Sobre el tema puede verse John Grover Dorado, "Los contratos electrónicos de consumo en el derecho argentino", *SAIJ*, 26 de octubre de 2016. https://acortar.link/Awxbap (acceso diciembre 10, 2021); "Nuevos modelos de negocios en Internet: regulación jurídica de servicios prestados a través de aplicaciones móviles. El caso 'Uber", *SAIJ*, 23 de mayo de 2018, https://acortar.link/Awxbap (acceso diciembre 10, 2021).

comercio electrónico tradicional —nos referimos a las transacciones B2C o C2C, que suele tener por objeto la adquisición de productos digitales o tangibles, sea de manera directa entre los actores involucrados o por medio de un *marketplace*—, aquella ha logrado expandirse a otros ámbitos como los servicios, sean prestados por particulares (v. gr. transporte urbano o alojamiento turístico) o por los propios Estados (v. gr. cuando la Administración utiliza APPS en la prestación de servicios públicos como salud, educación o seguridad, o como medio para pago de impuestos, solicitudes o trámites, etc.).

En este marco, en el que la contratación electrónica mediante APPS parece ser la nueva regla, el derecho, en particular el de los contratos, se ha visto obligado a reconsiderar viejos dogmas e instituciones ante los cambios impuestos por los avances tecnológicos y su adopción por los usuarios. Muchos cambios han sido actualizados gracias a la esencia dinámica del derecho comercial, comprensivo de un joven y receptivo derecho del consumo, que fue previendo nuevos fenómenos ante la contratación en masa, y un emergente y transversal derecho informático, que fue allanando el camino al conocimiento de los problemas jurídicos planteados por la tecnología informática, desde los primeros *softwares* e intercambios de pequeñas cantidades de datos mediante un rudimentario Internet. No obstante, en una actualidad de intrincados conceptos como macrodatos, IA, Internet de las cosas, cadena de bloques, criptomonedas, etc., que sobrevuelan una sociedad y una economía globales, digitales, del conocimiento preciso, el derecho, cuyo fin es regular conductas humanas con leyes generales, se ha visto aturdido, rezagado y en permanente reflexión acerca de su rol frente a las nuevas tecnologías. Esto es así porque, en gran parte, el mercado de la innovación le exige respuestas inmediatas, so pena de hacerle responsable de no contribuir al progreso humano.

Es allí, en ese espacio de reducida libertad, donde el derecho debe elegir qué hacer con la tecnología, es decir, dar espacio a la autorregulación o regularla de un modo más o menos estricto. Cualquiera que sea el camino que cada Estado elija, está claro que, más allá de una disposición dirigida de modo general (v. gr. legislación o regulaciones administrativas), lo que importará, al final de cuentas, serán las disposiciones contractuales.

En otras palabras, observamos que el derecho de los contratos —modernizado con las nociones propias del derecho del consumo y del informático— adquirió especial importancia a la hora de regular las relaciones emergentes del uso de las aplicaciones móviles. Será la convención entre las partes —plasmada en las condiciones o los

términos de uso— la principal fuente de derecho confiable a la que los individuos querrán acudir para que rija sus conductas y determine responsables, en caso de incumplimiento.

Cláusulas habituales

Entre las cláusulas más utilizadas en los términos y las condiciones de uso de los APPS encontramos las siguientes, a saber:

- Contenidos de propiedad intelectual: una de las cláusulas más importantes es aquella que otorga al proveedor del APP los derechos sobre todo material o contenido que aporta el usuario, pues queda aquel con derecho a administrar y disponer de derechos de propiedad intelectual. Debemos recordar que los contenidos aportados y cedidos por los usuarios que sean protegidos por la vía del derecho de autor, muchas veces consistirán en comentarios, fotografías y videos que guardan relación con la intimidad de la persona. De esta forma, no solo se comprometen derechos de autor, sino también el derecho de imagen, que corresponde reivindicar a quienes hayan sido retratados, o el derecho de autodeterminación informativa sobre datos personales, en caso de que el material permita la vinculación con la identidad de una persona en particular.

La mayor discusión respecto a estas cláusulas surge de la falta de claridad en los textos de las condiciones de contratación, ya que, en muchas ocasiones, el alcance de la mentada licencia puede ser excesivo.

