Edición Especial

REVISTA DEL DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN DE LA UNIVERSIDAD DE CHILE

Bits DE CIENCIA

EDICIÓN N°19 | PRIMER SEMESTRE 2020

Ciencias de la Computación
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
UNIVERSIDAD DE CHILE

TECNOLOGÍAS DIGITALES Y PROCESO CONSTITUYENTE

¿Representan los datos de medios sociales a Chile? / Ricardo Baeza-Yates

Votación electrónica y democracia / Alejandro Hevia

Muro de expresión. Expertos opinan sobre temas de tecnología digital a considerar en una nueva Constitución

Contenidos

Tecnologías digitales y proceso constituyente

Revista Bits de Ciencia Nº19
ISSN 0718-8005 (versión impresa)
www.dcc.uchile.cl/revista
ISSN 0717-8013 (versión en línea)

Departamento de Ciencias de la Computación

Avda. Beauchef 851, 3º piso, edificio norte. Santiago, Chile. 837-0459 Santiago

www.dcc.uchile.cl

56 22 9780652

revista@dcc.uchile.cl

/ dccuchile

Editorial

FEDERICO OLMEDO
Editor General
Revista Bits de Ciencia

Sin duda, el estallido social del 18-O es uno de los hitos más relevantes de la historia chilena contemporánea. Si bien hay cierto consenso sobre cuáles fueron sus causas, cuáles serán sus consecuencias a largo plazo parece ser más incierto y difícil de predecir hoy en día. Lo que sí podemos asegurar es que abrió un proceso constituyente, dando paso a la inminente posibilidad de una nueva carta magna.

Las tecnologías digitales han jugado un rol no menor en el desarrollo y análisis del conflicto social (recordar, por ejemplo, la "información extraordinariamente sofisticada [...] con tecnología de big data" de Blumel y compañía) y tendrán, potencialmente, un rol mucho más protagónico en el proceso que se viene. Por tanto, hemos decidido lanzar este número especial de la Revista abocado enteramente a dicha temática. Abordamos interrogantes que van desde qué rol jugaron las redes sociales en la gestación del estallido y qué tan fielmente refleja Twitter la opinión de toda la población chilena, hasta qué tan razonable sería adoptar la votación electrónica y qué aspectos del mundo digital deberían incorporarse en una nueva Constitución.

Desde nuestro lugar, esperamos que este material sirva como punto de partida para un oportuno debate y reflexión respecto al rol de las tecnologías digitales en el Estado de derecho, especialmente frente a la relevancia de los acontecimientos que nos deparan los próximos meses en el porvenir de todos los chilenos y todas las chilenas. ▪

La tentación tecnológica

Alcances y límites de las tecnologías digitales para la democracia

CLAUDIO GUTIÉRREZ

Profesor Titular del Departamento de Ciencias de la Computación de la Universidad de Chile. Investigador Senior del Instituto Milenio Fundamentos de los Datos. Ph.D. Computer Science, Wesleyan University. Líneas de investigación: fundamentos de la computación, lógica aplicada a la computación, bases de datos, semántica de la Web, máquinas sociales.

cgutierr@dcc.uchile.cl

Estamos viviendo un momento histórico gatillado por el estallido del 18 de octubre. La movilización social ha impulsado una discusión, a través de cabildos y reuniones varias, sobre la forma en que queremos convivir en sociedad. Y luego, sobre las reglas generales que debiéramos fijarnos para esa convivencia, que en términos legales se llama *Constitución*. Un aspecto muy relevante de esa discusión es la manera en que debiéramos llevar a cabo ese proceso, que en el fondo, es una discusión sobre la democracia. Lo que sigue es una reflexión sobre los alcances y límites de las tecnologías digitales para la democracia.

La democracia es un asunto complejo y de muchas facetas. Para lo que sigue, me centraré en un aspecto, muy relevante, de ella: cómo *proceder* a la hora de adoptar decisiones.[1] ¿Qué significa un procedimiento (de decisión) democrático? Robert Dahl, afamado cientista político estadounidense, pensador liberal, a quien nadie osaría acusar de inspirar la crisis chilena, define los siguientes criterios para ello, que para los efectos de este artículo son un buen piso mínimo [1]:

1. ***Participación efectiva:*** todxs deben tener oportunidades iguales y efectivas, que sus puntos de vistas sean conocidos por otros miembros de la sociedad.

2. ***Igualdad de voto:*** cuando llegue a adoptarse una decisión, todxs deben tener una igual y efectiva oportunidad de votar.

3. ***Comprensión ilustrada:*** dentro de tiempos razonables, todxs deben tener oportunidades iguales y efectivas de instruirse sobre las alternativas relevantes y sus consecuencias.

4. ***Control de la agenda:*** todxs deben tener oportunidades exclusivas de elegir qué asuntos y cómo deben ser incorporados a la agenda de discusión.

5. ***Inclusión de adultxs:*** todxs quienes sean adultxs deben tener los plenos derechos de ciudadanía incluídos en los puntos anteriores.

La democracia es un asunto antiguo, cuyo origen es atribuído a las ciudades griegas de antes de nuestra era. Una élite, usualmente reunida en una plaza pública, tomaba las decisiones políticas, esto es, determinaba las maneras de convivir, mientras artesanos, esclavos y mujeres trabajaban para mantenerlos. La idea se extendió a partir de la revolución francesa y comenzó a incluir a poblaciones cada vez más amplias. En Chile, recién en 1950 se incluyó a todos los adultos: hasta 1949 la mitad de la población, las mujeres, no tenía derecho a decidir sobre asuntos políticos del país.

Las maneras de tomar decisiones colectivas en una población grande y en países tan extensos territorialmente como Chile no son sencillas. Por ejemplo, ¿cómo se produce la participación efectiva? ¿Cómo un ciudadano de Punta Arenas conoce los puntos de vista de una ciudadana de Arica? ¿Cómo establecer la agenda de temas? ¿Cómo integrar luego las preferencias? ¿Qué hacer para que todxs conozcan las alternativas relevantes y sus consecuencias?

Ha surgido de un tiempo a esta parte la idea de que las tecnologías digitales resolverían muchos o todos estos problemas. A primera vista las redes sociales y el acortamiento (o según lxs más optimistas, la anulación) de las distancias por las comunicaciones digitales hacen gran parte del trabajo. Otro tanto lo harían los algoritmos de agregación que podrían implementarse para grandes cantidades de datos de manera casi instantánea. También las nuevas tecnologías digitales resolverían los problemas de presentación de información y facilidades de votar sin las barreras espaciales como el tener que ir a un lugar, etc. Incluso algoritmos nuevos de votación evitarían los conocidos sesgos y limitaciones de la agregación de preferencias clásica [2]. Pero sobre todo, está la idea de que las tecnologías y algoritmos resolverían los sesgos inherentes a los procesos humanos y harían todo más neutro y limpio.

1 | Algunos (como Robert Dahl) consideran que ello constituye la esencia de la democracia. Se los denomina *procedimentalistas.* Otra faceta fundamental son los fines: ¿qué se persigue con la democracia? Supondremos aquí un tácito consenso sobre la necesidad y virtudes de la democracia.

Algunos ejemplos para motivar la reflexión. En Chile la creencia de que los problemas políticos que tenemos son resolubles por tecnologías tiene historia. Probablemente el primer caso paradigmático es el sitio http://www.tuconstitucion.cl/ del expresidente Ricardo Lagos. "Aprovechando las oportunidades que ofrecen las nuevas tecnologías para canalizar la participación" se propuso "recoger ideas y sueños" para la elaboración de una Constitución. El proceso constitucional del Gobierno de Bachelet "Una Constitución para Chile" (cuyas trazas pueden rastrearse en el estudio de Jorge Pérez *et al.*)[2] es otro intento de usar tecnologías digitales para canalizar una discusión constitucional. Pocos días después del 18 de octubre, el emprendedor César Hidalgo lanzó la plataforma http://chilecracia.cl con la consigna: "Priorizamos la demanda ciudadana para ayudar a construir las soluciones que nuestro país necesita hoy". Recibió fuertes críticas por la calidad del muestreo y el ordenamiento (por ejemplo su algoritmo rankeó "nueva Constitución" bastante bajo a contrapelo de lo que todos observaban), lo que sumado a otros detalles desdibujó el proyecto inicial. La Asociación Chilena de Municipalidades lanzó una consulta ciudadana en diciembre de 2019 cuya novedad en el país fue el uso sistemático de votación digital. Por su parte el Gobierno, desde los primeros días después del 18 de octubre, levantó la idea de "diálogos ciudadanos" que se desarrollarían en una plataforma digital como "un mecanismo que permita canalizar el descontento y demandas ciudadanas, junto con contener la actual crisis" [3]. Terminó siendo el sitio https://chilequequeremos.cl/ con la consigna "escuchémonos y construyamos el Chile que queremos", el que implementaría una "proceso abierto de Escucha Social".

Estos ejemplos muestran potencialidades y limitaciones de las tecnologías digitales.

¿Qué es mi opinión ingresada en una plataforma que luego los gobernantes no consideran o la desprecian?

¿Son ellas intrínsecas al medio digital? Con estos casos en mente, reflexionemos sobre los alcances y limitaciones de las tecnologías digitales para cumplir los cinco puntos de Dahl. Veamos.

1. Participación efectiva.

Lo que aseguran las tecnologías digitales es la posibilidad *teórica* de que los puntos de vista de todxs sean conocidos. Hoy —particularmente después del advenimiento del proyecto original de la Web— tenemos los mecanismos técnicos para poder participar independientemente de idiomas, territorio, aparato, etc. [4]. Destacan aquí también una serie de iniciativas de participación ciudadana como encuestas deliberantes, presupuestos participativos, conferencias de consenso, mapeos deliberativos, jurados ciudadanos [5]. Y, por supuesto, las redes sociales. En la práctica, sin embargo, hay determinantes sociales que dificultan esas posibilidades. La difusión de información en plataformas y redes sociales sigue una ley de potencias o ley de Zipf (llamada así por el lingüista Zipf que enunció algo que todos sabemos: hay pocas palabras conocidas por todos y muchas, muchas, que la mayoría desconoce). Por un lado, por más que uno tenga acceso a redes sociales, por más que me ofrezcan plataformas para "escuchar" mi opinión, ella será raramente escuchada si nadie me conoce. ¿Qué es mi opinión, mi "página" o mi tweet, comparado con la portada de El Mercurio o La Tercera o el noticiario de TVN o T13? ¿Qué es mi opinión ingresada en una plataforma que luego los gobernantes no consideran o la desprecian? Todo lo anterior se agrava en Chile con la segregación social, cultural y económica existente. La democracia es esencialmente un espacio de iguales. Y como escribe el profesor Enrique Fernández Darraz, "las élites chilenas nunca han considerado al pueblo como un igual. No solo eso, con frecuencia lo han concebido como inferior cultural, moral y hasta biológicamente. De ahí que se alejen y aíslen de él, nucleándose en sectores alejados y reproduciéndose de manera endogámica" [6]. Menos querrán "escucharlo". En resumen, la participación efectiva es el resultado de un complejo sistema, por un lado, de reconocimiento y de valoración de los otros, por otro de posesión de recursos y, finalmente, de equidad en el acceso a los medios de comunicación. Es bueno que quienes trabajamos en tecnología digitales estemos muy conscientes de esto a la hora de diseñar sistemas para participación política.

2. Igualdad de voto.

Se afirma que con las tecnologías digitales todxs tendrán oportunidad de expresar su preferencia (o de votar), particularmente porque facilitan la vida a quienes viven lejos de los centros urbanos o tienen dificultades para desplazarse. Esta afirmación es un asunto en debate hoy y de respuesta negativa por el momento. En efecto, la posiblidad de la votación electrónica segura es un (gran) debate abierto en las ciencias de la computación [7]. En este aspecto, las tecnologías digitales hoy ayudan poco a expresar preferencias. Es imposible determinar identidad, manipulación, etc. y la evidencia indica que no mejoran la

2 | http://constitucionabierta.cl/

participación presencial. La experiencia de la consulta de los alcaldes en diciembre puede ayudar a reflexionar sobre los puntos positivos y negativos de ello hoy.

Las tecnologías digitales a lo más dan mayor acceso a materiales de información y estudio, pero para procesarlos hay que tener tiempo y educación.

3. Comprensión ilustrada.

Oportunidades iguales y efectivas de instruirse sobre las alternativas. Descontando la formación política (el entendimiento de cómo se organiza la sociedad y los factores que inciden en ello), éste es un punto donde las tecnologías inciden hoy de manera más relevante. Desde las pervasivas redes sociales que se han transformado casi en medios de comunicación alternativos, hasta plataformas de información a los votantes (las VAA, *Voting Advice Applications*) que permiten hacerse una idea de candidatxs y sus programas [9]. Es importante aquí destacar dos sesgos que afectan estas posibilidades. El primero, y menos visible, son las brechas digitales, tanto a nivel de acceso a aparatos y a conectividad como el más relevante, de comprensión de los contenidos. Aquí hay que incluir la disposición y el tiempo. Las tecnologías digitales a lo más dan mayor acceso a materiales de información y estudio, pero para procesarlos hay que tener tiempo y educación. El segundo sesgo, ligado al anterior, es la manipulación a través de redes sociales, desde las *fake news* (como toda mentira, afecta más a quién tiene menos conocimientos y herramientas de comprensión) hasta las campañas usando técnicas como *microtargeting* (esto es, haciendo propaganda dirigida a cada persona o grupo de personas, con mensajes informativamente sesgados o incluso contradictorios). Luego la responsabilidad de los desarrolladores hoy no es solo desarrollar plataformas amigables, accesibles, etc., que ayuden a superar las brechas, sino también estudiar y proveer las herramientas para evitar los sesgos, para empoderar al ciudadano común respecto de la manipulación que pueden realizar quienes tienen más poder (económico, cultural y tecnológico).

