Big Data Research in Social Media.Legal, Ethical and Social Responsibility Challenges.

Riva Fabiana María, Abbatemarco Martín, Cervino Alejo

Departamento Ingeniería en Sistemas de Información
Facultad Regional Rosario, Universidad Tecnológica Nacional
E. Zeballos 1341, (2000) Rosario, Santa Fe, Argentina
fabianamriva@gmail.com, abbatemarco.martin@gmail.com, alejocervino@hotmail.com

Resumen The present paper is intended to approach the legal, ethical and social responsibility challenges encountered by Information Systems and Technologies professionals in their daily practice. Following the studies in Science, Technology and Society, while basing the analysis on the paradigm of complexity, the problem of the indiscriminated treatment of virtual social networks data is used as a trigger, where the systematic revision of laws, norms and related doctrine emerges as relevant to the subject; among others, the argentinian Law 25.326 on the Protection of Personal Data and related decrees. Acknowledging the inadequacy of the current normative set that arises from the constantly increasing complexity of technological developments, progress is made on the analysis of an ethical and social responsibility perspective, which leads to reflect on the competences that future graduates should acquire as part of their integral formation.
Keywords: Technology - Informatics - Ethics - Social Responsibility - Complexity

1. Introducción

Intelectuales, juristas, investigadores y profesionales de las más diversas áreas alrededor del mundo se encuentran hoy perplejos y con pocas herramientas con las que defenderse ante la rapidez con que los avances tecnológicos se instalan en una sociedad cada vez más permeable a ellos. A pesar de los beneficios logrados, la evaluación minuciosa de los riesgos nos permite advertir la ambivalencia de estos progresos; desde automóviles autónomos que provocan accidentes, pasando por drones y cámaras de vigilancia que invaden la privacidad de las personas, la construcción de bases de datos con historias clínicas cuyos datos sensibles son utilizados para estudios no previstos inicialmente, como así también el tratamiento masivo de datos en redes sociales virtuales sin consentimiento previo informado.

En todos estos ejemplos se podría identificar el trabajo interdisciplinario requerido, que aporta conocimientos científicos, tecnológicos y metodológicos apropiados a la solución buscada. Sin embargo, la complejidad del impacto social, cultural y ambiental que traen aparejado estos y otros progresos hace que

deban ser abordados con una actitud hacia el conocimiento transdisciplinario, que reconozca la multidimensionalidad de la realidad y que tome en cuenta el flujo de información circulando entre varias ramas de conocimiento, fomentando su integración [1].

En este contexto, el desarrollo profesional se torna cada día más complejo, no sólo en lo que respecta a la formación en competencias específicas, sino en relación a las genéricas, como lo son el respeto por las leyes, el compromiso ético y la responsabilidad social, cuyas bases se ven, a su vez, sometidas a reconsideración fruto de los mismos cambios tecnológicos.

Esta breve introducción pretende poner en contexto el trabajo que desarrollamos, que por un lado analiza los retos legales, éticos y de responsabilidad social a los que se expone el profesional de sistemas y tecnologías de la información durante el tratamiento masivo de datos en redes sociales virtuales, mientras que por el otro reflexiona, a partir de esta experiencia, sobre la formación en competencias que debe adquirir el futuro egresado como parte de su formación integral.

2. Marco Contextual y Metodológico

2.1. Contexto del Trabajo

Este trabajo se origina como parte de las actividades desarrolladas en el marco del Proyecto de Investigación y Desarrollo: Observatorio Regional de Desarrollo de la Ingeniería en Sistemas de Información e Informática (IISI.d.r.O.) [2] de la Universidad Tecnológica Nacional (UTN) Facultad Regional Rosario (FRRo), cuyo objetivo principal es *"el diseño, construcción e implementación de una plataforma tecnológica integrada y abierta que recopile, analice y administre información sustantiva en torno al desarrollo y evolución de las Tecnologías de Información y Comunicaciones, Software y Servicios Informáticos (TIC-SSI) y su aporte a las cadenas productivas transversales, para atender a las necesidades de los diferentes sectores que conforman el Triángulo de Sábato (Universidad-Estado-Industria)"*.

El equipo que conforma IISI.d.r.O. adhiere a la linea de los estudios sobre Ciencia, Tecnología y Sociedad (CTS) con una mirada desde el paradigma de la complejidad.

Afrontando el problema a partir de los principios del pensamiento complejo e intentando poner en práctica el *diálogo* necesario entre las múltiples áreas de conocimiento y actores que se entrelazan en el desarrollo de la Ingeniería en Sistemas de Información e Informática, el equipo encontró en el constructo competencias un puente que permite *pensar en red* [1], aspecto privilegiado en la transdisciplinariedad.

Emerge entonces, como una de las estrategias, el planteo de una red configurada para el análisis comparado de competencias en la trama productiva de Software y Servicios Informáticos [3] y la necesidad de proveerla de datos a partir de diversas fuentes, entre ellas, los datos provenientes de redes sociales

virtuales; y uno de los subproductos de la recolección de datos que es la posibilidad de generar un mapa interactivo de los alumnos y graduados de la carrera que desempeñan su actividad en la profesión. Indicadores y datos que estarán disponibles a la comunidad que desee consultarlos.

La recolección de datos a la que se hace referencia en este trabajo refiere particularmente a los conocimientos, competencias y habilidades que les son requeridos por las empresas a los profesionales en sistemas y tecnologías de la información y que pueden recabarse de los requerimientos que las empresas vuelcan en las solicitudes laborales, como así también a la formación y experiencia que estudiantes y graduados de la carrera aportan en sus perfiles en linea en redes sociales virtuales como LinkedIn y Facebook.

A su vez, en IISI.d.r.O. se pone en juego el principio de *recursividad*, es decir, la utilización del conocimiento adquirido sobre la formación en competencias para nutrirse de ellas y aplicarlas para el logro de las metas. Estas últimas requieren de la solución de problemas en donde se analiza el ejercicio de habilidades, que no sólo son técnicas, competencias específicas, mas también genéricas.