Aunque muchos de los APPS contienen en sus términos cláusulas orientadas hacia un recto tratamiento de datos personales y un reconocimiento de los derechos de autor en cabeza de los usuarios, en la realidad de la dinámica contractual ocurre algo muy distinto. En el fondo, la cláusula de licencia de propiedad intelectual —que suele afirmar que el usuario es el propietario de todo el contenido y la información que se publica en la red social— funciona como una autorización para que el APP pueda disponer de dicho material, aun cuando el usuario da de baja su perfil, de modo que termina siendo lisa y llanamente una cesión gratuita y exclusiva de propiedad intelectual que, además, suele permitir utilizar los contenidos cedidos con fines publicitarios u otros fines no previstos en las condiciones de uso.

- Seguridad informática: también es habitual que los APPS, sobre todo aquellos que alojan contenidos de terceros, quieran garantizar a sus usuarios un estándar mínimo de seguridad informática. En tal sentido prevén prohibiciones —muchas de

ellas vinculadas a la privacidad—como la de publicar comunicaciones no deseadas (spam), recopilar información o contenidos de otros usuarios (data mining), utilizar medios automáticos para ingresar al sitio web (bots), subir virus o códigos malicioso (spyware, malware, badware, rootkits, gusanos, troyanos, etc.), cometer ataques de denegación de servicio (DoS), alterar la presentación de páginas u otra funcionalidad de la plataforma de la red social (phishing), entre otras.

- Normas de conducta: otro punto que merece regulación lo constituye el conjunto de estándares de conductas esperables del usuario. Entre las estipulaciones que suelen incluir los APPS se cuentan prohibiciones de afectar legítimos derechos de terceros, por ejemplo, crear cuentas falsas o inexactas, suplantar identidades, afectar la seguridad informática de las cuentas propias, de terceros o de cualquier otro *software*, *hardware*, sistema, servidor, redes, equipo de telecomunicaciones, o cualquier sistema, datos, contraseña u otra información de la cual el proveedor del aplicativo es propietario. Para el caso de que el aplicativo permita alojar contenido de usuarios, se acostumbra prever la prohibición de publicar contenidos ofensivos, pornográficos, que inciten a la violencia o que contengan desnudos o violencia gráfica o injustificada, que causen molestia, hostigamiento, intimidación o acoso a otros usuarios, que impliquen injurias o fraudes o, en fin, que resulten actos engañosos, malintencionados, discriminatorios y, en general, contrarios a toda disposición legal que garantice el honor, la imagen y la intimidad, el secreto en las comunicaciones, los derechos de propiedad industrial e intelectual o toda norma de protección de datos personales.

- Violación de derechos de terceros: los términos de uso de APPS suelen poner a disposición de los usuarios sistemas de denuncia ante cualquier eventual infracción a la propiedad intelectual o a las normas de conducta ya referidas. Este mecanismo permite notificar al proveedor del aplicativo acerca de cualquier contenido inadecuado, ilícito o contrario a las condiciones del servicio, con el objeto de bloquear o dar de baja el perfil infractor.

Estos sistemas se utilizan con frecuencia en el resto de los sitios web que alojan contenidos que pueden afectar principalmente derechos de propiedad intelectual (v. gr. sitios de compraventa o subastas en línea e ISP de alojamiento o hostings) y se conocen como "notice and take down", en alusión al bloqueo inmediato que debe efectuar el ISP luego de que fuera puesto en conocimiento de su existencia, so pena de ser responsables legalmente.

- Resolución de conflictos: en caso de conflictos judiciales entre usuarios y proveedores de APPS, los términos de uso suelen comprender disposiciones que limitan las responsabilidades de estos últimos, otras que fijan la legislación y la competencia en el lugar donde el proveedor tiene su sede principal, como también cláusulas compromisorias que prevén la opción del arbitraje como método alternativo de resolución de disputas. Muchas de estas cláusulas son abusivas para el usuario, desde el punto de vista del derecho del consumidor.

- Otras cláusulas: por último encontramos normas específicas dirigidas a anunciantes que desean hacer publicidad en el aplicativo o a intermediarios de pagos para los servicios que no son gratuitos, así como aquellas referidas a la rescisión, la integridad y los cambios en las condiciones de uso, etc.