4. Control de la agenda.

¿Qué asuntos y cómo deben ser incorporados a la agenda de discusión? Fíjense que ésta es la pregunta más importante que hace que la política no podrá nunca escapar del debate humano. En general, las tecnologías digitales han mostrado ser muy buenas *operacionalizando* ideas. Sin embargo, aún con metodologías estadísticas que evitan el razonamiento "cuadrado" de la lógica formal (usualmente asociado a los computadores tradicionales), falta lo que se conoce como definición de agendas, que es nada más (ni nada menos) que combinar diferentes niveles lógicos (para lo que los computadores son aún muy malos y vaya a saber si habrá limitaciones fundamentales). Piense en cómo organiza y jerarquiza usted lo que quiere hacer en su vida, su "agenda" de vida. No hay un menú fijo ni una taxonomía universal. Se combinan —de acuerdo a cada uno— planos lógicos muy diferentes: el apego filial, el mercado laboral, las posibilidades físicas, las oportunidades del momento, los deseos, los planes a largo plazo, etc. etc. No hay una vitrina ni un catálogo de actividades vitales dado para proceder a la agregación de preferencias. ¿Quién define entonces la agenda política? Ese proceso, lo opuesto a lo operacional, es elemento esencial de la democracia. Obviamente plataformas tecnológicas y algoritmos no resolverán eso. A lo más, ayudarán a implementar algunos de esos procesos.

6. Inclusión de los adultxs.

Finalmente llegamos a un punto obvio, pero que no es tan obvio para muchos. Todxs deben tener derecho a los puntos anteriores. Hay una idea muy difundida de que, como los problemas políticos y sociales son complejos (de hecho, cada día más complejos), hay que dejarlos en manos de "expertos", que usarían nuestros "insumos" (nótese el lenguaje empresarial) para tomar las "buenas" decisiones. A nosotros solo nos correspondería ser consultados. Y aquí es dónde es más común ver surgir plataformas consultivas que muchos pretenden hacer pasar como la democracia instituída.

A manera de conclusión

Las tecnologías digitales, hoy más que nunca, con la disponibilidad de datos masivos (big data) e inteligencia artificial (*deep learning* y otros mecanismos), muestran una potencialidad casi ilimitada. Las aplicaciones sobre redes sociales, plataformas de participación, métodos de votación, etc. han cambiado la manera de informarse, de comunicarse y de participar. Particularmente las redes sociales han mostrado un potencial tremendo contra la desinformación y para convocar distribuidamente.

Esto puede llevar a la "tentación tecnológica", esto es, a pensar que estas tecnologías pueden resolver el problema de la democracia y la política. Quienes trabajamos en tecnologías digitales debemos no solo estar muy conscientes, sino que tenemos una gran responsabilidad en alertar y educar a la población, sobre estos alcances y estas limitaciones. Las tecnologías digitales —como cualquier tecnología— no resolverán el problema de la democracia ni menos sustituirán el hacer humano en ese ámbito. A lo más lo pueden apoyar, como pudiera hacerlo toda tecnología. Pero las responsabilidades y las decisiones codificadas en ellos siguen siendo nuestras.

Una reflexión final. La esencia de las limitaciones de las tecnologías digitales en este ámbito es que la democracia no es solo un procedimiento, sino que tiene un fin. ¿Para qué queremos democracia? ¿Para qué queremos decidir democráticamente? El profesor Dan Wallace de la Universidad de Princeton escribía: "El propósito de un sistema de votación no es nombrar al ganador, sino convencer al perdedor" [7, 8]. Parafraseándolo para el ámbito de la democracia (que es mucho más que votar) podríamos decir: el fin de la democracia no es elegir una determinada decisión política, sino que lxs ciudadanxs se convenzan de que esa decisión fue tomada entre todxs y luego la haremos nuestra. Una de las demandas más escuchadas en esta crisis es que quienes gobiernan no solo nunca escucharon a la gente (salvo cuando hubo destrozos), sino que nunca se intentó siquiera hacer que los ciudadanos se hicieran partícipes de las decisiones que se tomaban allá arriba y luego las asumieran como propias. Los abogados le llaman a este tema legitimidad de la ley.[3] Ese es un problema político, no técnico. La tecnología codifica humanidad, pero no crea humanidad. Algo similar ocurre con la democracia. El destacado educador y filósofo John Dewey escribía que nos hemos acostumbrado a pensar que la democracia es una especie de mecanismo, pero es un modo de vida. La democracia no es algo hecho que se pueda traspasar o heredar; tiene que ser (re)creada por cada nueva generación. Nuestro rol es apoyar ese proceso, no intentar reemplazarlo. ▪

REFERENCIAS

[1] Robert Dahl. *La Democracia. Una guía para los ciudadanos.* Editorial Taurus, 1999. Cap. IV. ¿Qué es la democracia?

[2] Michel Balinski y Ridi Laraki. *Majority Judgement. Measuring, Ranking, Electing*. MIT Press, 2010.

[3] Sebastián Sichel. Diálogo Ciudadano. 30 de octubre de 2019. https://issuu.com/psegura/docs/di_logo_nacional_llamado_por_sichel

[4] Tim Berners-Lee. *World Wide Web – Past, Present, Future*. 2002. https://www.w3.org/2002/04/Japan/Lecture.html

[5] Sebastián Ureta. *Escuchar a la gente, pero en serio.* CIPER. 3 de diciembre de 2019. https://ciperchile.cl/2019/12/03/ escuchar-a-la-gente-pero-en-serio/

[6] E. Fernández Darraz. *El conflicto social y el modelo de desarrollo chileno.* El Mostrador. 5 de noviembre de 2019. https://www.elmostrador.cl/destacado/2019/11/05/el-conflicto-social-y-el-modelo-de-desarrollo-chileno/

[7] Alejandro Hevia. *El Camino hacia la Votación Electrónica Segura en Chile.* Presentado en el Senado de la República, 6 de julio de 2018. Diapositivas en: www.dcc.uchile.cl/ahevia/votacion-electronica-senado-2018-07-06.pdf

[8] Andreas Ladner y Joëlle Pianzola. *Voting Advice Applications*. Encyclopedia of Information Science and Technology. 3º Edición. Editorial IGI Global. 2015.

[9] Alejandro Hevia. *Votación electrónica y democracia.* Revista Bits de Ciencia Nº19, 2020. https://www.dcc.uchile.cl/Bitsdeciencia19.pdf

[10] Juan Carlos Mañalich. *Sobre la obligatoriedad de la ley.* El Mostrador. 5 de noviembre de 2019. https://www.elmostrador.cl/destacado/2019/11/05/sobre-la-obligatoriedad-de-la-ley-a-proposito-de-la-exhortacion-de-la-ministra-rubilar/

3 | Ver la columna "Sobre la obligatoriedad de la ley" de Juan Carlos Mañalich en *El Mostrador* [10]. Si por "ley" entendemos el conjunto de reglas a las que solemos atribuir "validez" jurídica, entonces la pregunta apunta a cómo explicar, si cabe explicar en lo absoluto, que las normas que conforman el derecho de un país lleguen a tener fuerza obligante, o "vinculante", sobre los individuos a quienes esas normas se encuentran "dirigidas".

¿Qué dice Twitter?

Redes sociales en tiempos de incertidumbre

MAGDALENA SALDAÑA

Profesora Asistente de la Facultad de Comunicaciones de la Pontificia Universidad Católica de Chile, e Investigadora del Instituto Milenio Fundamentos de los Datos. Sus áreas de investigación incluyen periodismo digital, redes sociales, comunicación política y estudios latinoamericanos. Ha publicado múltiples artículos en revistas de corriente principal, y su trabajo ha sido premiado en importantes congresos internacionales del área del Periodismo y la Comunicación.

En Twitter la encuentras como @magdalenasaldan.

El 18 de octubre de 2019 (de aquí en adelante, 18-O), la manifestación que comenzó con la evasión del pasaje del Metro detonó un proceso social que afectó todas las esferas de la vida pública y privada en Chile. Las redes sociales, que se han convertido en espacios de expresión para los usuarios de Internet, no han estado ausentes del estallido. Autoridades políticas, deportistas, líderes internacionales y figuras del espectáculo han manifestado su opinión sobre la situación del país usando sus redes sociales. Cada día, los *trending topics* de Twitter en Chile muestran al menos una tendencia relacionada con el movimiento social y las protestas, como **#RenunciaPiñera** o **#ChileDespertó** (Claro, 2019; El Mostrador, 2019), y los llamados "hilos" elaborados para entregar información u opiniones que no caben en 280 caracteres son cada vez más populares. Por su parte, muchos periodistas han usado sus cuentas para expresar abiertamente sus opiniones personales, aun cuando dichas opiniones reciban troleo y juicio por parte de sus seguidores. Las cuentas de Twitter de Mirna Schindler, Daniel Matamala y Mónica Rincón son buenos ejemplos de ello.

Instagram, por otro lado, se ha convertido en cantera inagotable de información visual sobre el movimiento. Videos grabados tanto por manifestantes como por profesionales de la prensa, infografías explicativas y cápsulas informativas de medios nacionales e internacionales se han difundido viralmente en esta red, ayudando muchas veces a la organización de reuniones y marchas. Ejemplos puntuales incluyen las imágenes y videos de **#LaMarchaMásGrandeDeChile**, que convocó a más de un millón de personas el pasado 25 de octubre (BBC News Mundo, 2019), o la rápida viralización de la performance del colectivo **#LasTesis**, que se replicó en distintos lugares del mundo y se tradujo a diversos idiomas (Francis, 2019). Instagram también ha funcionado como un repositorio de grafitis, rayados y afiches generados durante la protesta social. Para algunos, las intervenciones gráficas en muros o estatuas constituyen un daño a la ciudad y al patrimonio público; para otros, son una expresión artística legítima de los manifestantes (Valles & Espinoza, 2019). Tanto el debate sobre la legitimidad de los rayados como las imágenes en sí han viajado por las redes sociales a partir de las fotografías publicadas por los usuarios. Otros íconos visuales que se han viralizado en las redes son el Negro Matapacos y Baila Pikachu, transformándose en símbolos de las protestas durante el estallido.

El papel de las redes sociales, no obstante, ha ido más allá de la viralización de imágenes o la organización social. Numerosas organizaciones de derechos humanos han denunciado la excesiva violencia ejercida por las fuerzas de orden hacia los manifestantes, llegando a identificarse múltiples casos de violaciones a los derechos humanos (Amnesty International, 2019; Human Rights Watch, 2019). El registro de videos y fotografías por parte de los manifestantes ha sido de gran importancia en el proceso de documentación de las denuncias; tanto es así que *The New York Times* realizó un reportaje audiovisual sobre el estallido social en Chile a partir de material que la periodista Nilo Tabrizy solicitó abiertamente a usuarios chilenos a través de Twitter (Botti et al., 2019; Opazo, 2019). La foto con sangre brotando de los ojos del estudiante Gustavo Gatica (quien perdió la visión de ambos ojos tras ser herido por perdigones durante una manifestación en noviembre), es probablemente uno de los ejemplos más gráficos de la violencia durante las protestas.

Desde 2012 vengo estudiando sistemáticamente el uso e impacto de las redes sociales. Primero me enfoqué en cómo los periodistas utilizan plataformas como Twitter y Facebook para reportear e informar eventos noticiosos. Luego estudié cómo el uso de redes sociales incide en comportamientos sociales y políticos de los usuarios, tales como consumir noticias, votar, o participar en marchas. En los últimos años me he centrado en el uso de las redes sociales para discutir asuntos de interés público, poniendo especial atención al concepto de "troleo" en las conversaciones online. De aquí han salido aprendizajes útiles para entender parte de lo que ha ocurrido en las redes sociales del Chile post 18-O.

Redes sociales para la deliberación

El surgimiento de las redes sociales ofreció oportunidades que ninguna tecnología había entregado antes: un espacio para que cualquier usuario pudiese expresarse libremente, sin *gatekeepers*, sin intermediarios. A diferencia de las cartas al director, donde un tercero decide qué cartas son publicadas, las redes prometían que cualquier persona podría interpelar a un medio para manifestar su opinión sobre un hecho de interés, permitiendo a otras personas conocer dicha opinión, aplaudirla, o debatirla. El ideal *habermasiano* de deliberación pública parecía haber encontrado un escenario que daba lugar a todos los actores.

La creación de Facebook en 2004, YouTube en 2005, Twitter en 2006, WhatsApp en 2009 e Instagram en 2010 ha significado un aumento en las conexiones a Internet en Chile (principalmente desde dispositivos móviles), llegando a ser uno de los países con mayor penetración de redes sociales en América Latina. Según datos de la Subsecretaría de Telecomunicaciones, existen 91,9 conexiones móviles a Internet por cada 100 habitantes (Subtel, 2019), y se estima que el 77% de la población es usuario activo de alguna red social (We Are Social, 2019).

Además de permitir a los usuarios opinar libremente sobre temas de interés,

"La gente en redes sociales dice tal cosa", argumentamos, olvidando que nuestras redes sociales han sido sometidas a nuestra propia curatoría.

las redes sociales se han posicionado como un espacio de resistencia a los discursos de actores hegemónicos. Por ejemplo, la cobertura del estallido en los días inmediatamente posteriores al 18-O fue duramente cuestionada por la opinión pública, especialmente la cobertura televisiva. Se dijo que los noticiarios se empeñaban en mostrar los destrozos causados durante las protestas sin ahondar en las peticiones de los manifestantes. Más de alguna vez, periodistas realizando despachos en vivo fueron interpelados por ciudadanos molestos por el trabajo realizado hasta esa fecha (Lagos & Faure, 2019). Este malestar, sumado a la creciente desconfianza de la ciudadanía hacia los medios de comunicación, dio paso a una especie de cobertura informativa paralela, donde los usuarios de las redes sociales compartían videos grabados por sus celulares con imágenes que no se mostraban en los medios de comunicación tradicionales. Incluso hubo un llamado masivo a **#ApagarlaTele** e informarse por medios como Piensa-Prensa o Prensa Opal, espacios que se presentan como una opción a los medios informativos tradicionales.