Siguiendo esta línea de acción, se avanzó con el análisis de competencias referidas al trabajo en equipo analizando y poniendo en práctica metodologías para el desarrollo de los productos requeridos por IISI.d.r.O [4] y al estudio sobre la posibilidad de proveer de datos a la anteriormente mencionada red a partir del tratamiento masivo de datos [5].

2.2. Metodología de Trabajo

Como se expresó en el apartado anterior, adherimos a la linea de Estudios CTS que, para explicar brevemente, *"busca comprender la dimensión social de la ciencia y la tecnología, tanto desde el punto de vista de sus antecedentes sociales como de sus consecuencias sociales y ambientales; es decir, tanto por lo que atañe a los factores de naturaleza social, política o económica que modulan el cambio científico-tecnológico, como por lo que concierne a las repercusiones éticas, ambientales o culturales de ese cambio"* [6].

Por otra parte, utilizando como sustento epistemológico de construcción del conocimiento el paradigma de la complejidad, diremos que aquel que se pretende alcanzar es un conocimiento contextualizado, caracterizado por el rechazo a los efectos reduccionistas y unidimensionales que puede producir la *"hipersimplificación que ciega la complejidad de lo real"* y aspirando a un conocimiento multidimensional, aunque sin perder de vista lo inacabado e incompleto de todo conocimiento [7].

Morin explicita tres principios ligados entre sí que permiten pensar la complejidad: el principio dialógico, el principio de recursividad organizacional y el principio hologramático. Para comprenderlos haremos referencia a cuestiones presentes en el trabajo.

El principio dialógico lo veremos plasmado en el diálogo entre las diferentes concepciones en cuanto al tratamiento masivo de datos en redes sociales. En primer lugar, encontramos la lógica de las corporaciones que detentan el poder de uso en función de la posesión de los datos. Luego, la lógica del usuario de

las redes quien por un lado entrega sus datos privados a estas corporaciones para un fin específico y que más tarde puede verlos utilizados para fines que él suponía no previstos. Por último, la lógica seguida dentro de IISI.d.r.O., la cual pretende hacer uso de estos datos para lograr las metas del proyecto. Lógicas aparentemente antagonistas entre sí, aunque indisociables para comprender la realidad.

En cuanto al principio de recursividad organizacional, para cuya comprensión Morin utiliza el proceso del remolino en el cual cada momento del remolino es producido y, a la vez, productor, podremos encontrarlo en el desarrollo de leyes, normas y marcos éticos motivados por el progreso tecnológico y que se nutren del mismo progreso para ser reformulados. En todos los casos se observa que es en el contexto dónde se desarrollan los procesos, para luego producirse una serie de intercambios cuyos resultados pasan nuevamente a formar parte del contexto. Se produce un ciclo que rompe con la idea de la linealidad y de la relación causa-efecto.

El principio hologramático, ligado al principio recursivo, y asociado a su vez al principio dialógico, es el que nos permite enriquecer al conocimiento de las partes por el todo y del todo por las partes en un mismo proceso. Así, la praxis-reflexiva que realizaremos podrá ser aplicada como estrategia para el análisis y reflexión de cuestiones más amplias que trascienden al tratamiento masivo de datos en redes sociales, sirviendo como base para el establecimiento de las concepciones que giran alrededor de la formación en competencias legales, éticas y de responsabilidad social del profesional en Sistemas y Tecnologías de Información.

Finalmente, con el objetivo de referirnos específicamente al aspecto metodológico del presente estudio, se considera que el método de investigación derivado de las premisas anteriores nace del juego dialógico entre orden, desorden y organización a medida que avanza la investigación. En función de esto es que preferimos hablar de estrategias que permiten *afrontar los riesgos, lo inesperado, lo incierto, y modificar su desarrollo en virtud de las informaciones adquiridas en el camino. Es necesario aprender a navegar en un océano de incertidumbres a través de archipiélagos de certeza* [8]. Las estrategias aplicadas han sido el uso de un disparador para la praxis: el tratamiento masivo de datos en redes sociales virtuales, la revisión sistemática de información y el grupo de discusión hacia el interior de IISI.d.r.O. Este último, conformado por investigadores, docentes, alumnos y egresados de la carrera de Ingeniería en Sistemas de Información, fue el medio para el planteo de interrogantes y el hallazgo de patrones y actitudes prevalentes, que dan paso luego a la búsqueda de información como sustento de la práctica.

Partiendo de los interrogantes predominantes a lo largo de la investigación, que pondrán de manifiesto el desconocimiento que pueden manifestar especialistas en Sistemas y Tecnologías de la Información frente a los retos legales, éticos y de responsabilidad social que supone su práctica diaria, se desarrollan las secciones del trabajo en las que se analizan las problemáticas emanadas del tratamiento masivo de datos en redes sociales virtuales.

3. Los retos del Tratamiento Masivo de Datos en Redes Sociales Virtuales

El tratamiento masivo de datos almacenados en Redes Sociales Virtuales y en otras plataformas de Internet está asociado a lo que se conoce hoy como Big Data. Indudablemente trae consigo diversos retos técnicos, que han sido resumidos en populares cuatro 'V': volumen, velocidad, variedad y veracidad.

Si bien el *volumen* de datos puede generar un excesivo costo en muchos casos, hay que destacar el advenimiento de nuevas tecnologías de libre acceso para el procesamiento distribuido y en paralelo de grandes volúmenes de datos (Hadoop, Apache Spark, etc.), como así también las enormes posibilidades que brindan las plataformas de infraestructura para procesamiento en la nube (Google Cloud, Amazon Web Services o Microsoft Azure).

Afrontar el problema técnico de la gran *variedad* de datos a procesar, dadas las diversas fuentes, formatos, codificaciones, fuentes de errores, etc., no es tarea fácil. A tal punto que una gran proporción del tiempo en un proyecto de estas características se orienta sólo a la extracción, transformación y normalización de los datos. Luego pasan a aplicarse técnicas ya consolidadas de minería de datos, aprendizaje automático, redes neuronales, y todas sus diversas vertientes, según las características del problema y los objetivos a alcanzar.