Es menester destacar que la regulación contractual no solo debe procurar atender en forma precisa y estricta los derechos y las obligaciones mencionados, sino que, además de las cláusulas previstas en el contrato, debe prestar especial cuidado a la forma y la prueba de los contratos, así como al cumplimiento de leyes de orden público en las jurisdicciones nacionales, como leyes de defensa de los consumidores y de protección de datos personales, entre otras.

Políticas de privacidad

Existe una enorme capacidad de procesamiento de un gran volumen de datos en tiempo real, de los cuales una cantidad significativa se encuentra disponible pública y globalmente.[16]

Ahora bien, la forma de proteger esa cantidad masiva de datos elegida por los proveedores de APPS —y por todo proveedor de servicios de Internet que esté obligado según las leyes de protección de datos— consiste en proveer a los usuarios de las herramientas para establecer distintos niveles de privacidad de acuerdo con sus preferencias (privacidad desde el diseño), aunque deben, por defecto, mantener

[16] Según el supervisor europeo de Protección de Datos, el big data "se refiere al análisis de grandes volúmenes de fuentes diversas de información que utiliza sofisticados algoritmos para fundamentar decisiones. El big data se basa no sólo en la creciente capacidad tecnológica para recolectar y almacenar grandes cantidades de datos, sino también en sus capacidades para analizar, comprender y aprovechar plenamente el valor de los datos". Supervisor Europeo de Protección de Datos [SEPD], *Opinion 7/2015. Meeting the Challenges of Big Data; A Call for Transparency, User Control, Data Protection by Design and Accountability* (Bruselas, 19 de noviembre de 2015), 7.

los datos personales en un grado de privacidad tal que no sean accesibles a un número indefinido de personas (privacidad por defecto).[17]

En este contexto de cierta libertad contractual emergen las llamadas Políticas de privacidad, que son cláusulas que prevén las condiciones de protección de los datos personales de los usuarios en distintos APPS. Si bien se encuentran en documentos separados, a los cuales remiten las condiciones generales de uso, en realidad, se trata de cláusulas principales que integran el contrato de servicio y que resultan esenciales a los fines de informar al usuario —con anterioridad a formar parte de la red social— acerca de la existencia de un procesamiento de sus datos personales, quién es el responsable del mismo, cuál va a ser su finalidad, si serán cedidos y a quién, cómo va a ser el proceso de recolección, tratamiento, almacenamiento, revelación y otros usos de la información, y cuáles son sus derechos, es decir, cómo se accede a los datos que se tengan sobre él, y cómo se modifican, eliminan o someten a confidencialidad, en caso de ser erróneos.[18]

Las políticas de privacidad normalmente incluyen disposiciones referidas a:

- Recolección y uso de datos: los proveedores de APPS recolectan distintos tipos de informaciones, que incluyen todas aquellas que el propio usuario voluntariamente provee a la plataforma con motivo del registro y toda la que se recolecta automáticamente o por medio de terceros proveedores de diversos servicios que interactúan con la plataforma, como los proveedores de servicios de pagos, proveedores de aplicaciones y sitios web que integran botones, cuadros y demás widgets o plug-ins desde los cuales los usuarios se registran para autenticación o identificación, o simplemente para acceder a contenidos del aplicativo.

Encontramos datos que otros usuarios comparten sobre una persona (v. gr. comentarios, etiquetas sobre fotografías, videos, ubicaciones); del uso del aplicativo; del dispositivo (v. gr. del teléfono móvil, identificadores de *hardware*, sistema operativo, etc.); de la red (v. gr. proveedor de servicios de Internet, ubicación, dirección IP, identificadores de red, etc.); metadatos (v. gr. fecha, hora y lugar de los archivos que aporta el usuario, si aplica), entre otros.

[17] Comisión Europea, "¿Qué significa la protección de datos 'desde el diseño' y 'por defecto'?", https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_es (acceso diciembre 6, 2021).