No todo lo que brilla es oro

Sin embargo, existen numerosas problemáticas asociadas a los contenidos que circulan en redes sociales. Por un lado, la falta de un trabajo periodístico riguroso implica que contenidos no verificados o malinterpretados se viralicen rápidamente, desinformando a la población (como el caso de la bomba molotov que supuestamente fue lanzada desde un retén móvil de Carabineros hacia un edificio, y que en realidad fue un proyectil que rebotó en el vehículo). Por otro lado, usuarios que no se toman el tiempo para verificar la información que consumen, terminan compartiendo información errónea porque está en línea con sus propias creencias (el llamado *sesgo de confirmación*), lo cual evita que se cuestionen la veracidad de los contenidos compartidos (Del Vicario et al., 2017). Esto genera cadenas de desinformación que compiten con la información verificada por la prensa profesional.

En cuanto a espacios para opinión personal, la participación en redes sociales no es necesariamente deliberativa; muchas veces ni siquiera es constructiva. Al ser un espacio para la libre expresión, los comentarios posteados en redes sociales rápidamente pueden caer en la intolerancia, las funas, el ciberacoso y los discursos de odio (Papacharissi, 2004). Los estudios en la materia señalan que las personas expuestas a agresiones en redes sociales pueden sufrir traumas similares a los que causaría una agresión cara a cara (Chen, 2017). En otras palabras, el troleo online puede ser tan dañino como una interacción verbal entre personas compartiendo un mismo espacio físico.

¿Qué hacer? Algunas (posibles) soluciones

A mi juicio, el cultivar redes sociales diversas es tal vez la medida más fructífera para evitar las problemáticas ya descritas, pero es también la más difícil de implementar. Cuando una persona se rodea de quienes comparten sus opiniones (tanto en círculos online como offline) corre un alto riesgo de percibir

que su opinión representa el sentir de la mayoría. Por ejemplo, si estoy a favor de votar por una acción determinada, probablemente mis amigos y miembros de mi círculo más cercano también estén a favor. Si en redes sociales me rodeo de estas mismas personas, y además sigo a usuarios cuyo razonamiento y posición política/valórica se parecen a los míos, probablemente mis creencias se reafirmen una y otra vez, negando la existencia de posturas diferentes. En consecuencia, nunca me expongo a visiones distintas, y me cuesta creer que existan sectores que no piensen como yo. "La gente en redes sociales dice tal cosa", argumentamos, olvidando que nuestras redes sociales han sido sometidas a nuestra propia curatoría. Si mi inicio de Facebook o de Twitter está lleno de opiniones acordes a las mías, no significa que "la gente en redes sociales" esté de acuerdo conmigo; solo significa que "la gente" que yo misma he escogido como parte de mis redes sociales está de acuerdo conmigo, y los algoritmos que controlan dichas redes aprendieron de mis gustos personales y me muestran aquellos posteos a los que suelo darles like, o pasar más tiempo leyendo, comentando o compartiendo (Baekdal, 2016).

Si, en cambio, en un esfuerzo consciente por expandir el alcance y composición de mis redes sociales, decido no eliminar/bloquear/dejar de seguir usuarios cuyos comentarios me violentan, ya sea porque son abiertamente agresivos, o porque simplemente no estoy de acuerdo con lo que argumentan, y además decido seguir a usuarios con los cuales no tengo nada en común, mi red social se volverá más diversa y me obligará a exponerme a opiniones heterogéneas. Los beneficios de estas decisiones son múltiples: 1) estaré en contacto con puntos de vista que desconozco, 2) seré consciente de que mi opinión es una más en un abanico de opiniones que (como la mía) concentran apoyo de otros usuarios, 3) tendré la oportunidad de entender los argumentos que sustentan estas opiniones que no comparto, 4) podré desarrollar nuevos argumentos para defender mi punto de vista a la luz de discusiones que antes me eran ajenas. El resultado de estas interacciones no implica que yo cambie de opinión, pero sí que mis niveles de tolerancia hacia las ideas de otros se incrementen, y eventualmente se flexibilicen.

El troleo online puede ser tan dañino como una interacción verbal entre personas compartiendo un mismo espacio físico.

Este camino no está exento de dificultades. La exposición a opiniones en desacuerdo con un punto de vista puede generar rechazo y alejar a los usuarios de las conversaciones online. Si percibo que los niveles de violencia son demasiado altos (usuarios empleando insultos para atacar una postura) tendré menos inclinación a opinar. Algunos estudios muestran que ciertos usuarios se sienten motivados por estos ambientes, porque sienten una mayor necesidad de defender sus convicciones (Borah, 2014), pero no son la mayoría. La generalidad indica que cuando un usuario se enfrenta a una conversación respetuosa y deliberativa, las chances de que este usuario postee un comentario respetuoso se incrementan (Sukumaran et al., 2011). Por ende, la civilidad en las conversaciones es crucial y cada persona puede contribuir, intentando (en la medida de lo posible) corregir a quienes rompen el acuerdo tácito de lo socialmente aceptable en conversaciones online. Responder con más incivilidad, o llanamente bloquear a un usuario, no ayuda. Ya lo dice el meme del Amigo Gorila: "Todos tenemos un amigo gorila en Facebook. No lo elimines: edúcalo".

Otra estrategia para afrontar las problemáticas observadas en redes sociales es la educación. Existen universidades chilenas que han implementado asignaturas de desinformación para sus estudiantes, pero la instrucción en alfabetización mediática debería comenzar en estadios tempranos de la formación educativa. Es preocupante la falta de herramientas para discernir entre la información que es real y la que no lo es, o es engañosa, o incluso satírica. Una consecuencia positiva de la explosión de las llamadas *fake news* durante el estallido social es la proliferación de organizaciones académicas y periodísticas trabajando para chequear información en tiempos de incertidumbre. *Fake News Report* y la Red Estudiantil de Información, rei_chile, son ejemplos de *fact checkers* que trabajaron arduamente durante los primeros días del estallido clarificando información y desmintiendo contenido engañoso o equivocado. Pero combatir la desinformación no es tarea solo de los periodistas o de organizaciones de *fact checking*, sino de cada usuario que decide compartir información con sus redes. Por eso insisto en la necesidad de educar a las audiencias en el uso de redes sociales y el consumo de información. La utilización consciente e informada de plataformas sociales es primordial para evitar tanto las *fake news* como el troleo y los discursos de odio.

Epílogo: la importancia de tomar en cuenta las conversaciones online

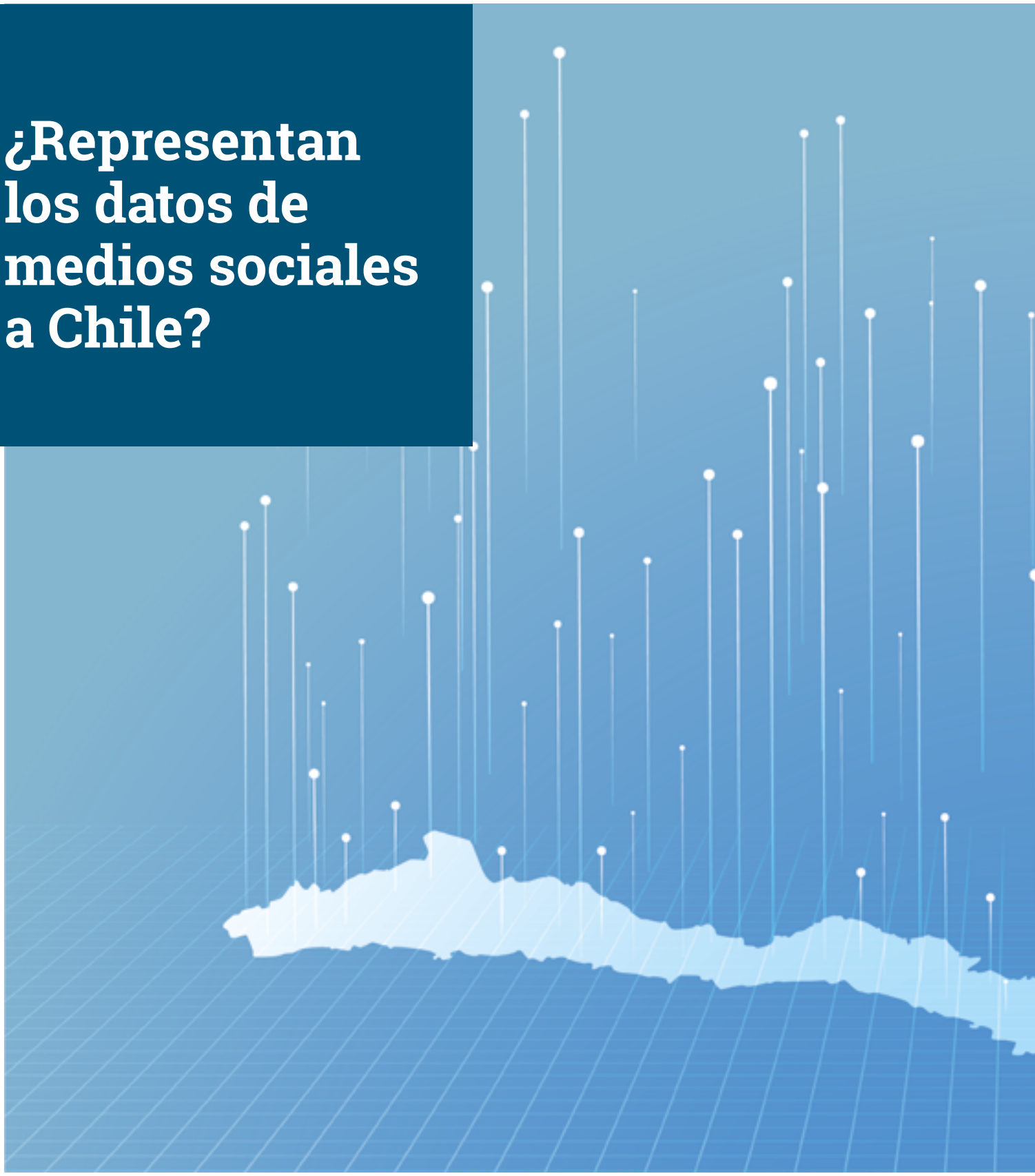
Las redes sociales pueden convertirse en esferas de resistencia, donde los individuos tienen la opción de contrarrestar las narrativas dominantes de los medios o de los grupos de poder al introducir narrativas alternativas en la

discusión. Sin embargo, no se puede generalizar lo observado en redes sociales al resto de la ciudadanía. Pese a la alta penetración de las redes en Chile, los usuarios que discuten la contingencia nacional en Twitter, Facebook o Instagram son una muestra no representativa de la población chilena. Esto no deslegitima la validez de considerar lo que las personas discuten en las redes sociales, las problemáticas que les aquejan y las soluciones que exigen. Las potencialidades de las redes sociales se han explotado al máximo durante el estallido social y son un insumo importante para entender la evolución del proceso social y político que estamos viviendo. Pero hay que observar estos discursos con cautela, y reconocer que muchas opiniones no están representadas en estos espacios. Al final del día, la interrogante de "¿qué dice Twitter?" solo apunta a eso: lo que dice la gente en Twitter. ▪

REFERENCIAS

- Amnesty International (2019). Chile: Amnesty International denounces human rights violations to the Inter-American Commission on Human Rights. *Amnesty International*. Recuperado desde https://www.amnesty.org/en/latest/news/2019/11/chile-amnistia-internacional-denunciara-violaciones-ante-cidh/
- Baekdal, T. (2016). How We Lost Social Media to Algorithms. *Baekdal Plus*. Recuperado desde https://www.baekdal.com/strategy/how-we-lost-social-media-to-algorithms/
- BBC News Mundo (2019). Protestas en Chile: la histórica marcha de más de un millón de personas que tomó las calles de Santiago. *BBC.com*. Recuperado desde https://www.bbc.com/mundo/noticias-america-latina-50190029
- Borah, P. (2014). Does it matter where you read the news story? Interaction of incivility and news frames in the political blogosphere. *Communication Research, 41*(6) 809–827.
- Botti, D., Koettl, C. & Tabrizy, N. (2019). Chile's Security Forces Have Injured Hundreds. See What the Videos Show. *The New York Times*. Recuperado desde https://www.nytimes.com/video/world/americas/100000006782083/chile-protests-riots.html?src=vidm
- Chen, G.M. (2017). *Online Incivility and Public Debate. Nasty talk*. Austin TX: Palgrave Macmillan.
- Claro, H. (2019). Cómo se vivieron los 60 días del estallido social chileno en Twitter. *El Dínamo.* Recuperado desde https://www.eldinamo.com/nacional/2019/12/18/estallido-social-60-dias-en-redes/
- Del Vicario, M., Scala, A., Caldarelli, G. et al. (2017). Modeling confirmation bias and polarization. *Scientific Reports, 7*, 40391.
- El Mostrador (2019). Los temas más comentados en Twitter durante el primer mes del estallido social. *El Mostrador*. Recuperado desde https://www.elmostrador.cl/agenda-pais/2019/11/25/los-temas-mas-comentados-en-twitter-durante-el-primer-mes-del-estallido-social/
- Francis, A. (2019). 'The rapist is you': why a viral Latin American feminist anthem spread around the world. *The Conversation*. Recuperado desde http://theconversation.com/the-rapist-is-you-why-a-viral-latin-american-feminist-anthem-spread-around-the-world-128488
- Human Rights Watch (2019). Chile: Llamado urgente a una reforma policial tras las protestas. *Human Rights Watch*. Recuperado desde https://www.hrw.org/es/news/2019/11/26/chile-llamado-urgente-una-reforma-policial-tras-las-protestas
- Lagos, C. & Faure, A. (2019). Periodismo precarizado: ¿puede/quiere la prensa proteger a los ciudadanos? *Ciper*. Recuperado desde https://ciperchile.cl/2019/10/31/periodismo-precarizado-puede-quiere-la-prensa-proteger-a-los-ciudadanos/
- Opazo, T. (2019). Cómo el New York Times usó las redes sociales para mostrar el estallido social en Chile. *La Tercera*. Recuperado desde https://interactivo.latercera.com/los-videos-del-estallido-social/como-el-new-york-times-uso-las-redes-sociales-para-mostrar-el-estallido-social-en-chile/
- Papacharissi, Z. (2004). Democracy online: civility, politeness, and the democratic potential of online political discussion groups. *New Media & Society, 6*(2), 259–283.
- Subtel (2019). Chile sube cinco lugares en ranking OCDE de penetración de accesos móviles a Internet. *Subtel*. Recuperado desde https://www.subtel.gob.cl/chile-sube-cinco-lugares-en-ranking-ocde-de-penetracion-de-accesos-moviles-a-internet/
- Sukumaran, A., Vezich, S., McHugh, M., & Nass, C. (2011). Normative influences on thoughtful online participation. In *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems - CHI '11* (pp. 3401–3410). New York, New York, USA: ACM Press.
- Valles, P. & Espinoza, D. (2019). Protesta en los muros: grafitis, rayados y afiches en el estallido social. *Culto*. Recuperado desde https://culto.latercera.com/2019/11/16/protesta-rayados-muros/
- We Are Social (2019). Digital 2019: Global Digital Yearbook. *Datareportal*. Recuperado desde https://datareportal.com/reports/digital-2019-chile?rq=chile

¿Representan los datos de medios sociales a Chile?