Como si los desafíos que imponen el volumen y la variedad de los datos no fueran suficientes, otra variable entra en juego: la *velocidad*. Dada la rapidez con que se producen y multiplican los datos en Internet, muchas veces resulta imposible o muy poco práctico, bien por su gran volumen o por la velocidad con que se desvalorizan, almacenarlos para su posterior análisis. Ejemplos de estas situaciones se dan en flujos de datos de redes sociales como Twitter, como así también en el ámbito de los negocios y las finanzas, al analizar datos de transacciones comerciales y activos en bolsas de valores, por mencionar algunas. Es aquí donde entran en juego tecnologías para el manejo de streaming de datos y análisis de datos en tiempo real (Spark, Flink o Storm, todos proyectos de Apache y de libre acceso).

Finalmente, resta hablar de la *veracidad*. Nadie puede estar completamente seguro de que los datos recolectados sean fidedignos, imparciales y actualizados. El acceso masificado a Internet ha hecho que cualquier individuo, más allá de su intencionalidad, pueda subir datos falsos, parciales o poco certeros a una plataforma; fenómeno que se profundiza con los perfiles fraudulentos en redes sociales virtuales y con la escasez de tecnologías que apoyen a los investigadores.

De las problemáticas mencionadas hasta aquí, consideramos a la *veracidad* como la característica de Big Data que más riesgos supone para alcanzar las metas que nos proponemos.

Ahora bien, ¿existen otros riesgos asociados al tratamiento masivo de datos? ¿Forma parte del análisis de factibilidad considerar otros aspectos que vayan más allá de los técnicos y económicos?.

Considerando que las redes sociales virtuales han abierto inmensas puertas a investigadores, empresas y profesionales alrededor del mundo para la recolección casi indiscriminada de datos personales de los usuarios y que su tratamiento

se ha transformado en una de las formas más rentables de aprovechamiento del valor intelectual.[13], nos proponemos considerar el problema de la legalidad del acceso a dichos datos.

Tanto Facebook como LinkedIn, por dar ejemplos, cuentan con puntos de acceso, con mayores o menores restricciones técnicas, que permiten la extracción de datos sin grandes dificultades. La primera impresión que esto da es que los datos extraídos son públicos y con posibilidad de ser utilizados en investigación para una amplia variedad de propósitos con restricciones legales aparentemente mínimas. ¿Es posible que los datos sean considerados públicos por el sólo hecho de la posibilidad de su acceso?. Burkell et al. [9] trabajan sobre la noción de *privacidad en público* como una lente interesante a través de la cual ver la cuestión de la privacidad en los espacios sociales en línea. En un estudio referido a Facebook donde involucran a sus participantes en un diálogo sobre prácticas de intercambio de información, y que además recorre diferentes posturas en torno a esta temática, reflexionan, a partir de los datos obtenidos, que las redes sociales son de hecho vistas y tratadas por la mayoría de los participantes como espacios "públicos", sin embargo, al menos en algunas circunstancias y con respecto a cierta información, las personas pueden mantener un interés de privacidad en la información que revelan en un dominio público.

Las redes sociales virtuales han logrado tal grado de penetración en la sociedad moderna que derechos fundamentales de las personas, tales como el derecho a la privacidad y a la intimidad, parecen ser vulnerados constantemente, muchas veces invocando el derecho a la información. Como agravante, en reiteradas ocasiones son los mismos usuarios quienes proporcionan gran parte de sus datos sensibles a las corporaciones que detentan el poder de estos espacios. Éstas últimas tampoco parecen hacer grandes esfuerzos por resguardar de terceros los datos obtenidos; sino que por el contrario, admiten realizar negocios vendiendo los datos personales de sus usuarios a empresas de marketing y publicidad.[1]

En este sentido, es claro el análisis que realiza Scanavino[10] de los límites entre el derecho a la privacidad y el derecho a la información, donde plantea que es en este último donde el individuo se puede volver más vulnerable, y es ahí donde el Estado está obligado a velar por el respeto al derecho a la intimidad, resguardando determinados datos "sensibles", teniendo en cuenta entre otros los principios de: limitación legal, especificación del fin, restricción del uso, confidencialidad, consentimiento del afectado, entre otros.

En las próximas secciones del presente artículo nos abocaremos a los aspectos legales que trae aparejado el tratamiento masivo de datos, considerando que los mismos merecen un análisis más amplio.

4. Aspectos Legales

Coincidimos con Sotelo Vargas [11] cuando sostiene que *"[. . .] el derecho no puede permitirse dejar este nuevo fenómeno social por fuera de sus alcances, ya*

[1] Se puede consultar la Declaración de Derechos y Responsabilidades de Facebook como así también su Política de Datos para mayor detalle.

que con el uso de la computadora e Internet, se han generado nuevas situaciones de riesgo, que si bien son de interacción virtual, estas tienen consecuencias materiales. Por tal razón, la exigencia de una reglamentación imperativa o coercitiva que busque proteger los intereses del individuo [...] y el fenómeno de la recolección universal de datos personales".

Hoy en día, la protección de los derechos fundamentales que exige Sotelo Vargas no es tarea fácil en el mundo de las redes sociales, sobre todo teniendo en cuenta lo mencionado por Mutiz et al. [12] cuando plantean: *"La normatividad aplicable a las redes sociales resulta insuficiente ante las múltiples actividades que se realizan a través de ellas, las diferentes nacionalidades que convergen en éstas y las disímiles posturas que se toman frente a la regulación de Internet [...]"*, estudiando la existencia de tres amplios modelos de regulación jurídica, estadounidense, latinoamericano y europeo, para la protección de datos personales en redes sociales.

Ya han habido interesantes contribuciones de diversos autores sobre esta temática. Mientras que Vercelli [13] y Buck [14] discuten diferentes posiciones ante la regulación o autoregulación de la red de redes, Olivera, en su conferencia el marco de las 46 JAIIO/XLIII CLEI, extiende estas consideraciones a partir del planteo de *A dónde vamos: ¿Regular tecnologías o repensar el derecho?*.