[18] Sobre el tema puede verse John Grover Dorado, "Derecho a la intimidad y protección de datos personales en las condiciones de uso y políticas de privacidad de las redes sociales", *SAIJ*, 30 de mayo de 2016, https://acortar.link/X6fb4U (acceso diciembre 10, 2021).

Muchos de estos, en tanto permitan ser vinculados a la identidad de una persona, constituyen informaciones personales protegidas por las leyes de protección de datos y por tal motivo deben ser sometidos a estándares de protección más altos que cualquier otra.

- Responsable del tratamiento de datos personales: no hay duda alguna de que la actividad que desarrollan los proveedores de aplicaciones puede encuadrarse en el concepto previsto por las leyes de protección de datos personales referido al tratamiento de datos personales y que, en consecuencia, ellos resultan responsables por esta. Por eso, en toda política de privacidad se especifica la identificación del responsable del tratamiento de los datos personales de los usuarios, como el nombre o la razón social, el domicilio y demás fuentes de contacto (dirección postal o electrónica) de la casa matriz o filial que hará el procesamiento según la ubicación del usuario.

- Derechos del titular de datos personales: es de rigor incluir en el contrato disposiciones protectoras de los datos personales del usuario, entre las que se destacan los derechos a acceder a los datos que se tenga sobre él, a modificarlos, eliminarlos y someterlos a confidencialidad.

A los fines de hacer efectivos estos derechos, la tendencia adoptada por los proveedores de APPS es otorgar a sus usuarios la posibilidad de configurar el grado de privacidad que desean; pueden elegir qué será compartido con el aplicativo; con quiénes se comparte; si se requiere una autorización para compartir determinados datos o contenidos propios o de terceros, etc. Estas circunstancias suelen informarse en un momento anterior a la descarga del aplicativo.

-Transferencia de datos: el referido tratamiento de datos personales puede realizarlo directamente el responsable del aplicativo o indirectamente por medio de una cesión a terceros. En este último caso, el proveedor principal se reserva la facultad de compartir los datos personales con terceros proveedores de servicios, conforme a las obligaciones de confidencialidad compatibles con sus políticas de protección de datos y a condición de que los terceros utilicen sus datos personales únicamente conforme a sus instrucciones y a los fines informados.

- Cambios en la estructura organizacional: en toda política de privacidad se dispone que, en caso de que el proveedor del aplicativo sufra alguna eventualidad en su estructura societaria (concurso, quiebra, fusión, adquisición, reorganización, venta

de activos, etc.), los datos de los usuarios también podrán ser vendidos o transferidos a terceros participantes de dichos cambios.

- Conservación y divulgación de datos: los proveedores de APPS, en su afán de intentar cumplir con las legislaciones locales, comunican al usuario que existe la posibilidad de que todos sus datos, incluidos los personales, puedan ser conservados o revelados si se considera que es necesario para cumplir con una ley, un reglamento o un requerimiento legal o judicial, para hacer efectivas las condiciones de uso y otros acuerdos que sean partes de aquellas, o para proteger sus derechos, su propiedad o seguridad, así como la de sus empleados, usuarios u otros terceros.

- Cookies y tecnologías similares: todos los APPS se valen de la utilización de pequeños archivos llamados cookies o tecnologías similares de almacenamiento, que se guardan en el dispositivo del usuario a instancias del navegador web y que tienen por objeto mejorar la experiencia de navegación del usuario, al facilitar al sitio web sus datos de identificación y de preferencia.

La información recolectada por estos medios, no obstante, también permite crear perfiles de usuarios, con datos sobre su comportamiento en línea, sus preferencias en la web, la cantidad de tiempo que se dedica a cada elección, y avisos y publicidades visitados, entre otros.

En el contexto de los APPS, las políticas de privacidad estipulan que las cookies y tecnologías similares sirven para: a) autenticación; b) recordar preferencias de usuarios; c) detección de spam, abuso y otras actividades violatorias de las reglas de conducta; d) análisis e investigación de datos; e) mostrar al usuario contenido personalizado, y f) elaboración de avisos publicitarios precisos, etc.