RICARDO BAEZA-YATES

Director tecnológico de NTENT, empresa de tecnología de búsqueda semántica basada en California, director de los programas de postgrado en ciencia de datos de la Northeastern University, sede Silicon Valley e investigador senior del Instituto Milenio Fundamentos de los Datos. Profesor del Departamento de Ciencias de la Computación de la Universidad de Chile. PhD en ciencia de la computación por la Universidad de Waterloo, Canadá. Sus áreas de investigación son búsqueda en la Web, minería de datos y algoritmos. Es ACM Fellow e IEEE Fellow.

http://www.baeza.cl/

Desde el estallido social del 18 de octubre de 2019, los medios sociales en Internet (*social media* en inglés) y particularmente Twitter, han sido usados para tratar de entender las motivaciones y opiniones de los chilenos, culminando con el escándalo del famoso informe de big data que recibió el Gobierno. Motivado por estos hechos, en este artículo analizamos los sesgos de los datos de los medios sociales y si es posible mitigarlos para que realmente representen la opinión del país. También de paso explicamos qué son los datos masivos (big data en inglés) y mostramos cómo incluso datos correctos pueden ser manipulados para difundir información falsa. Una presentación preliminar basada en estas ideas se puede encontrar en [2].

Datos masivos y medios sociales

Wikipedia define datos masivos o macrodatos de la siguiente manera: *"Macrodatos es un término que hace referencia a conjuntos de datos tan grandes y complejos como para que hagan falta aplicaciones informáticas no tradicionales de procesamiento de datos para tratarlos adecuadamente"*. Esta definición es bastante abstracta pues no nos dice a partir de qué tamaño son masivos ni cuán complejos deben ser. Por esto se usan las siguientes características para precisar esta definición:

- ***Volumen***: la cantidad de datos generados y guardados.
- ***Variedad***: el tipo y naturaleza heterogénea de los datos.

Cualidad	Problemas de datos	Problemas de computación	Problemas humanos
Volumen	escala, **redundancia**	escalabilidad	sobrecarga de información
Variedad	heterogeneidad, complejidad	adaptabilidad, extensibilidad	complejidad
Veracidad	exhaustividad, **sesgo, escasez, ruido, spam**	fiabilidad, confianza	**sesgo, escasez, ruido, spam**
Velocidad	tiempo real (instantáneo)	en línea (menos de unos segundos)	sobrecarga de información
Valor	utilidad, **privacidad**	depende del objetivo	**privacidad, ética y legalidad**

Figura 1. Características distintivas del big data y problemas asociados a cada una de ellas.

Medio social	¿Datos públicos?	Usuarios chilenos	Penetración aproximada
Facebook	pocos	13,0M*	71%
WhatsApp	ninguno	12,4M	68%
YouTube	muchos	11,7M	64%
FB Messenger	ninguno	7,3M	40%
Instagram	bastantes	7,0M*	38%
LinkedIn	muchos	4,8M	26%
Twitter	**todos**	1,5M*	8%
Snapchat	pocos	1,1M*	6%

Figura 2. Penetración de los medios sociales más populares en Chile.

- ***Velocidad***: tasa a la cual se generan y procesan los datos.
- ***Veracidad***: calidad de los datos obtenidos.
- ***Valor***: los datos obtenidos deben ser útiles y accionables.

[Además de los sesgos de género, edad y demografía] los datos de Twitter tienen otros sesgos, empezando con que representan a menos del 20% de la población.

Notar que aunque tengamos datos masivos, éstos no necesariamente son big data si ellos no son veraces o no tienen relación (valor) con el análisis que queremos realizar. En cada una de estas dimensiones, hay problemas inherentes a los datos, al procesamiento informático de los mismos y a las personas que los usan, como mostramos en la Figura 1, donde hemos destacado con negrita los más importantes.

En base a esta definición, no es difícil concluir que la mayoría de las organizaciones (empresas, instituciones, etc.) no tienen big data y nunca lo tendrán pues no cumplen con alguna de las tres primeras V's (ver Figura 1). De hecho, personalmente opino que el verdadero problema hoy son los datos normales, pequeños o *small data,* pues así más organizaciones podrían tener la posibilidad de aprovechar los avances en aprendizaje automático y minería de datos [1, 7].

Por otro lado, ciertamente los datos de medios sociales cumplen con las tres primeras V's y si son bien usados, también son veraces y tienen valor. Esto sigue siendo válido si nos circunscribimos a Chile. Sin embargo, cuando el análisis es realizado con una muestra de datos en un segmento de tiempo predeterminado, deja de ser big data, pues ya no posee velocidad.

La Figura 2 muestra los ocho medios sociales más usados en Chile a comienzos de 2019 [4], donde algunos son redes sociales implícitas (es decir, suponemos que si una persona conoce la identidad de otra persona, están conectados), destacadas en negrita. También mostramos la penetración de cada una de ellas considerando una población de 18,3 millones que da una penetración de Internet del 82% (15 millones de personas conectadas) que baja al 77% si consideramos usuarios activos en medios sociales (14 millones) y al 71% si solo consideramos teléfonos celulares (13 millones) [4]. Las cifras marcadas con un "*" se han calculado usando la audiencia para publicidad en Internet que representa los usuarios activos mensuales y no el número total de usuarios, a excepción de LinkedIn donde se consideran todos los usuarios chilenos registrados. También indicamos si los datos son públicos o no, destacando que Twitter es el único medio completamente público. Finalmente, recalcamos que cuatro de los cinco primeros medios sociales pertenecen a Facebook, a excepción de YouTube que pertenece a Google.

Todos estos números anteriores son aproximados por diversas razones. Primero, solo cada medio sabe exactamente el número de usuarios registrados y activos por mes en cada país. Segundo, estos usuarios incluyen organizaciones y *bots* (usuario que es un agente de software) que no son personas, además de individuos que pueden tener más de un perfil.

Sesgos demográficos en medios sociales

Si consideramos que hay 14 millones de usuarios activos en medios sociales (77%), estos usuarios también tienen sesgos demográficos. Si comparamos los porcentajes de hombres y mujeres por rangos de edad considerando la estimación de usuarios activos de Hootsuite [4] (incluyendo un ajuste de 0,7% por una suma incorrecta que da sobre el 100%) y las estimaciones a partir del

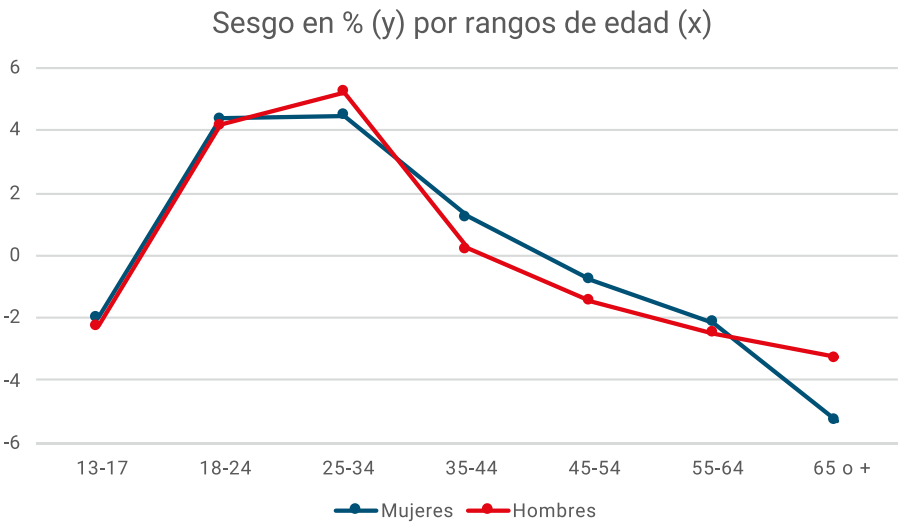


Figura 3. Sesgo de participación entre hombres y mujeres en una muestra de datos de Twitter.

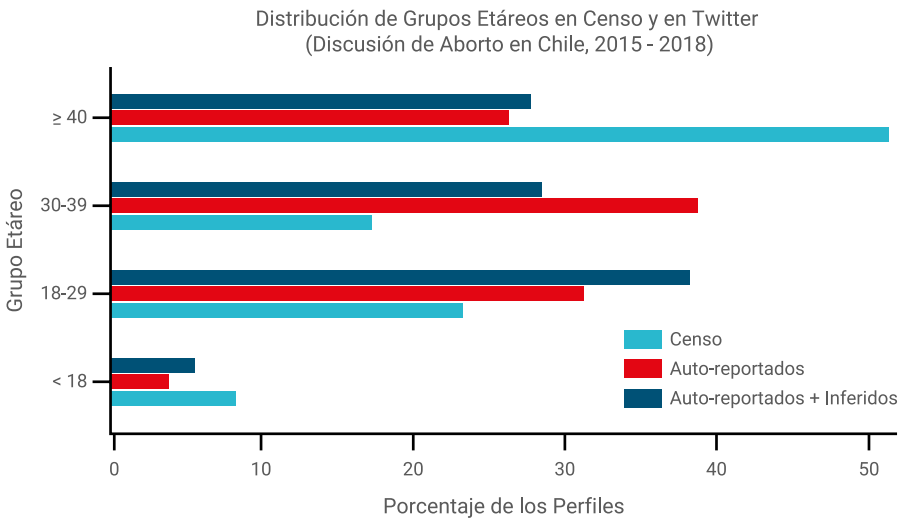


Figura 4. Perfil de los distintos grupos etáreos en Twitter (auto-reportados y autoreportados + inferidos) y en la población general chilena (censo de 2017).[1]

último censo [8], obtenemos las diferencias para personas de al menos 13 años (que excluye al 8.6% de la población) en la Figura 3.

Como podemos ver, entre 18 y 44 años (y particularmente entre 18 y 34) tenemos una sobrerrepresentación mientras que en el resto es lo opuesto. También los hombres están más representados que las mujeres en general (un 9% más en el rango de 25 a 34 años y 17% más para mayores de 64 años), pero en el rango de 35 a 64 años, son las mujeres las que están sobrerrepresentadas en mayor medida.

Considerando que la mayoría de las redes sociales son principalmente privadas, usar los datos que son públicos sesga cualquier muestra a personajes públicos o extrovertidos y en general solo temas de interés público, entre otros. Por esta razón, la mayoría de los análisis de medios sociales usa Twitter, donde potencialmente todos los datos son públicos.

Sesgos de datos en Twitter

Por supuesto los datos de Twitter tienen otros sesgos, empezando con que representan a menos del 20% de la población, ya que el número de usuarios registrados chilenos es menor a 3,5 millones si consideramos los seguidores de los medios de comunicación más populares, lo que es una cota superior de los usuarios registrados. Por otro lado, solo podemos conseguir datos de usuarios activos y, por lo tanto, considera a menos del 10% de los chilenos.

Respecto a los sesgos demográficos ya mencionados, el sesgo de género en Twitter es más pronunciado que en el promedio de todas las redes sociales, pues se estima que solo el 29% de los usuarios son mujeres [4]. Este sesgo de género es el primero que hay que mitigar, seguido de los sesgos de edad.

Otro sesgo de Twitter es que los datos de la API pública (interfaz para solicitar datos) son ya una muestra y no sabemos si Twitter los selecciona aleatoriamente o hace algún tipo de filtrado por temas (por ejemplo, eliminando contenido adulto o de incitación al odio). Además para seleccionar contenido muchas veces se usan palabras claves (*e.g.*, "estallido social") o términos temáticos (*hashtags*, e.g., "**#chiledesperto**") y por supuesto esto deja fuera a todos los usuarios que no usan estas palabras claves o términos temáticos, normalmente por pereza o ignorancia, lo que es común en personas que no se preocupan o no saben usar bien la tecnología.

Mitigando sesgos demográficos

Una forma de mitigar los sesgos demográficos es segmentar la muestra y sopesar cada segmento para que represente la población real. Esto es lo que hicimos en [3] para contrastar los cambios de opinión en Twitter con respecto al proceso de legislación sobre la ley que despenaliza el aborto en Chile y compararlos con los de la población en general. Para ello usamos los usuarios que indicaban su género y edad para entrenar modelos basados en aprendizaje automático para predecir el género y rango de edad para el resto de los usuarios. Luego sopesamos su opinión (a favor o contra el aborto) y la comparamos con la encuesta CEP de este tema en 2017, encontrando un error de solo 3% para las mujeres y de 7% para los hombres.

En la Figura 4 mostramos el proceso de mitigación para la edad, donde los datos de entrenamiento (auto-reportados) han sido usados para predecir el resto de la muestra, comparando el resultado con los datos del censo de 2017 [6].

1 | Agradecemos a Eduardo Graells por la realización de este gráfico.

Aquí vemos que los menores de 18 y los mayores de 39 están subrepresentados y, por lo tanto, se necesita multiplicar por un factor mayor a 1, mientras que entre 18 y 39 están sobrerrepresentados y necesitamos multiplicar por un factor menor que 1. En el caso de género encontramos que el 55,7% de la muestra eran hombres y 43,3% mujeres (mayor al mencionado anteriormente, seguramente por el tema en discusión, el aborto). Considerando que en el censo el 48,6% eran hombres y 51,4% mujeres, tenemos que multiplicar por 0,87 la opinión de los hombres y por 1,19 la de las mujeres, para que sean representativas.