Nos proponemos, entonces, nuevos interrogantes. ¿Existe en la actualidad algún marco legal o regulatorio que podamos tomar como base para nuestro análisis? Suponiendo afirmativa la respuesta, ¿está vinculado dicho marco con los términos y condiciones que un usuario acuerda al registrarse en plataformas tales como Facebook y LinkedIn, los cuales habilitan la cesión o venta de los datos que pretendemos utilizar? Cabe además preguntarse: ¿podemos basarnos en dichos términos y condiciones para hacer un uso indiscriminado de los datos?.

En el plano nacional, lo planteado nos refiere al análisis de las leyes y regulaciones específicas existentes orientadas a la protección de datos personales: el artículo 43 de la Carta Magna argentina, como así también la Ley 25.326 de Protección de Datos Personales (LPDP) y sus decretos reglamentarios.

4.1. Normativa Específica

La reforma del año 1994 de la Constitución Nacional Argentina introdujo nuevos derechos y garantías para los ciudadanos, entre los cuales aparece la acción de Habeas Data. Este recurso, que otorga un instrumento de acción ante violaciones a los derechos de privacidad o intimidad de las personas, quedó plasmado en el tercer párrafo del artículo 43 de nuestra constitución, donde se lo define como una acción legal que toda persona podrá interponer: *para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos.*

Es de destacar que el ejercicio de este derecho aparece también en pactos internacionales a los que la Argentina ha suscrito y que tienen en nuestro país fuerza constitucional, pues son incorporados a la Constitución Nacional por el

artículo 75 inciso 22 de la misma. El Pacto de San José de Costa Rica en su artículo 14 establece que: *"Toda persona afectada por informaciones inexactas o agraviantes emitidas en su perjuicio a través de medios de difusión legalmente reglamentados y que se dirijan al público en general, tiene derecho a efectuar por el mismo órgano de difusión su rectificación o respuesta en las condiciones que establezca la ley"*.

Basada en el párrafo tercero del artículo 43 de nuestra Constitución Nacional, se sanciona y promulga en el año 2000 la Ley Nacional para la Protección integral de los Datos Personales que estén almacenados en bancos de datos públicos y privados, Ley de Protección de los datos Personales 25.326 (LPDP)[2] la cual busca *"[...] garantizar el derecho al honor y a intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre [...]"*.

Con la reglamentación de la LPDP a partir del decreto 1558/2001 [3], se crea el órgano de control mencionado en el artículo 29 de la LPDP, con todas las funciones que en él se indican. Este órgano, dependiente del Ministerio de Justicia y Derechos Humanos de la Nación, es el que se conoce como Dirección Nacional de Protección de Datos Personales(DNPDP). La DNPDP *"asesora y asiste a los titulares de datos personales, recibiendo las denuncias y reclamos efectuados contra los responsables de los registros, archivos, bancos o bases de datos por violar los derechos de información, acceso, rectificación, actualización, supresión y confidencialidad en el tratamiento de los datos"* y tiene la atribución de complementar el plexo normativo aplicable a partir normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas en la LPDP[4]. Además de la misión y funciones específicas que explicita en su página institucional, permite el acceso a las leyes y disposiciones referidas a su ámbito de actuación, así como a cursos de capacitación virtuales y comunicaciones sobre las actividades de relaciones institucionales que realiza.

4.2. Aplicabilidad del Marco Legal

Del análisis de la LPDP y su reglamentación podemos encontrar algunas cuestiones significativas para el trabajo que nos proponemos y que, para organizarnos en función de nuestro Proyecto, IISI.d.r.O., hacen referencia a la incidencia de la LPDP sobre: la recolección de datos cuya obtención requiere del consentimiento informado, la posibilidad de almacenamiento de los datos en forma segura para su tratamiento y la necesaria disociación de los mismos de forma tal que sus titulares no sean identificables al momento de divulgación. En el intento de explicarnos cada una de estas cuestiones, podremos ver los retos a los que nos enfrentamos al aplicarlas.

[2] Ley de Protección de los Datos Personales de la República Argentina (Ley 25326) Disponible en: http://www.jus.gob.ar/media/33481/ley_25326.pdf

[3] Decreto Reglamentario N° 1558/2001 de la Ley de Protección de los Datos Personales N° 25.326. Disponible en: http://www.jus.gob.ar/media/33382/Decreto_1558_2001.pdf

[4] Extraído de Dirección Nacional de Protección de Datos Personales - Página institucional: http://www.jus.gob.ar/datos-personales

De la Recolección de Datos y el Consentimiento Informado. Los artículos 5º y 6º de la LPDP son muy claros al establecer que es totalmente necesaria la obtención del consentimiento *"libre, expreso e informado"* de los titulares de los datos para su recolección y futuro tratamiento. En la reglamentación del artículo 4º, a través del decreto 1558/2001, se define al consentimiento informado como *"el que está precedido de una explicación, al titular de los datos, en forma adecuada a su nivel social y cultural, de la información a que se refiere el artículo 6º de la Ley 25.326"*. Para ello, se debe informar a cada uno de los participantes sobre: la finalidad del tratamiento, la existencia del banco de datos y sus responsables, las consecuencias de proporcionar o no los datos y, además, sobre todos los derechos de acceso, rectificación y supresión de los datos que puede el titular ejercer. La DNPDP da especial importancia al consentimiento informado aclarando los aspectos del mismo sobre todo en el caso de Investigaciones médicas [5].

La no obtención del consentimiento hace que el tratamiento de los datos sea considerado ilícito, lo cual tiene consecuencias administrativas según el artículo 31º y penales según el artículo 32º.

Dada la existencia de términos y condiciones que todo usuario de red social acepta en el momento de su registro, podríamos suponer que ya ha dado el consentimiento para cualquier uso de sus datos. No obstante, respecto a la relación que existe entre la LPDP y las políticas de privacidad de las plataformas de redes sociales, Dorado [15] detalla ciertas tensiones entre las mismas. En particular, cuando se trata de cesión y/o transferencia internacional de datos en favor de terceros o cuando se efectúan cambios en las Condiciones de Uso o Políticas de Privacidad de estas plataformas.