- Eliminación de datos: una cláusula harto habitual es aquella que dispone que, incluso después de eliminar la cuenta o el perfil del usuario, pueden permanecer copias de esa información visibles en otros lugares, en la medida en que haya sido compartida con otras personas, haya sido distribuida de alguna manera conforme a la configuración de privacidad del usuario o haya sido copiada o almacenada por otros usuarios. Asimismo, se prevé que toda información eliminada o borrada puede permanecer en copia de seguridad por un plazo razonable antes de ser eliminada de los servidores de los proveedores de APPS.

Conclusiones

Referente a la transparencia y los datos abiertos, podemos establecer que la aplicación es un ejemplo de reutilización de datos públicos que no poseen restricciones por reserva o clasificación en los términos que establece la ley, por lo que se permite su uso y reutilización por parte de la ciudadanía como fin de la propia ley. Así mismo, el resultado de su reutilización concede a las entidades desarrolladoras, si lo desean, un usufructo de los datos resultantes que llevaría a cerrar el círculo que pretende la ley, al crear nuevos datos.

La protección de los datos es un imperativo. Las nuevas tecnologías de información y el uso de IA posibilitan obtener grandes volúmenes de datos que es preciso proteger almacenándolos y transmitiéndolos de modo seguro, mediante sistemas de encriptación. Con esto se busca su efectivo resguardo, para evitar riesgos y daños.

La ciberseguridad y la ciberdefensa son temas ineludibles, tanto desde los convenios interestatales como desde la normativa interna de cada país y ya sea en su fase preventiva como en la reparativa. Desde allí deben ser asuntos a tener en cuenta al abordar cualquier tipo de desarrollo como el que nos ocupa. Por supuesto, en su etapa de implementación, Navega Seguro debe tener internalizados estos conceptos y ser lo menos vulnerable a ataques externos, que es lo buscado.

En cuanto a los términos y las condiciones de uso de aplicaciones móviles, luego de haber destacado la importancia y enumerado brevemente las cláusulas habituales en los términos de uso, incluidas las que se encuentran también en las políticas de privacidad, debe concluirse que, más allá del paradigma actual utilizado por los proveedores de los servicios de aplicaciones móviles basado en una protección de la privacidad desde el diseño y por defecto, el cual es un excelente punto de partida, debe complementarse con previsiones contractuales robustas que respeten los estándares legales previstos en normas de vanguardia en materia de privacidad y defensa del consumidor, tales como el Reglamento europeo de protección de datos y la directiva de los consumidores. Aunque en los países de América Latina no existen normas comunitarias como las señaladas, entendemos que la mejor forma de establecer un equilibrio contractual, por el que los derechos vinculados con la privacidad y la protección de datos personales sean adecuadamente respetados en las condiciones de uso y en las políticas de privacidad, es la inclusión de estándares irrenunciables de orden público como los previstos en la legislación europea, la cual

proponemos como modelo para los documentos legales que rigen en el aplicativo Navega Seguro.

En nuestro mundo actual, la existencia de *software* que facilite desempeñar distintas actividades es una necesidad esencial, notoria con más fuerza luego de la pandemia del covid-19, por la cual gran parte de las actividades fueron virtualizadas y el teletrabajo, una realidad imperante que llegó para quedarse. En este contexto, es menester proteger nuestros datos personales de programas que puedan resultar intrusivos o que infieran posibles datos privados mediante cruzamiento o data mining. En el caso de la aplicación que aquí analizamos, Navega Seguro, solo se apunta a conocer datos públicos de los usuarios y, en muy pequeña cantidad, algún dato privado, como su correo electrónico, con la finalidad de brindarles información y novedades para el mejor desarrollo de sus actividades náuticas en aguas de la bahía de Cartagena.

Referencias

Becerra, Jairo, Lorenzo Cotino Hueso, Claudia Bibiana García Vargas, Marco Emilio Sánchez y Jheison Torres Ávila. *La responsabilidad del Estado por la utilización de las tecnologías de la información y la comunicación (TIC)*. Bogotá: Editorial Universidad Católica de Colombia, 2015.

Chacón Gómez, Nayibe. "Las tecnologías disruptivas: los retos a la protección de datos" en *Memórias do XXIII Congreso Ibero-americano de Direito e Informática 2019*, organizado por Fiadi y Luiz Fernando Martins Castro, 445-455. Timburi: Cia do eBook, 2019.