Incluso los datos correctos pueden ser manipulados

En 1907, Mark Twain en su autobiografía, menciona que "hay tres tipos de mentiras: mentiras blancas, mentiras malditas y estadísticas", atribuyendo este texto erróneamente al primer ministro británico Disraeli. Esta frase describe el poder persuasivo de los números, el cual puede usarse para todo tipo de fines [5]. En los años sesenta, durante una charla en la Universidad de Virginia, el premio Nobel de economía de 1991, Ronald Coase, dijo que "si torturamos los datos el tiempo suficiente, ellos confesarán lo que queramos". Esto puede ser hecho de una manera burda, de una manera sutil o incluso sin

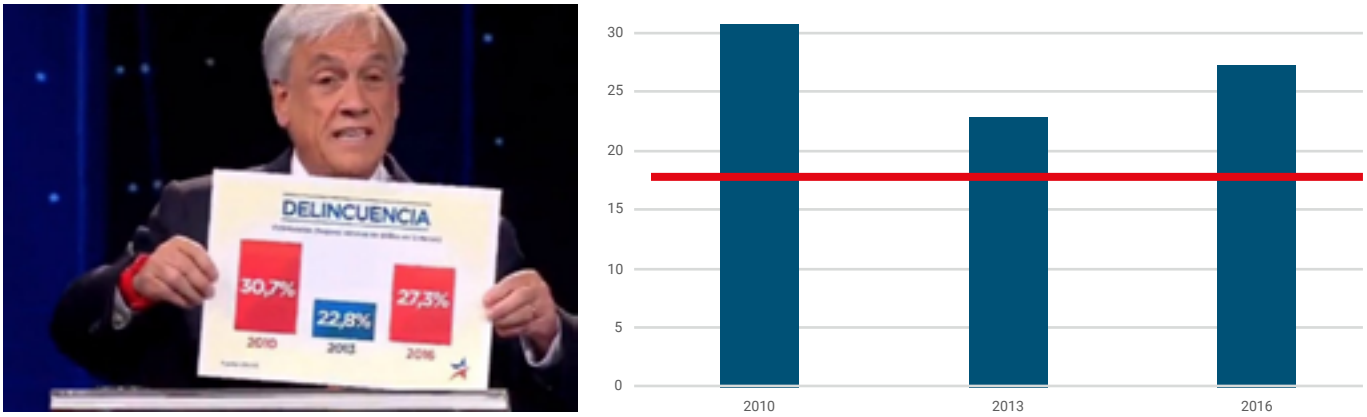


Figura 5. Izquierda: gráfico comparativo sobre delincuencia mostrado por Sebastián Piñera en el debate presidencial de 2017. Derecha: gráfico en su escala "real".

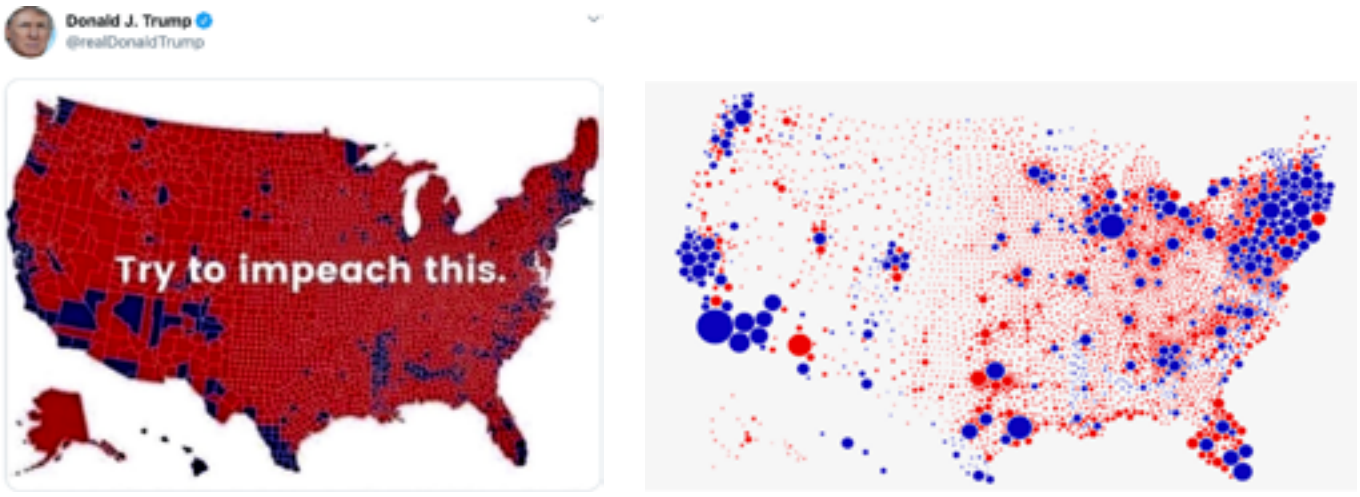


Figura 6. Izquierda: Mapa publicado por Donald Trump mostrando su apoyo en Estados Unidos. Derecha: Mapa ponderado por la densidad poblacional.

"Si torturamos los datos el tiempo suficiente, ellos confesarán lo que queramos". Ronald Coase, premio Nobel de economía.

intención. Veamos algunos ejemplos, enfatizando que datos no es lo mismo que información.

Durante un debate presidencial en 2017, Sebastián Piñera mostró el gráfico a la izquierda de la Figura 5 sobre cifras de delincuencia, donde el número durante su primer mandato parece ser la mitad de los números durante los gobiernos de Michelle Bachelet. Por supuesto esto no es efectivo pues 22,8% no es la mitad de 27,3%. Para que se visualice esto de esa manera, se ha elegido comenzar las barras desde el 18% en vez del 0, como lo muestra el gráfico de la derecha.

En octubre de 2019, el presidente de Estados Unidos, Donald Trump, publicó un tweet con el mapa a la izquierda de la Figura 6, que visualmente hace parecer que la mayoría de la población de ese país lo apoya. Sin embargo, esto supone que la densidad de población es uniforme, lo que no es cierto en ningún país. Si convertimos este mismo mapa a esferas que indican el tamaño de la población, como el que mostramos al lado derecho, vemos que la ilusión de mayoría se desvanece.

Finalmente, incluso cuando todo parece estar correcto, podemos engañarnos. Consideren el gráfico de la Figura 7 que muestra la influencia de 250 usuarios de mayor a menor (por ejemplo, el número de seguidores en Twitter). Ésta es una típica distribución de ley de potencias donde hemos incluido un 5% de usuarios extranjeros que están destacados en rojo. Escojamos ahora calcular la influencia extranjera en los 20 usuarios más populares (noten que normalmente se escogen múltiplos de 10, un sesgo antropomórfico, que es algo completamente arbitrario). Si ahora calculamos la suma de los seguidores de usuarios extranjeros comparados con los usuarios chilenos en los 20 primeros, obtenemos una influencia del 20,8%. ¿Preocupante, no?

¿Dónde está el engaño? Bien, este porcentaje en realidad depende de cuántos usuarios populares escogemos. De hecho, si hubiéramos elegido 19, habríamos encontrado el máximo posible, 21,4%. El gráfico de la Figura 8 calcula el porcentaje de influencia extranjera dependiendo del número de usuarios populares que escogemos. Si usamos los 250, llegaríamos al valor correcto que es el mínimo, 11,3%. Por supuesto, otra falacia de este análisis es suponer que seguir a alguien significa ser influenciado por esa persona, pocas veces ocurre esto e incluso muchas de las personas a las que seguimos opinan exactamente lo contrario a nosotros, pero los seguimos porque nos interesa conocer la opinión contraria. Volveremos a esto antes de terminar.

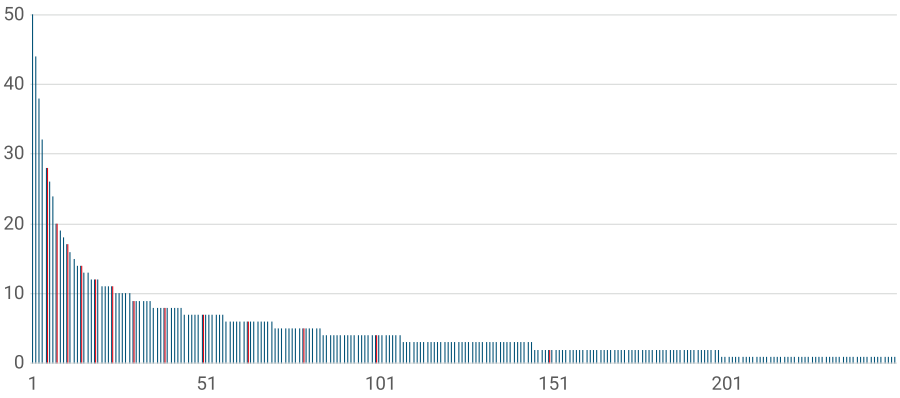


Figura 7. Influencia (medida en cantidad de seguidores) de 250 usuarios ficticios. Las barras en rojo representan usuarios extranjeros.

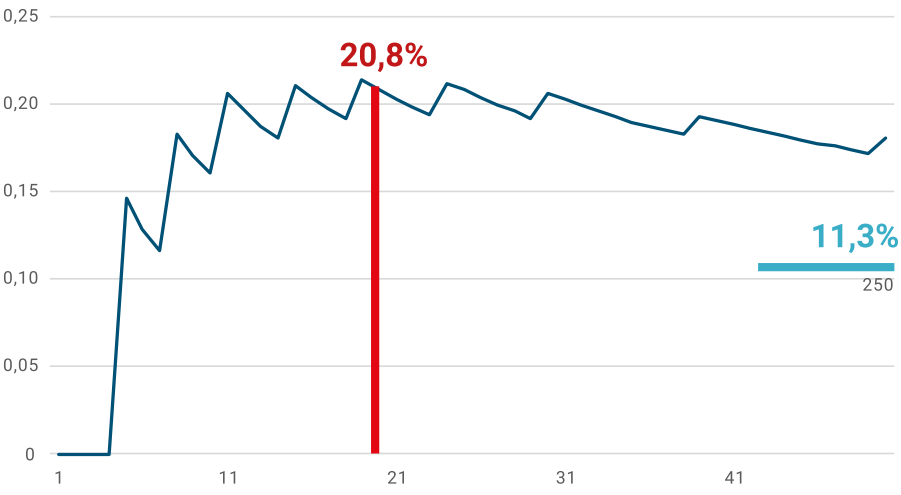


Figura 8. Fracción extranjera (eje vertical) dependiendo del número de usuarios influyentes seleccionados (eje horizontal).

Para recordar

Volviendo al famoso informe de big data, este suceso muestra también otras suposiciones que mucha gente hace sin ninguna justificación, claramente retratadas por las noticias en la Figura 9. Primero, asociación (o correlación) no implica causalidad. Por ejemplo, no es extraño que manifestantes jóvenes gusten del K-Pop, pues es un gusto típico para su edad. De allí al hecho de que eso implique una influencia coreana hay mucho trecho. Segundo, que personalidades de la música aparezcan, no significa que sean importantes, ya que presencia no siempre implica influencia. Finalmente, presencia tampoco implica tendencia, ya que podemos seguir a muchas personas de tendencias opuestas y, por lo tanto, suponer que toda posible influencia tiene el mismo mensaje es una generalización simplista y errónea.

En marzo de 2019, durante un evento en Stanford en el que participé, el famoso historiador israelí Yuval Harari dijo: "Las personas más fáciles de manipular son las que creen que no pueden ser manipuladas". Así que la próxima vez que su sesgo de confirmación le haga creer que lo que le están comunicando es cierto, recuerde esta frase e intente vencer sus sesgos cognitivos. ■

Figura 9. Selección de noticias relacionadas con el informe del big data.

Nota: Después de escribir este artículo, Alto Analytics publicó lo que parece ser un resumen del informe de big data para Chile y Colombia, el que contiene muchos errores conceptuales y analíticos, incluyendo los sesgos demográficos y el de la Figura 8. Mi análisis de este estudio se puede encontrar en Los Asombrosos Errores del Análisis de Redes Sociales Chilenas de Alto Analytics, Medium, febrero 2020, https://medium.com/@rbaeza_yates/los-asombrosos-errores-del-2b0225c2e622.

REFERENCIAS

[1] R. Baeza-Yates. BIG, small or Right Data: Which is the proper focus? KDnuggets. 2018. https://www.kdnuggets.com/2018/10/big-small-right-data.html

[2] R. Baeza-Yates. ¿Representan los medios sociales a Chile? XI Encuentro Sociedad y Tecnologías de la Información. 2020. https://www.elperiodista.cl/encuentro-big-data-y-social-media/

[3] E. Graells-Garrido, R. Baeza-Yates, M. Lalmas. How Representative is an Abortion Debate on Twitter? ACM Web Science, Boston. 2019. https://dl.acm.org/doi/10.1145/3292522.3326057

[4] Hootsuite & We Are Social. Digital 2019 in Chile. 2019. https://www.slideshare.net/-DataReportal/digital-2019-chile-january-2019-v01

[5] D. Huff. How to Lie with Statistics. W. W. Norton & Company. 1993.

[6] Instituto Nacional de Estadísticas. Censo 2017. 2018. http://www.censo2017.cl/microdatos/

[7] M. Lindstrom. Small Data: The Tiny Clues that Uncover Huge Trends. St Martin's Press, New York, EE.UU. 2016.

[8] Population Pyramid. Pirámide demográfica de Chile. 2019. https://www.populationpyramid.net/-chile/2019/

Votación electrónica y democracia

ALEJANDRO HEVIA

Profesor Asistente del Departamento de Ciencias de la Computación de la Universidad de Chile. Director del Laboratorio de Criptografía Aplicada y Ciberseguridad, CLCERT. Doctor en Computación por la Universidad de California, San Diego. Sus intereses de investigación incluyen criptografía aplicada y seguridad computacional.

ahevia@dcc.uchile.cl

"El derecho a voto es un derecho básico sin el cual todos los otros carecen de sentido. A las personas, a los individuos, les entrega control sobre sus propios destinos". Lyndon B. Johnson.