Por otra parte, y en un alto porcentaje, los usuarios de redes sociales o cualquier otra tecnología para la cual se solicita el mencionado consentimiento informado, no leen los términos y condiciones. Esta situación ha inspirado proyectos que buscan paliar en alguna medida esta situación, entre ellos los impulsados por EFF[6], Internet Society[7] y ToS;DR[8].

Los riesgos en cuanto a la recolección de datos, aún mediando un consentimiento informado, se traducirán en posteriores problemas en el almacenamiento, tratamiento y divulgación de los mismos.

Procesos de Almacenamiento y Tratamiento de los Datos. No tendrá sentido la obtención del consentimiento informado del titular de los datos para la recolección de los mismos sin el propósito de almacenarlos para su posterior tratamiento. En este punto nos encontramos con tres posiciones antagónicas:

[5] Dirección de Protección de Datos Personales - Obligaciones - Consentimiento Informado Investigaciones Médicas. Disponible en: http://www.jus.gob.ar/datos-personales/tus-obligaciones/consentimiento-informado-investigaciones-medicas.aspx

[6] Electronic Frontier Foundation: https://www.eff.org/

[7] Internet Society: http://www.internetsociety.org/

[8] ToS;DR: Terms Of Service; Didn't read: https://tosdr.org/

la necesidad de almacenarlos para los objetivos de IISI.d.r.O., los términos y condiciones de las plataformas que impiden su almacenamiento, y los principios y obligaciones que establece la LPDP.

Una vez obtenido el consentimiento del titular para cedernos sus datos, si bien son los que el usuario registró inicialmente en alguna plataforma, no debiera haber, prima facie, impedimentos legales que nos coloquen ante un inconveniente frente a las corporaciones que detentan estos datos.

Ahora bien, el artículo 4º de la LPDP dice que en todo momento los datos recolectados deberán ser:

- **Ciertos**: por lo que será menester buscar la forma de verificar la veracidad o falsedad de los mismos.
- **Adecuados y no excesivos**: asumiendo que no se recolectarán datos sin relación al fin que busca o que no se utilizarán en un futuro.
- **Pertinentes**: es fundamental comprender si los datos extraídos realmente aportarán información relevante a la investigación.

En este aspecto y para cumplir frente al titular de los datos y ante la LPDP, el diseño tanto de la interfaz para la obtención del consentimiento como el del modelo de datos, que será plasmado en la base de datos para sustentar el tratamiento posterior, cumplirán un rol clave a la hora de fundamentar qué datos han sido extraídos y cuál será su aporte a IISI.d.r.O.. Esto respeta el principio de considerar la seguridad y privacidad desde el diseño como lo plantea la disposición 18/2015: Guía de Buenas Prácticas en Privacidad para el Desarrollo de Aplicaciones [9], cuyas consideraciones serán válidas, además, para el tratamiento específico de los datos.

Por otro lado, no queremos dejar pasar por alto un tema no menor que es el de inscribir la base de datos en la DNPDP. Si bien, como veremos más adelante, podremos estar exceptuados de este trámite, no lo estaríamos si este trabajo se desarrollara por fuera de los marcos de un Proyecto de Investigación y Desarrollo homologado por la Universidad.

¿Finaliza con estas consideraciones el tema del almacenamiento de los datos? No. El artículo 9º de la LPDP nos indica que: *."El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado"*. En este aspecto, el decreto 1558/2001 no agrega mucha más información diciendo que la DNPDP *"promoverá la cooperación entre sectores públicos y privados para la elaboración e implantación de medidas, prácticas y procedimientos que susciten la confianza en los sistemas de información, así como en sus modalidades de provisión y utilización"*. Sin embargo, surgen con posterioridad las

[9] Disposición 18/2015: Guía de Buenas Prácticas en Privacidad para el Desarrollo de Aplicaciones. Disponible en: http://www.jus.gob.ar/media/2854264/disp_2015_18.pdf

disposiciones 11/2006 y 09/2008 que aprueban las *"Medidas de Seguridad para el Tratamiento y Conservación de los Datos Personales Contenidos en Archivos, Registros, Bancos y Bases de Datos Públicos no estatales y Privados"* y prorrogan su plazo de cumplimiento respectivamente. Aunque en la actualidad estas disposiciones estén siendo revisadas por cuestiones de aplicabilidad, según se indica en la página institucional de la DNPDP, las mismas han establecido niveles de seguridad, medidas y modelos para el registro[10]

Nuestro desafío será aquí poder equiparar lo requerido por estas disposiciones, muchas veces desactualizadas en cuanto al avance de la tecnología, con los principios de normas reconocidas internacionalmente, más particularmente con la familia de normas ISO 27.000 que refieren específicamente al tema de Seguridad de la Información y son abarcativas de lo enunciado por las disposiciones.

Disociación y Divulgación de los Datos. Obtenido el consentimiento y almacenados los datos, nos restaría llevar adelante su tratamiento, y así producir indicadores clave relevantes a IISI.d.r.O. y la construcción del mapa interactivo que nos proponemos. Situados en este punto, comenzamos a ver ciertas cuestiones que nos pueden llevar a posiciones contradictorias.

Si por un lado para divulgar los datos aplicáramos primero un proceso de disociación de forma tal que su titular no fuera identificable, por lo explicitado en el artículo 11°, no sería necesario el consentimiento informado. La disociación nos permitiría también, siguiendo el artículo 7° de la ley en su inciso 2, el tratamiento de datos sensibles cuando sea con fines estadísticos y no puedan ser identificables sus titulares, que es bueno tener en cuenta, si bien los datos a recolectar por nuestro proyecto no encuadran dentro de los considerados datos sensibles. Ahora, si antes de almacenar los datos los sometiéramos a un proceso de disociación, no sería necesario ni el consentimiento ni la necesidad de adoptar normas de seguridad en función de la Ley, aunque sí para resguardar los productos del proyecto. Entonces, ¿sólo estaríamos solicitando el consentimiento para no provocar conflictos con las corporaciones que detentan el poder de los datos?