Colombia, Congreso de la República. *Ley 1712 de 2014*, "Por medio de la cual se crea la Ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones". Bogotá: *Diario Oficial* núm. 49 084, 6 de marzo de 2014.

Comisión Europea. "¿Qué significa la protección de datos 'desde el diseño' y 'por defecto'?". https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_es (acceso diciembre 6, 2021).

Comisión Europea. *Libro blanco sobre la inteligencia artificial. Un enfoque europeo orientado a la excelencia y la confianza. COM(2020) 65 final*. Bruselas, 19 de febrero de 2020.

Dorado, John Grover. "Derecho a la intimidad y protección de datos personales en las condiciones de uso y políticas de privacidad de las redes sociales". *SAIJ*, 30 de mayo de 2016. https://acortar.link/X6fb4U (acceso diciembre 10, 2021).

Dorado, John Grover. "Los contratos electrónicos de consumo en el derecho argentino". *SAIJ*, 26 de octubre de 2016. https://acortar.link/Awxbap (acceso diciembre 10, 2021).

Dorado, John Grover. "Nuevos modelos de negocios en Internet: regulación jurídica de servicios prestados a través de aplicaciones móviles. El caso 'Uber". *SAIJ*, 23 de mayo de 2018. https://acortar.link/Awxbap (acceso diciembre 10, 2021).

Estévez Mendoza, Lucana María. "Regulación de la inteligencia artificial y la protección de los derechos fundamentales en la cuarta revolución industrial" en *Memórias do XXIII Congreso Ibero-americano de Direito e Informática 2019*, organizado por Fiadi y Luiz Fernando Martins Castro, 266-278. Timburi: Cia do eBook, 2019.

Fonseca, Claudia Elizabeth, Ivonne Luz Perdomo, Miguel Arozarena Gratacos y Javier Ulises Ortiz. "El Manual de Tallin y la aplicabilidad del derecho internacional de la ciberguerra". *La Revista de la Escuela Superior de Guerra*, núm. 588 (2014): 127-144. http://www.cefadigital.edu.ar/bitstream/1847939/993/1/Revista%20ESG%20no.588-2014_Fonseca_172.pdf (acceso diciembre 20, 2021).

Hernández, Jeice. "El reto de la cuarta revolución industrial en Colombia: datos, diseño y artes" en *Colombia 4.0: retos y perspectivas sobre el desarrollo de la cuarta revolución industrial*, editado por Eduardo Andrés Perafán del Campo, Catalina Miranda Aguirre y Sebastián Polo Alvis, 153-175. Bogotá: Tirant lo Blanch, 2020.

Ortega Ruiz, Luis Germán y Jairo Becerra. "La inteligencia artificial en la decisión jurídica y política". *Araucaria, Revista Iberoamericana de Filosofía, Política, Humanidades y Relaciones Internacionales*, núm. 49 (2022): 217-238. https://dx.doi.org/10.12795/araucaria.2022.i49.10

Pérez, Paula, Becerra, Jairo y Julián Rodríguez. "The Colombian Freedom of Information Act Using Media Literacy to Understand and Implement the Law" en *Media Literacy in a Disruptive Media Environment*, editado por William G. Christ y Belinha S. de Abreu, 217-238. Nueva York: Routledge, 2020.

Rodríguez, Julián y Andrew M. Clark. "Big data y periodismo: cómo el periodismo estadounidense está adoptando el uso de big data". *Novum Jus 15*, núm. 1 (2021): 69-89. https://doi.org/10.14718/NovumJus.2021.15.1.4

Silva García, Germán. "¿El derecho es puro cuento? Análisis crítico de la sociología jurídica integral". *Novum Jus 16*, núm. 2 (2022): 49-75. https://doi.org/10.14718/NovumJus.2022.16.2.3

Supervisor Europeo de Protección de Datos [SEPD]. *Opinion 7/2015. Meeting the Challenges of Big Data; A Call for Transparency, User Control, Data Protection by Design and Accountability*. Bruselas, 19 de noviembre de 2015.

Unión Internacional de Telecomunicaciones. *Resolución 181*, "Definiciones y terminología relativas a la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación". Guadalajara, 4-22 de octubre de 2010.