Introducción

La elección democrática de nuestros representantes es probablemente hoy en día uno de los procesos sociales colectivos más importantes en una sociedad. Debatida, amada y frecuentemente vilipendiada, la elección de representantes requiere de legitimidad, esto es, no solo debe cumplir objetivos como participación ciudadana, facilidad y libertad de ejercer el derecho, sino debe proveer transparencia y confianza. En otras palabras, debe ser convincente. "El propósito de un sistema de votación no es nombrar al ganador, sino convencer al perdedor" habría dicho Dan Wallace, académico de la Universidad de Princeton. La legitimidad entonces debe cumplirse con respecto a todos (o la gran mayoría de) los participantes, tanto los involucrados directamente en el proceso eleccionario como de los que no, dado que su resultado tiene efectos para toda la sociedad.

Alcanzar los objetivos, sin embargo, depende crucialmente del sistema de votación, esto es, el mecanismo o procedimiento, utilizado para lograr la elección. Por ejemplo, un sistema de votación a mano alzada es simple y fácil de usar, pero no escala cuando la comunidad crece. Peor aún, este sistema revela la preferencia individual (el voto) de cada ciudadano, dando pie a posible intimidación y compra de votos, coartando así la libertad de votar por una preferencia. El sistema actual de votación chileno lo hace posiblemente mejor: cada ciudadano toma un papel preimpreso donde aparecen todos los candidatos (denominado la "papeleta australiana") y marca allí su preferencia en forma secreta con un lápiz. Luego, la papeleta es despojada de toda referencia al votante y depositada en una urna, donde se confunde o mezcla con las otras papeletas. El conteo de votos luego se hace en forma pública, abriendo la urna en presencia de participantes que velan por el correcto desarrollo del conteo. El sistema también contempla un paso previo, menos mencionado pero no por eso menos importante: el manejo del registro electoral. Esto incluye tanto la inscripción inicial de los votantes (por el votante cuando es voluntaria, o por la agencia estatal a cargo cuando es obligatorio) así como la mantención del registro (muertes, cambios de domicilio, etc.).

Desafortunadamente, los procesos basados en papel como el chileno son frecuentemente vistos con desdén en una era donde los teléfonos inteligentes están en todos lados e Internet juega un rol central en la vida de las personas. ¿Si podemos usar nuestros computadores para hacer transacciones bancarias, participar remotamente en reuniones, e incluso hacer cirugías médicas en forma segura, por qué no podemos votar usando computadores en forma segura? Como veremos, la respuesta a esta pregunta requiere un análisis más complejo de lo sospechado a primera vista.

El objetivo de un sistema de votación

En principio, un sistema de votación pareciera ser algo simple ¡solo debemos contar! En realidad, un sistema de votación es un proceso complejo por la combinación de requerimientos aparentemente contradictorios que nos demanda. Desde un punto de vista funcional, un sistema de votación debe cumplir los siguientes requisitos:

1. ***Integridad:*** el resultado de la elección debe coincidir con las intenciones de voto de los votantes. Tal requerimiento usualmente se divide en dos condiciones (a) el voto es emitido (registrado) de acuerdo a la preferencia del votante, y (b) los votos son contados considerando las preferencias registradas.

2. ***Secreto del voto:*** nadie puede saber cómo votó un votante. Frecuentemente, se pide incluso algo más fuerte; nadie puede saber cómo votó **aún si el votante** desea revelarlo.

3. ***Autentificación de los votantes:*** solo los votantes autorizados pueden emitir votos, pero cada votante puede hacerlo solo una vez.

4. ***Derecho a voto:*** todas las personas autorizadas tienen la oportunidad de votar.

5. ***Disponibilidad:*** el sistema de votación debe ser capaz de (a) aceptar todos los votos emitidos durante un periodo pre-especificado, y (b) producir resultados razonables después de un periodo razonable.

Diseñar sistemas de votación es complejo pues los requerimientos anteriores están en tensión: por ejemplo, la integridad del sistema y la privacidad de los votos[1], o la autentificación de los votantes con el derecho a voto.

Peor aún, todo sistema de votación no ocurre en un ambiente ideal, con ciudadanos ejemplares y candidatos honestos. Un sistema de votación es usado para una elección concreta, la cual tiene amenazas, personas y entidades (adversarios) que desean atacar o usar el siste-

1 | Por ejemplo, la votación a mano alzada es obviamente correcta pero no privada.

Figura 1. "La Elección en el Condado, 1852", G.C. Bingham, pintor norteamericano 1811–1879; Museo de Arte de Saint Louis. Muestra la naturaleza caótica de una elección en 1800, incluyendo acarreos y compra de votos en un proceso a viva voz.

Fuente: Wikipedia, dominio público.

ma en su beneficio. Candidatos que desean ganar a toda costa, o sus mismos votantes quienes pueden querer alterar los votos de otros o vender sus propios votos, funcionarios encargados de ejecutar el sistema pero excesivamente politizados que pueden desear ver ganador a un cierto candidato, los fabricantes de algunas de las partes tecnológicas del sistema utilizado, o incluso potencias extranjeras posiblemente afectadas por el resultado que desean manipularlo o desacreditarlo (ver Figura 1).

El tipo de amenazas es crucial para evaluar un sistema de votación. Una elección gremial, o estudiantil pequeña, es considerada de "bajo perfil" puesto que quien gane o pierda es poco relevante para actores poderosos que pudieran montar ataques significativos. Probablemente pueda llevarse a cabo en forma segura utilizando un sistema de votación relativamente simple.

La efectividad y severidad de los ataques que reciba estarán acotados, simplemente porque las amenazas serán pequeñas: tanto los candidatos, como los votantes o incluso observadores externos serán probablemente poco sofisticados o tendrán financiamiento limitado, por lo que explorarán maneras simples de alterar la votación. Una elección de "alto perfil" cambia necesariamente esta dinámica. Tal elección sería, por ejemplo, una de nivel nacional, del tipo presidencial o parlamentaria, o incluso local pero significativa, como la de alcaldes. En tal tipo de elección, el sistema de votación debe resistir amenazas más potentes y complejas, esto es, ataques de adversarios mejor financiados, técnicamente más hábiles, y de escala mayor.

¿En qué consiste la votación electrónica?

En general, un sistema de votación electrónica es un sistema de elecciones que utiliza un computador en forma sustantiva en alguna de sus fases. Ahora bien, hoy por hoy, todos los sistemas involucran algún sistema computacional[2] así que es necesario precisar nuestra definición. Llamaremos votación electrónica a todo sistema donde computadores son utilizados en forma exclusiva en algún paso de la votación, ya sea en el proceso de capturar una preferencia ("votar" o transformar una preferencia mental en una marca en una papeleta) o en el proceso de transmitir o contar los votos, descartando el proceso de registro.

Los sistemas de votación mecánicos existen desde fines de 1800. Sistemas basados en procesos mecánicos con palancas y engranajes *(lever machines)*, y en papel perforado manualmente *(punch-card systems)* siguieron en uso hasta inicios de este siglo, siendo populares en Estados Unidos. Los sistemas propiamente electrónicos basados en componentes computacionales comenzaron a usarse en la década de 1960 en la forma de escáners para leer formularios llenados manualmente. Recién en la década de 1970 surgen los primeros computadores utilizados para registrar y contabilizar los votos.

Una primera distinción: remota versus presencial

Frecuentemente el ciudadano común entiende por "votación electrónica" a la votación remota, esto es, al sistema donde emitir el voto es hecho en computador pero en forma remota respecto

2 | En Chile, por ejemplo, el sistema de registro de votantes y el sistema de recopilación preliminar de conteos utilizan computadores.

Figura 2. Escáner usado para leer papeletas de votación en la forma de formularios.

Fuente: Wikipedia.

Figura 3. Computador marcador de papeletas: solicita las preferencias al usuario y luego las imprime en una papeleta de votación.

Fuente: Wikipedia.

Figura 4. Máquina de tipo DRE usada en Estados Unidos.

Fuente: Verified Voting Foundation.

al lugar donde se cuentan los votos, y donde la transmisión de las papeletas con las preferencias registradas es hecha por una red computacional. En otras palabras, votar en un computador o teléfono inteligente en la casa. Si esta red es Internet, hablaremos de votación por Internet.

La votación electrónica puede ser también presencial *(pollsite)* sin embargo. Esto es, puede ocurrir en un recinto de votación físicamente protegido y monitoreado al cual los votantes acceden en persona, y donde el computador ayuda al votante ya sea a emitir y/o contar los votos. Discutiremos este tipo, históricamente más antiguo, a continuación.

Los inicios de la votación electrónica

La variante más antigua de votación usando computadores tal como los entendemos hoy, toma la forma de escáners. En ella, los votantes llenan (usualmente en forma manual) una papeleta con sus preferencias o votos. Esta papeleta, denominada *"optical-scan ballots"*, toma la forma de un formulario legible por un computador, por ejemplo, con óvalos en blanco como los utilizados en las pruebas de selección universitaria. Luego, un computador (un escáner) utiliza una cámara para leerlas ópticamente, calculando el conteo o almacenando localmente los totales parciales (ver Figura 2). Con la llegada de interfaces gráficas y táctiles, los computadores también empezaron a ser usados para interactuar con el votante, obtener sus preferencias y permitirle más fácilmente producir (imprimir) la papeleta llena, previo al conteo (ver Figura 3).

En retrospectiva, los computadores pasaron desde ser usados solo para contar papeletas (calcular el total), a ser usados también para generar las papeletas completas. No es sorprendente que el siguiente paso fuera hacer ambos simultáneamente, sin imprimir la papeleta. La máquina de "Captura y almacenamiento electrónico directo", o DRE por su sigla en Inglés (Direct-Recording Electronic machine) es posiblemente la implementación más directa de un sistema de votación electrónico usando íntegramente un computador (ver Figura 4). Frecuentemente usando una interfaz gráfica, el DRE despliega opciones o candidatos desde donde el votante escoge sus preferencias. En teoría, su selección es registrada y almacenada en forma interna, en memoria o disco. Al finalizar la elección, el conteo puede realizarse en el mismo DRE y/o la información de los votos o totales transmitirse a un servidor central. La transmisión puede hacerse vía tarjetas de memoria, USB, o incluso utilizando una red computacional.

Los sistemas DRE siguen siendo muy populares en Estados Unidos y en el mundo pese a las dificultades que mencionaremos a continuación.

Muchos ataques y pocas defensas

"Lo que realmente cuenta no son las personas que votan, sino las personas que cuentan los votos". Atribuido a José Stalin.

¿Cómo sabemos si un sistema es seguro? Intuitivamente, debe cumplir los requerimientos mencionados anteriormente. Claramente, si existe un ataque que viola alguno de ellos, no es seguro.

Existen ataques documentados a varios sistemas basados en escáners donde el total puede ser manipulado si el atacante llegara a tener acceso limitado a los escáners [Kiayas et al. 2006]. Pese a estas noticias, en la práctica los sistemas basados en escaneadores son, entre todos los sistemas que utilizan computadores, probablemente los más fáciles de "segurizar" hoy en día. Basta notar que

su operación produce naturalmente una traza verificable en papel (esto es, el formulario lleno) cuya correctitud puede ser verificada directamente por el votante en forma manual antes de ser contada por el computador. Suponiendo un manejo adecuadamente seguro de las papeletas, cualquier problema es corregible; basta recontar las papeletas. Lamentablemente, en la práctica no siempre es posible, como observaremos luego.

En general, la seguridad de los dispositivos DRE ha sido paupérrima. Desde inicios del 2000, los ataques documentados a estos sistemas han sido numerosos y devastadores. Por ejemplo, investigadores de Princeton en 2006 mostraron serios ataques al sistema "Diebold Accuvote TS". Un votante con un breve acceso físico a la máquina era capaz de alterar el programa de la máquina cambiando los totales en forma indetectable. Peor aún, el atacante podría crear un virus (malware) capaz de infectar otras máquinas y el sistema de conteo central [Feldman et al. 2006]. Diversos otros ataques han sido documentados para sistemas similares, desde violación del secreto del voto vía emanaciones electromagnéticas de un sistema en Holanda [Gonggrijp et al. 2007] hasta instalar juegos en el sistema (DEFCON hacking village 2018).

Diseñar sistemas DRE seguros ha resultado extremadamente difícil aún si son simples. Ejemplo de ellos son los sistemas usados en Brasil desde 1996, del tipo DRE, muy simples usando tarjetas de memoria para almacenar los votos (ver Figura 5). Un estudio académico mostró que el total podía ser alterable por un votante malicioso, y que, peor aún, los registros públicos podían filtrar el voto de cada ciudadano, solo conociendo la hora de inicio de la votación [Aranha et al. 2019]. El sistema DRE usado en la India en forma nacional desde de 2004 fue diseñado para ser aún más básico, sin pantalla y con una interfaz simple consistente en botones (ver Figura 6). Pese a que el conteo se realiza en el mismo dispositivo al finalizar la elección, se mostró que eran susceptible a ataques similares a los descritos anteriormente [Wolchok et al. 2010].

La deficiencia principal de los sistemas DRE es su opacidad. Sin mecanismos para garantizar que el conteo es realizado correctamente, cuando dicho conteo se realiza en forma interna y los registros de los votos se mantienen en forma digital, ¿cómo puede un observador externo verificar a ciencia cierta que el total fue calculado correctamente? ¿Cómo puede un votante asegurarse que el computador no viola la privacidad del voto llevando un registro subrepticio de cómo han votado los ciudadanos? La clave aquí es la ausencia de evidencia convincente, comprobable por externos, que el resultado es correcto. Esta evidencia debe ser compatible con el secreto del voto, y con el requerimiento de confiar lo menos posible en la menor cantidad de entidades posibles, dado que cualquier participante es potencialmente un adversario.

Una estrategia para mitigar la inseguridad de los sistemas DRE consiste en extenderlos con un mecanismo para imprimir trazas en papel verificables por el votante (VVPAT, por su nombre en inglés) (ver Figura 7). Cada votante puede verificar que su preferencia ha sido correctamente capturada al menos en una copia en papel de su voto, permitiendo una contabilidad basada en las papeletas físicas en caso de cuestionamiento. Desafortunadamente, esta posibilidad de recuento puede no concretarse nunca si se carece de procedimientos y/o legislación que garantice la preservación de dichas papeletas y permita a los ciudadanos solicitar su revisión y conteo posterior bajo condiciones razonables. En varios estados de Estados Unidos, en las elecciones de 2016, y pese a utilizar sistemas con VVPAT en muchos estados, intentos de recuento fueron obstaculizados y negados administrativa y legalmente, inutilizando los VVPATs como mecanismo de verificación en la práctica.