Primero deberíamos respondernos a la factibilidad de resolver el problema tecnológico de la disociación o anonimización de los datos. ¿Será efectiva esa disociación en todos los casos? En el caso específico del mapa interactivo que pretendemos construir, ¿Cuánto tiempo tardaría en identificarse a un profesional de nuestra institución si el mapa nos informa que hay sólo un graduado trabajando en un cierto país del extranjero, en una empresa particular y que es experto en ciertas tecnologías? ¿Querrá esa persona participar de nuestro *aparentemente* inofensivo mapa?

Esta última pregunta, que tiene efectos luego de la divulgación de los datos obtenidos, nos trae a la reflexión sobre un nuevo riesgo no considerado hasta aquí: los usos imprevistos de las tecnologías. Para citar algunos ejemplos: los trabajos del artista belga Dries Depoorter [17] que trabaja sobre cuestiones de

[10] Todas las Disposiciones de la DNPDP pueden ser consultadas en: http://www.jus.gob.ar/datos-personales/normativa/disposiciones-pdp.aspx

Internet, privacidad, identidad en línea y vigilancia, y los usos que se realizan de los datos recolectados por la plataforma Waze en España[18].

Excepciones. En relación a lo tratado en las secciones anteriores, debemos citar el artículo 28º, cuyo contenido refiere a los archivos, registros o bancos de datos relativos a encuestas. El mismo declara: *"Las normas de la presente ley no se aplicarán a [...] investigaciones científicas o médicas y actividades análogas, en la medida que los datos recogidos no puedan atribuirse a una persona determinada o determinable. Si en el proceso de recolección de datos no resultara posible mantener el anonimato, se deberá utilizar una técnica de disociación, de modo que no permita identificar a persona alguna".*

Teniendo en cuenta que todas las actividades que realizamos están enmarcadas en el proyecto de investigación y desarrollo IISI.d.r.O., sumado a nuestro compromiso hacia la correcta e integral disociación de los datos publicados, la ley bajo análisis no parece poner impedimentos en el logro de nuestras metas. Aún así, la decisión tomada inicialmente ha sido la de no considerar esta excepción para así poder tener en cuenta todas las implicancias en cualquier contexto donde se requiera el tratamiento masivo de datos.

4.3. Algunas Conclusiones Preliminares

Como al parecer gran proporción de los usuarios no lee los términos y condiciones de uso, ni las políticas de privacidad de las plataformas, es altamente probable que, al momento de dar o no el consentimiento para brindarnos sus datos para nuestro proyecto, el usuario no preste atención a las explicaciones que le brindemos sobre cómo y a qué estará encausado el procesamiento y tratamiento de sus datos. ¿Podríamos aducir, entonces, el principio latino *"nemo auditur propriam turpitudinem allegans"* - nadie puede alegar su propia torpeza-? Más allá de los riesgos que podrían presentarse en un futuro con un titular de datos que haya brindado su consentimiento, para más tarde considerar inapropiado nuestro objetivo, algo nos lleva a continuar con el análisis. Nuestros valores, nuestro *ethos* y la responsabilidad que nos cabe como profesionales ante la sociedad.

5. Compromiso Ético y Responsabilidad Social

Como expresa Cabrera [19,20]: *"Las reglas de ética son importantes y fundamentales para nuestra riqueza comunitaria, la vida en sociedad civil, tanto familiar como profesional, como también para nuestra elevación personal como seres humanos, creciendo moralmente. La Protección de Datos Personales es un medio efectivo para el real cumplimiento de las Garantías Constitucionales y los Derechos Humanos[...] Al respetar la información personal de nuestros semejantes, respetamos sus derechos, y por ende, sus garantías constitucionales, y sus Derechos Humanos[...]".*

Ahora bien, y según lo planteado en nuestras conclusiones preliminares, no hemos encontrado en la LPDP respuestas concretas al planteo que nos hacemos

referidos a los aspectos éticos y de responsabilidad social que deben guiar nuestro trabajo.

Bucear en estos aspectos nos llevaría a plantearnos un recorrido que, como lo hace Mitcham [21], atraviesa posicionamientos que surgen en el siglo XVI, *en una concepción de la tecnología entendida como medio para alcanzar el bien; si no en sí mismo, una forma del bien*, y gran cantidad de diferentes posicionamientos en el siglo XX, desde la interpretación de *la tecnología como un nuevo tipo de coacción sobre la condición humana* hasta la emergencia *de una serie de preguntas dirigidas al humanismo tecnológico*. En este recorrido Mitcham individualiza respuestas prácticas y teóricas, así como nuevas opciones aparecidas en el siglo XXI al que caracteriza como *el siglo que ha comenzado con una nueva idea de la relación entre tecnología y ética*. Identifica además al menos tres áreas en las que se ha avanzado hacia los temas de ética y tecnología: la filosofía, los estudios de ciencia y tecnología, y el ámbito de la política de ciencia y tecnología.

De manera más específica a nuestro contexto, Vayena et. al [16] plantean la necesidad de la existencia de un marco ético para la investigación en Big Data, que cuente con definiciones y estándares para la consideración de la privacidad de los sujetos de la investigación, incorporando a su vez mecanismos que permitan verificar los usos previstos, beneficios, amenazas, daños y vulnerabilidades asociadas con la actividad de investigación específica. Sostienen que dicho marco ético debería ser producto de un proceso en el que participen los múltiples actores involucrados y ser diseñado de forma tal que capture la más reciente comprensión científica de la privacidad, métodos analíticos, salvaguardas disponibles, normas sociales, como así también las mejores prácticas para la ética de la investigación, en la medida que éstas evolucionan con el tiempo.

Con miras a alcanzar el conocimiento contextualizado que pretendemos en IISI.d.r.O. y tomando como base las consideraciones expuestas anteriormente, nos formulamos un nuevo interrogante, que trataremos de responder desde las ópticas de nuestras comunidades técnica, científica y académica locales. ¿Existen marcos éticos que nos guíen en desarrollar conductas apropiadas relativas al tratamiento de datos tanto como profesionales, investigadores o docentes?

Desde nuestra óptica como profesionales, encontramos el Código de Ética Profesional y Disciplina[11] del Colegio de Ingenieros Especialistas, siendo ésta la asociación que nuclea a los profesionales de la Ingeniería en Sistemas de Información en conjunto con otros profesionales de la Ingeniería en la Provincia de Santa Fe. El código dedica gran cantidad de artículos al tratamiento de cuestiones netamente administrativas, de la conformación del Tribunal de Ética Profesional, del desarrollo del proceso que se inicia a partir de la presentación por parte de un tercero de una causa comprendida en las faltas de éticas reconocidas por el código y de las sanciones y recursos que se pueden interponer. En cuanto a las

[11] Código de Ética Profesional y Disciplina. Aprobado por el Directorio Provincial del Colegio de Ingenieros Especialistas de la Provincia de Santa Fe el 16/04/2009. Disponible en: https://cie.gov.ar/web/images/Documentos/28.pdf.

cuestiones de fondo, que entendemos vinculadas a aquellas consideradas como actos contrarios a la ética profesional, sólo las vincula con actos para con los colegas, para con los comitentes o empleadores, deberes para con el Colegio y para la profesión. En este último caso, solo referidas a cuestiones técnicas, de procedimiento o que afecten a la imagen profesional. No existen menciones a la ética profesional en virtud del interés general, los riesgos ambientales, sociales, y menos aún, de las consecuencias del uso de las tecnologías en la práctica diaria.

Nuestra óptica como académicos nos hace remitirnos al Estatuto de la UTN[12] y en particular al Diseño Curricular de la Carrera de Ingeniería en Sistemas de Información[13].

El Estatuto de la UTN es claro en este sentido en la definición de la misión, a cuyos fines se propone objetivos relacionados con lo académico, con lo regional y local, con lo nacional, lo internacional, lo científico y tecnológico, lo social y lo humanístico y cultural. En este último punto se propone *Comprometerse con la formación de sus graduados, enriqueciendo los conocimientos científicos y tecnológicos con los productos de otras áreas de la cultura universal y los valores éticos que definen a los hombres cabales y solidarios.* Este enriquecimiento debiera verse plasmado en la definición del Perfil Profesional y del Diseño Curricular de la carrera de Ingeniería en Sistemas de Información anteriormente mencionado. Más allá de la intención planteada en el Perfil Profesional *la preparación integral recibida en materias técnicas y humanísticas, lo ubican en una posición relevante en un medio donde la sociedad demandará cada vez más al ingeniero un gran compromiso con la preservación del medio ambiente, el mejoramiento de la calidad de vida en general y una gran responsabilidad social en el quehacer profesional*, en la práctica la ética profesional sólo se destaca como parte del contenido en la asignatura Legislación.

Surge entonces, como consecuencia de lo expuesto, un nuevo interrogante: ¿podemos referirnos a la ética profesional en función de analizar el impacto que puede tener nuestro accionar junto con la responsabilidad que nos cabe como profesionales ante la sociedad? Esta perspectiva de responsabilidad social concierne a nuestro análisis, puesto que está vinculada íntimamente con el objetivo principal de IISI.d.r.O.

La construcción de la red y del mapa interactivo que proponemos procuran por un lado realizar aportes sustantivos a las metas de IISI.d.r.O, y por el otro ser un instrumento abierto a la comunidad en general. Se lograrían beneficios tanto para las empresas del sector y el Estado, como así también hacia el interior de la Universidad donde docentes, estudiantes y egresados, podrían verse beneficiados a través de contar con información para el planteo de estrategias referidas a los

[12] Estatuto de la Universidad Tecnológica Nacional. Resolución de la Asamblea Universitaria 1/2011. Disponible en: http://csu.rec.utn.edu.ar/docs/php/buscador.php3?categoriaid=0216

[13] Diseño Curricular de la Carrera de Ingeniería en Sistemas de Información. Ordenanza del Consejo Superior Universitario 1150/2007. Disponible en: http://csu.rec.utn.edu.ar/CSU/ORD/1150.pdf

planes de estudio, disparadas por las necesidades detectadas por el equipo que conforma IISI.d.r.O. Vemos así que el fin del tratamiento de datos en IISI.d.r.O. es en beneficio de la sociedad en su conjunto, a pesar de que en el proceso algún individuo pueda sentir su derecho a la privacidad menoscabado. Sin embargo, esto nos pone nuevamente en los posicionamientos discutidos ya en el Siglo XVI.

Será menester alcanzar un equilibrio entre el respeto al derecho de autodeterminación informativa del individuo consagrado por la LPDP, y el derecho a la información, en particular a la comunicación de información de base empírica que obtendremos de la realización del análisis de redes sociales que traería aparejado numerosas ventajas a los actores mencionados anteriormente.

6. Conclusiones y Reflexiones

Como podemos analizar del recorrido del trabajo, son numerosos y variados los retos a los que se enfrenta el profesional en Sistemas y Tecnologías de la Información en su práctica diaria y que van más allá de sus capacidades técnicas específicas.

El trabajo realizado intentó ir más allá de encontrar respuestas específicas al tratamiento masivo de datos para verificar la posibilidad de que los convocados a participar en el grupo de discusión de IISI.d.r.O. pudieran desarrollar una estrategia de abordaje de las cuestiones legales, éticas y de responsabilidad social. Preguntas y repreguntas fueron necesarias, a lo largo del estudio, para minimizar los efectos de nuestra formación, netamente tecnológica, frente a plantearnos el desafío de pensar como nos proponemos en IISI.d.r.O..

Por otra parte, el análisis de un caso en particular, como es el tratamiento masivo de datos almacenados en redes sociales virtuales, ha bastado para exponer, desde nuestra modesta opinión, lo insuficiente del plexo normativo ante la complejidad de los desarrollos tecnológicos y su continua evolución. Consideramos que poco se realiza desde los ámbitos institucionales para concientizar a los ciudadanos, y en particular a los profesionales en Sistemas y Tecnologías de la Información, de la necesidad del abordaje integral de estas problemáticas. Los esfuerzos que podamos hacer desde el lado de la investigación serán también insuficientes e indudablemente en poco tiempo quedarán obsoletos.