En caso de tener respaldo legal y administrativo robusto, los procedimientos de auditoría estadística denominados *Risk Limiting Audits* (RLA) permiten determinar, con alta probabilidad, si el resultado publicado es consistente con el registro auditable (VVPAT o similar). La operación consiste en seleccionar aleatoriamente un subconjunto pequeño de las papeletas emitidas y recontarlas (o compararlas) para garantizar la correctitud del resultado de la elección. Sin embargo, como lo demuestra la experiencia en Estados Unidos, este proceso debe ser la norma y no la excepción. La recomendación actual de la Academia Nacional de Ciencias, Ingeniería y Matemática (NASEM) de los Estados Unidos es de hecho incluir estrategias de verificación estadística como los RLAs en todos los proyectos de sistemas de

Figura 5. Urna de tipo DRE usada en las elecciones de Brasil en 2005.

Fuente: Wikipedia.

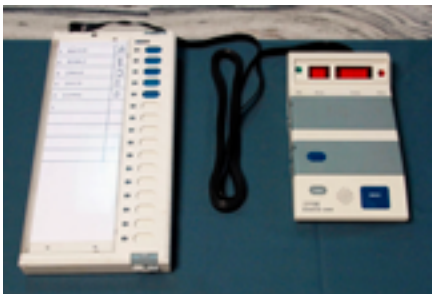


Figura 6. Máquina de votación utilizada en la India.

Fuente: Wikipedia.

Figura 7. Máquina DRE con VVPAT. La ventana de plástico transparente (a la izquierda en la foto) muestra la papeleta impresa completa para su aprobación por el votante.

Fuente: Verifiable Voting Foundation.

votación para los próximos diez años, partiendo con proyectos pilotos con miras a una implementación masiva, en elecciones de escala nacional [NASEM 5.7,5.8]. Asimismo, recomienda descontinuar sistemas que NO proveen papel legible por humanos [NASEM 4.11].

Votación remota y sus dificultades

Si la experiencia muestra que los sistemas de votación presenciales han sido difíciles de implementar correctamente, implementar votación remota pareciera ser un desafío de otro planeta. Con la tecnología actual, no sabemos realmente cómo diseñar un sistema de votación remoto seguro, siempre que el sistema use computadores o dispositivos móviles de propósito general. De hecho, es probable que "votar desde el teléfono" sea inherentemente inseguro. La razón es simple: tal sistema debe poder garantizar que la preferencia del votante es capturada correctamente aún si existe software malicioso (malware) en el teléfono o computador del votante. A priori, nada impide crear malware que pueda intervenir el software que registra el voto, mostrando el mensaje "Usted votó por Candidato A" cuando por detrás registra el voto por "Candidato B", una clara violación a la integridad de la elección. Peor aún, el malware conocería la preferencia del votante, violando el secreto del voto. Argumentar que para una cierta versión del sistema operativo o teléfono "no existe malware" es no entender el problema, ignorando los incentivos detrás de todo ataque. Si la elección es de alto perfil e importante, alguien creará tal malware.

Una posible estrategia para soslayar el problema anterior es disponer de un dispositivo cerrado, solo creado y configurado para permitirle al votante emitir su voto. Lograrlo no sería fácil, eso sí. El costo de proveer tal hardware para todos los votantes probablemente sería estratosférico. Además, si la historia reciente nos sirve de guía, desarrollar y mantener en forma transparente un software confiable (seguro y transparente) para dicho dispositivo parece ser una tarea impracticable, aún para gigantes tecnológicos.

Aún dejando de lado ambos problemas anteriores, hay asuntos más delicados que complotarían con esta solución: hoy no sabemos cómo evitar la coerción y venta de votos en un sistema remoto. Simplemente no sabemos cómo excluir los votos emitidos bajo presión en forma remota, cuando alguien le "mira sobre el hombro" o con "una pistola en la cabeza", y en situaciones donde el votante podría estar monitoreado en todo momento. Tampoco es claro qué hacer cuando el votante mismo puede querer vender su voto (por ejemplo haciendo *streaming* de la selección de su preferencia "en vivo"). Algunas sugerencias, como permitir un voto sustitutivo en persona (que un nuevo voto reemplace cualquier voto anterior del mismo votante) al final del periodo de votación pueden paliar parcialmente el problema de coerción, pero no eliminarlo. El robo o venta de credenciales siguen siendo amenazas reales en muchos escenarios de votación remota propuestos. De hecho, el problema de la venta de votos pareciera, hasta donde sabemos, insalvable en estas condiciones.

La dificultad del voto por Internet es al menos igual (sino mayor) pues el carácter abierto de la red introduce una preocupación más pedestre pero significativamente más grave: la posibilidad del "hackeo" remoto. Ataques computacionales basados en explotar vulnerabilidades en los protocolos de red o en la implementación del sistema pudieran comprometer la integridad del total.[3] Si dichos ataques son difíciles de mitigar ya en sistemas informáticos más simples, ¿seremos capaces de mitigarlos apropiadamente en sistemas de votación con requerimientos sustancialmente más complejos? El problema no es el ataque en sí, sino la escala de su impacto: el costo de cambiar 1 voto es probablemente similar al costo de cambiar millones de votos.

El uso de Internet también introduce un nuevo riesgo, la denegación de servicio (DoS). Si bien cualquier sistema

3 | Un ejemplo notable es el ataque al sistema de votación de Washington D.C. en Estados Unidos en 2010 por un equipo de investigadores universitarios los cuales, luego de comprometer totalmente el sistema, solo fueron detectados cuando pusieron el himno de su universidad a todo quien votara [Wolchok et al. 2012].

"El propósito de un sistema de votación no es nombrar al ganador, sino convencer al perdedor". Dan Wallace respecto del rol de la transparencia de los procesos de elección democrática.

conectado a Internet está expuesto a tal ataque, los procesos eleccionarios son extremadamente sensibles a fallas focalizadas. Por ejemplo, un DoS focalizado en una región específica del país con una historia particular de preferencias políticas podría afectar seriamente una elección. Hasta el día de hoy, los ataques DoS focalizados como éste siguen siendo una amenaza sin resolver para estos sistemas.

Un caso relevante de votación por Internet es el caso de Estonia. Usando una tarjeta inteligente, su tarjeta nacional de identidad, los ciudadanos pueden votar remotamente, por Internet, desde 2005. El sistema también implementa una variante del voto sustitutivo para mitigar la coerción. Pese a ser considerado un caso ejemplar de digitalización de servicios, su empleo de Internet y su falta de transparencia, lo ha hecho el blanco de críticas. Un análisis hecho por un grupo independiente de expertos internacionales en 2013 dejó en evidencia la falta de procedimientos verificables, la poca transparencia de ciertos procesos centrales de conteo, y debilidades operativas de ciberseguridad en dichos procesos [Springall et al. 2014]. El sistema era vulnerable a la manipulación de los resultados por atacantes con recursos (otros estados) y a la instalación de malware en el software cliente. Casos similares de votación por Internet en Australia (iVote), Noruega, Suiza y Estados Unidos (Washington D.C., Utah) han mostrado dificultades similares.

En general, tanto en sistemas remotos como presenciales, el principal punto de contención es la necesidad de confiar ciegamente en que ciertos procesos (las operaciones del software cliente o del servidor, y los procedimientos de control administrativos) hayan sido realizados en forma correcta, sin que el sistema tenga mecanismos para generar evidencia sólida de tal realización. Esto genera una dependencia completamente injustificada. Si a esto le agregamos la falta de modelos claros respecto a quienes tienen acceso a votos de otros y quienes no, es posible que serias debilidades en la integridad o privacidad de estos sistemas surjan en forma indetectable.

Es difícil justificar la seguridad de sistemas de votación remota en elecciones de alto perfil y de manera sostenible en el tiempo.[4] La recomendación actual de la Academia Nacional de Ciencias, Ingeniería y Matemática (NASEM) de los Estados Unidos lo refleja bien: *"En la actualidad, Internet (o cualquier red conectada a Internet) no debiera ser utilizada para devolver papeletas de votos marcadas.[5] Más aún, la votación por Internet no debiera ser usada en el futuro hasta y a menos que garantías sólidas de seguridad y verificabilidad sean desarrolladas e instaladas, puesto que ninguna tecnología actual garantiza la seguridad, confidencialidad, y verificabilidad de las papeletas de votación marcadas si ellas son transmitidas por Internet"* [NASEM 5.11].

¿Está condenada la votación remota? No lo sabemos a ciencia cierta; solo sabemos que desconocemos cómo hacerlo bien con la tecnología actual. La única manera de saberlo con certeza es estudiándolo. La misma NASEM propone estudiarlo evaluando "científicamente los potenciales beneficios y riesgos de la votación por Internet" [NASEM 7.3].

La promesa de las nuevas tecnologías

El desafío de generar evidencia verificable de que ciertos procesos han sido llevados a cabo correctamente, puede ser alcanzado utilizando técnicas de verificación punto a punto *(End-to-end verificaction, o E2E-V)*. Usando criptografía esta técnica permite a los votantes auditar la ejecución de sistemas de votación durante la ejecución misma, en forma online. Por ejemplo, un participante externo puede matemáticamente verificar que el contenido de una encriptación es un mensaje de una forma específica, digamos la identidad de un candidato válido. Esto ha permitido diseñar sistemas donde no es necesario confiar en los participantes, basta comprobar —usando criptografía— que han cumplido correctamente su labor.

Una enorme cantidad de sistemas E2E-V han sido desarrolladas en el ámbito académico en las últimas tres décadas pero pocos han llegado a realizaciones prácticas. Entre ellas se destacan los sistemas Prêt à Voter (utilizado en Victoria, Australia [Ryan et al. 2009, Culnane et al. 2015]), Scantegrity (utilizado en Tacoma Park, Estados Unidos [Carback et al. 2010]), y STAR-vote (en Travis County, Texas, Estados Unidos [Bell et al. 2013]).

4 | Elecciones de bajo perfil, o rápidas, con sistemas nuevos y poco estudiados pueden resultar circunstancialmente exitosos (por ejemplo la consulta de municipalidades de fines de 2019). El verdadero test de efectividad está en lograr elecciones de alto perfil de manera sistemática, lo cual se conjetura infactible hoy en día.

5 | El mismo reporte efectivamente permite el envío de las papeletas originales, sin marcar, hacia los votantes, siempre que las papeletas puedan ser autentificadas (por ejemplo con una firma digital).

La seguridad de los dispositivos DRE ha sido paupérrima.

De todas maneras, las técnicas criptográficas tienen sus limitaciones: los mecanismos son usualmente complejos de entender y explicar, demandando no solo votantes activos e instruidos, sino autoridades competentes, algo no siempre posible. También requiere de implementaciones cuidadosas, pues pequeños errores de implementación en las fórmulas pueden invalidar las garantías matemáticas en las cuales se basa la seguridad del sistema (como el caso reciente del sistema de votación de la agencia postal suiza [Lewis 2019]). Aún así, NASEM recomienda tanto conducir experiencias pilotos de sistemas E2E-V que usen VVPATs [NASEM 5.10], considerando incluso su utilidad potencial una votación por Internet [NASEM 7.3].

Un concepto propuesto para votaciones electrónicas importante de mencionar es el de *independencia de software* [Rivest 2008]. Los sistemas de votación electrónicos debieran ser "independientes del software", esto es, resilientes ante fallas y errores (posiblemente maliciosos) de los computadores utilizados en dichos sistemas. Más específicamente, un sistema de votación alcanza independencia del software si un cambio o error no detectado en su software no puede causar un cambio o error no detectado en el resultado o conteo de la elección.

Una tecnología frecuentemente mencionada para votación electrónica es blockchain. Si bien la tecnología es interesante y permite resolver problemas de consistencia en sistemas distribuidos dinámicos, su aplicación a votación electrónica no es necesaria ni requerida pues los requisitos son distintos. Si bien un sistema de blockchain permitiría a una entidad publicar preferencias y registros auditables en la blockchain, su utilidad es limitada dado que la autoridad del sistema centralizado de votación siempre lo puede hacer. Además, la falta de responsabilidad de los mineros en una blockchain (algo deseable, por ejemplo, para decidir si incluir o no transacciones) resulta poco deseable en un sistema de votación donde típicamente se requiere certeza de que ciertas operaciones fueron realizadas.[6]

Otros ataques

Como indicamos al comienzo, un sistema de votación electrónica es más que el sistema para emitir y registrar las preferencias de los usuarios, e involucra, por ejemplo, los mecanismos de registro de votantes. Recientemente, debido a una posible campaña de intrusión rusa en las elecciones presidenciales de Estados Unidos de 2016, se ha puesto en discusión la debilidad de los sistemas de votación ante ataques que buscan vulnerar la integridad del registro de votantes. El objetivo de dichos ataques sería alterar, borrar personas de las listas de posibles votantes para causar confusión, molestia y apatía en el electorado, violando así el derecho al voto. Si bien la protección de dichos sistemas está muy relacionada con la discusión respecto a "segurizar la red" donde operan dichos sistemas, la existencia de requisitos legales para permitir a los ciudadanos fácilmente consultar y actualizar sus registros dificulta el proceso pues abre la puerta a ataques de ingeniería social sobre ciudadanos cuya sofisticación tecnológica puede ser baja. Asimismo, existe la posibilidad de ataques remotos ("hackeo") dirigidos no a la autoridad que ejecuta el sistema de votación sino a las empresas fabricantes de componentes del sistema. Comprometer el *software* o *firmware* de dispositivos cruciales para el conteo de votos (por ejemplo el disco duro de un sistema de conteo centralizado) pudiera ser muy efectivo a la hora de perturbar un sistema eleccionario.

Problemas abiertos

El diseño de sistemas de votación es, al fin y al cabo, la elaboración de un sistema de software confiable y usable por todos los ciudadanos de un país. Eso significa que debe proveer buena usabilidad para la mayoría de (¿todos?) los ciudadanos y generar confianza en la robustez de la implementación (esto es, la implementación no debiera tener errores).