Como reflexión queda considerar la necesidad de avanzar sobre la construcción de una cultura de la ética y la responsabilidad social desde las premisas que guían a la formación humana integral: *Saber conocer, saber hacer, saber ser y saber convivir*. Éstas están fuertemente vinculadas a la formación en competencias que plantea Tobon [22] y son fundamentales para promover el *proyecto ético de vida* de profesionales y futuros egresados.

7. Trabajos a Futuro

Dado el interés del equipo de trabajo sobre la temática, sumado a las problemáticas aún no resueltas y los resultados que el Observatorio seguirá produ-

ciendo en el futuro, creemos conveniente dejar planteadas algunas futuras líneas de investigación:

- La aplicabilidad de las normas ISO 27.000 asociadas a la seguridad y privacidad de los datos recolectados por IISI.d.r.O.
- Análisis de marcos éticos y de responsabilidad social vinculados a los profesionales de Sistemas y Tecnologías de la Información nacionales e internacionales para una propuesta integral al Consejo de Ingenieros Especialistas de la Provincia de Santa Fe.
- Estrategias para la formación en competencias del Ingeniero en Sistemas de Información basado en el conocimiento de base empírica producido y gestionado por toda la plataforma tecnológica de IISI.d.r.O.
- Ética y Responsabilidad Social del Ingeniero en Sistemas de Información como competencias centrales en su formación profesional. Metodologías para su incorporación en el tronco integrador de la carrera.

Referencias

1. Carrizo, L., Mayra E., Julie K.: Transdisciplinariedad y complejidad en el análisis social. Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (2004)
2. Riva F., Amar E., Martín V., Gatto M., Pereira N.: Observatorio de Desarrollo Regional de la Ingeniería en Sistemas de Información e Informática(IISI.d.r.O.). Origen, Evolución y Perspectivas. En memorias: CONAIISI 2016. IV Congreso Nacional de Informática e Ingeniería en Sistemas de Información. UCASAL. Publicación on line - ISSN 2347-0372 (2016)
3. Riva F., Amar E., Martín V., Pereira N.: Una red para el análisis comparado de competencias en la trama productiva de la Industria del Software y Servicios Informáticos. En revista: Rumbos Tecnológicos de la Secretaría de Ciencia, Tecnología y Posgrado de la UTN-FRA – Volumen 8 Septiembre 2016. 135-143 (2016)
4. Malano R., Martín V., Riva F.: Favoreciendo el desarrollo de conocimientos y competencias en el contexto de un Proyecto de Investigación. En memorias: CONAIISI 2016. IV Congreso Nacional de Informática e Ingeniería en Sistemas de Información. UCASAL. Publicación on line - ISSN 2347-0372 (2016)
5. Abbatemarco M., Brizuela L., Cervino A., Riva F.: Las redes sociales como fuente de datos para un Observatorio Regional de Ingeniería en Sistemas de Información e Informática. Oportunidades y limitaciones técnicas, éticas y legales. En memorias: CONAIISI 2016. IV Congreso Nacional de Informática e Ingeniería en Sistemas de Información. UCASAL. Publicación on line - ISSN 2347-0372 (2016)
6. Palacios E.M.G., Galbarte J.C.G., Cerezo J.A.L., Luján, J. L., Gordillo, M.M., Osorio C., Valdés C.: Ciencia, tecnología y sociedad: una aproximación conceptual. Organización de Estados Iberoamericanos (OEI) (2005)
7. Morin, E.: Introducción al pensamiento complejo. Gedisa. Barcelona (1994)
8. Morin, E.: Los siete saberes necesarios para la educación del futuro. Unesco (1999)
9. Burkell, J., Fortier, A., Wong, L. L. Y. C. y Simpson, J. L.: Facebook: Public space, or private space?. Information, Communication and Society, 17(8), 974-985 (2014)
10. Scanavino, F. O.: Derecho a la intimidad vs Derecho a la información. Antagonismo o complementariedad. Sistema Argentino de Información Jurídica (2012)

11. Sotelo Vargas D. A.: El habeas data en las redes sociales online: responsabilidad y vigilancia. Revista Iter Ad Veritatem 10, Universidad Santo Tomás, Tunja (2012)
12. Mutiz, P. L. A., Hoyos, J. A. N., Leguizamón, F. G., Gómez, C. C.: Modelos de regulación jurídica de las redes sociales virtuales. Revista Via Iuris, 11, pp. 109-136 (2011)
13. Vercelli, A.: Repensando las regulaciones de Internet. Análisis de las tensiones políticas entre no-regular y re-regular la red-de-redes. Chasqui. Revista Latinoamericana de Comunicación, 129, pp. 95-112 (2015)
14. Buck, A. V. D.: La autorregulación en redes sociales como forma de garantizar los derechos de intimidad, privacidad y protección de datos personales. Derecom, 13, 10 (2013)
15. Dorado, J. G.: Derecho a la intimidad y protección de datos personales en las condiciones de uso y políticas de privacidad de las redes sociales. Sistema Argentino de Información Jurídica (2016)
16. Vayena, E., Gasser, U., Wood, A., O'Brien, D.R., Altman, M.: Elements of a New Ethical Framework for Big Data Research. Washington & Lee Law Review Online. Vol 72 pp. 420-441 (2016)
17. Greenberg, A.: Turning Live Surveillance Feeds Into Unsettling Works of Art. Revista Online Wired (2016)
18. Pueyo Busquets, J.: La aplicación Waze llega a los centros de control del tráfico. Diario El País, España (2016)
19. Cabrera, R. F.: Ética, secreto profesional y protección de datos. Observatorio Iberoamericano de Protección de Datos (2013)
20. Cabrera, R. F.: La ética, la privacidad y el secreto profesional. Observatorio Iberoamericano de Protección de Datos (2013)
21. Mitcham, C.: De la tecnología a la ética: experiencias del siglo veinte, posibilidades del siglo veintiuno. Revista iberoamericana de ciencia tecnología y sociedad 2.5 pp. 167-176 (2005)
22. Tobón, S.: Formación integral y competencias. Pensamiento complejo, currículo, didáctica y evaluación, volumen 3. Bogotá, Colombia (2013)