La usabilidad de un sistema de votación es de por sí un problema complejo de múltiples aristas. ¿Podemos diseñar sistemas fácilmente usables por todos los ciudadanos, sin discriminar a un segmento de la población? ¿Cómo evitamos el *"digital divide"*, la desconexión y reticencia natural de los ciudadanos mayores ante los dispositivos tecnológicos que pudiera conspirar contra su derecho al voto? Subyacente a este problema es la disyuntiva fundamental si el ciudadano puede o debe entender el sistema de votación usado. En sistemas complejos, como los basados en técnicas criptográficas, lo más probable es que no entienda las fórmulas ni por qué los procesos funcionan. Pero ¿debe hacerlo? Un fallo de la Corte Constitucional Alemana de 2009 puso severas restricciones al uso de sistemas de votación electrónica en elecciones federales en Alemania pues "los pasos esenciales de la votación y la determinación del resultado deben poder ser examinados por un ciudadano en forma certera sin poseer conocimiento

6 | Ron Rivest recientemente dijo que implementar votación electrónica usando blockchains es como "*traer un candado a un incendio en la cocina; puede ser bueno para algunas cosas, pero no para votación*" [Rivest 2020].

especializado en el tema" [Federal Constitutional Court, 2009]. Un contraargumento es la posibilidad de todo ciudadano de viajar en aviones o consumir medicamentos sin entender su funcionamiento. ¿Hasta qué punto el carácter del sistema (elección de representantes versus transporte aéreo) debiera determinar si el ciudadano debe entender su funcionamiento por sí solo para que el sistema sea válido?

La confianza en la robustez de la solución es otro problema difícil de resolver, particularmente en una comunidad abierta y bajo el escrutinio público. ¿Cómo podemos garantizar que el software fue implementado correctamente, sin errores lógicos ni de programación? ¿Es suficiente que el proyecto sea de código abierto y sometido a auditorías periódicas? (la respuesta es negativa en ambos casos). ¿Cómo manejamos el descubrimiento y notificación de fallas de seguridad, sobre todo justo antes o durante una elección? Aún si se utilizan mecanismos de auditoría periódica, ¿cómo el votante obtiene garantías que la versión en ejecución durante la elección es la versión auditada? Y respecto al hardware, ¿debemos usar hardware genérico o especializado en los computadores utilizados? ¿Cómo garantizamos que el hardware esté libre de puertas secretas y de dispositivos de monitoreo? Estrategias existen para mitigar estos problemas pero están lejos de proveer una solución robusta y convincente para todos.

Un problema similar es crear y mantener una confianza pública en el sistema. Si bien la búsqueda continua y sistemática de fallas del sistema es un mecanismo crucial para mejorarlo, la revelación de dichas fallas pudiera aumentar la desconfianza en el mismo (la paradoja es que mientras más fallas sean encontradas y resueltas, más seguro es el sistema pero menor es la confianza de la población en el sistema). Asimismo, anuncios falsos de problemas de seguridad pueden ser difíciles de desacreditar. La principal defensa, en mi opinión, es la solidez de la confianza pública inicialmente depositada en el sistema. Ésta solo puede ser fruto de una iniciativa amplia y académicamente sólida, ojalá basada en un proceso público e iterativo con participación ciudadana transversal e inclusiva.

Desafíos de corto plazo

Mejoras parciales: un nuevo sistema de votación debiera proveer al menos los mismos beneficios y cumplir los mismos requerimientos (sino más) comparado con el sistema que reemplaza. Esto nos pone un primer desafío, el de entender el sistema actual, con sus debilidades y fortalezas. Relacionado con esto está el identificar mejoras parciales al sistema actual antes de cambiarlo por un sistema completamente electrónico (por ejemplo, la disponibilidad de un claustro electoral electrónico que permita votar en distintos locales de votación, selección más transparente de los vocales y miembros del colegio escrutador, y participación masiva en los procesos de conteo de votos). Otras mejoras incluyen fortalecer la seguridad del registro electoral online, incluyendo estrategias de detección de intentos de intrusión y alteraciones [NASEM 4.6,4.8].

Políticas públicas: desde una perspectiva más global, el Estado debiera establecer una política (estrategia) consensuada y clara que defina los procesos de estudio y cambio de sistemas electorales. Definir de manera consensuada e informada las razones y objetivos detrás de modificaciones al sistema, definiendo métricas claras de progreso [NASEM 4.10]. El establecimiento de comisiones expertas y públicas para evaluar nuevas tecnologías es también recomendado [NASEM 5.12]. Además, cualquier sistema debe ser permanentemente auditado, sus procesos y resultados, en cada elección [NASEM 5.5-5.6]. La auditoría debe ser hecha por profesionales idóneos de manera abierta y transparente, posiblemente con observadores públicos en el caso de utilizar técnicas del tipo RLA.

Investigación: el Estado debiera definir políticas claras de fomento del estudio e investigación en estos temas, incluyendo la seguridad y confiabilidad de nuevas tecnologías de autentificación de votantes, los efectos de la coerción y compra de votos (especialmente en grupos vulnerables), y evaluaciones cuantitativas respecto a si los votantes (con y sin discapacidades) podrían verificar sus papeletas de votación, y detectar errores u omisiones [NASEM 7.3].

¿Vale la pena votación electrónica?

"El propósito de un sistema de votación no es nombrar al ganador, sino convencer al perdedor". Dan Wallace, Universidad de Princeton.

La confianza en el sistema actual de votación viene de nuestra experiencia y cotidianeidad con el sistema: escribir en un papel, doblarlo, guardarlo en una caja, y luego sacarlo y abrirlo, es una experiencia relativamente común. ¿Por qué entonces quisiéramos cambiarlo? Las razones típicamente esgrimidas para introducir computadores en el proceso son muchas, desde aumentar la participación y/o facilidad de uso, hasta simplemente posibles ahorros en los costos. No es claro qué razón prima en las motivaciones, pero la experiencia comparada muestra que son la facilidad de uso, junto a la de administración y ejecución del sistema los principales factores. Sin embargo, en público frecuentemente se argumenta como beneficios de los sistemas de votación una reducción en costos, mejor usabilidad en general, y el fomento de la participación de la ciudadanía en los

procesos eleccionarios. Examinemos estas razones a continuación.[7]

Menor costo: es común argumentar que un sistema de votación electrónico (especialmente sin VVPAT) si bien pudiera tener un alto costo inicial, puede implicar un ahorro significativo en el mediano plazo, especialmente en términos de ahorros en el suministro y administración del papel. Sin embargo, tales argumentos son debatibles pues no consideran los nuevos costos: el almacenamiento seguro, entrenamiento del personal, licenciamiento de software, y la reparación y actualización de los equipos y dispositivos [Zetter 2008].

Mejor usabilidad: aparte de dificultades asociadas al *"digital divide"*, el diseño de la interfaz de un sistema de votación electrónica requiere estudios cuidadosos de la población objetivo, lo cual no siempre es fácil ni da los resultados deseados [Herrnson et al. 2006; Oostveenet et al. 2009]. Además, puede introducir nuevos problemas de usabilidad [Conrad et al. 2009], posiblemente aumentando las tasas de voto fallido *(undervote)* [Acemyan et al. 2014]. No es sorprendente por lo tanto la recomendación de la NASEM respecto a utilizar asesoría especializada para diseñar tanto la interfaz (audio y pantalla) como la impresión de las papeletas de nuevos sistemas de votación electrónico con apoyo [NASEM 4.9].

Aumento de la participación: un argumento frecuentemente mencionado es que los votantes participarían más en votaciones remotas por la facilidad de no tener que desplazarse físicamente. Diversos estudios cuestionan esta conclusión. El estudio de Bochsler aplicado al caso Estonia en 2007 argumenta que "en vez de atraer nuevos votantes, pareciera que la votación por Internet principalmente sustituye a los votantes en las urnas" [Bochsler 2010]. Otro, de 2017 sobre dos circunscripciones en Holanda, reportó "ningún efecto en la participación" [Germann et al. 2017]. Y un estudio en Canadá sí detectó un aumento de participación de un 3.5% e incluso mayor en situaciones donde no existe voto por correo o el registro previo no es obligatorio pero comparable con aumentos obtenidos vía flexibilizaciones similares de las reglas para participar en la votación. El mismo estudio sin embargo concluye que, "si bien la votación por Internet puede mejorar la participación, es improbable que resuelva la crisis de participación". En resumen, la evidencia científica justificando un incremento en la participación sería aparentemente escasa.

Otras razones: pese a las (aparentemente) malas noticias anteriores, existen otras razones raramente mencionadas pero sin embargo beneficiosas de la votación electrónica. Estos sistemas tienen la potencialidad de permitir mejorar la usabilidad e inclusión para comunidades típicamente ignoradas, como ciudadanos con discapacidades (por ejemplo, interfaz de audio para personas con dificultad visual, distintos colores para gente con dificultad visual, o incluso pedales para personas con discapacidades en su torso superior), ciudadanos cuyo lenguaje no es el mayoritario en un país (por ejemplo, personas de habla Quechua o Mapudungún), o permitir mayor flexibilidad en el tipo de preguntas, permitiendo preguntas potencialmente más complejas (varias opciones rankeadas, por ejemplo). Lamentablemente, estos beneficios por sí solos no parecen ser suficientes cuando el sistema no cumple los requerimientos fundamentales enunciados al comienzo de este artículo.

Quizás el aspecto más interesante y prometedor es la posibilidad futura de construir variantes de sistemas de votación electrónica que permitan una interacción continua y fluida entre la ciudadanía con sus representantes, así como entre los distintos ciudadanos. Canalizar la voz de los ciudadanos en forma eficiente en procesos de participación democráticos preservando la seguridad es el gran desafío de los próximos años.

Conclusión

Los sistemas de votación son una pieza clave en nuestros procesos democráticos y su modificación no debe tomarse a la ligera. La introducción de sistemas electrónicos de votación, si bien presenta algunos beneficios, actualmente conlleva riesgos demasiado significativos comparados con la operación del sistema actual. Mientras la tecnología existente no permita minimizar y acotar dichos riesgos, no es claro que tal migración sea recomendable. Obviamente, eso no significa dejar de estudiar o testear nuevas técnicas y prototipos de votación. Todo lo contrario: nuestra sociedad, en conjunto con académicos, investigadores e innovadores, debiera hacer un esfuerzo por analizar los actuales desafíos, diseñar nuevos sistemas y experimentar con su aplicación específica a nuestra comunidad. El conteo local de votos, la generación de trazas en papel (VVPAT) con protección legal adecuada, el uso de técnicas criptográficas E2E-V para lograr independencia del software, y las auditorías estadísticas (RLA) post elección, son herramientas que debieran ayudarnos. Sin embargo, faltarán nuevos mecanismos y nueva ciencia, cuya creación no será trivial. Mejorar la calidad de la democracia, con mejor y mayor participación ciudadana nunca ha sido fácil. Pero ciertamente siempre ha valido la pena hacerlo. ▪

7 | Esta sección está basada en [Hevia 2018].

REFERENCIAS

- [Acemyan et al. 2014], "Usability of Voter Verifiable, End-to-end Voting Systems: Baseline Data for Helios, Prêt à Voter, and Scantegrity II.". C. Z. Acemyan, P. Kortum, Michael D. Byrne y D. S. Wallach. Electronic Voting Technology Workshop/Workshop on Trustworthy Elections, 2014.
- [Arahna et al. 2019], "The Return of Software Vulnerabilities in the Brazilian Voting Machine", D. F. Aranha, P. Y. S. Barbosa, T. N. C. Cardoso, C. Lüders de Araújo y P. Matias. Elsevier Computers & Security, 86, 2019.
- [Bell et al. 2013], "STAR-Vote: A Secure, Transparent, Auditable, and Reliable Voting System", S. Bell, J. Benaloh, M.D. Byrne, D. Debeauvoir, B. Eakin, G. Fisher, P. Kortum, N. McBurnett, J. Montoya, M. Parker y O. Pereira. USENIX Journal of Election Technology and Systems, 1(1), 2013.
- [Bochsler 2010], "Can Internet voting increase political participation", D. Bochsler. En conferencia 'Internet and Voting', Fiesole, 2010.
- [Carback et al. 2010], "Scantegrity II municipal election at Takoma Park: The first E2E binding governmental election with ballot privacy". R. Carback, D. Chaum, J. Clark, J. Conway, A. Essex, P. S. Hernson, T. Mayberry, S. Popoveniuc, R. L. Rivest, E. Shen y A. T. Sherman. USENIX Symposium, 2010.
- [Conrad et al. 2009], "Electronic voting eliminates hanging chads but introduces new usability challenges", F. G. Conrad, B. B. Bederson, B. Lewis, E. Peytcheva, M. W. Traugott, M. J. Hanmer, P. S. Herrnson, R. G. Niemi. Int. J. Human-Computer Studies 67, 2009.
- [Culnane et al. 2015], "vVote: a verifiable voting system". C. Culnane, P. Y. Ryan, S. Schneider y V. Teague. ACM Transactions on Information and System Security, 18(1), 2015.
- [Feldman et al. 2006], "Security Analysis of the Diebold AccuVote-TS Voting Machine", A. J. Feldman, J. A. Halderman y E. W. Felten, 2006. https://citp.princeton.edu/our-work/voting/
- [Germann et al. 2017], "Internet voting and turnout: Evidence from Switzerland". M. Germann y U. Serdült. Electoral Studies, 47, Elsevier, 2017.
- [Gonggrijp et al. 2007], "Studying the Nedap/Groenendaal ES3B voting computer: A computer security perspective", R. Gonggrijp y W-J. Hengeveld. USENIX workshop on accurate electronic voting technology, 2007. http://wijvertrouwenstemcomputersniet.nl/images/9/91/Es3b-en.pdf
- [Herrnson et al. 2006], "The Importance of Usability Testing of Voting Systems", P. S. Herrnson, R. G. Niemi, M. J. Hanmer, B. B. Bederson, F. G. Conrad, M. Traugott. USENIX/ACCURATE Electronic Voting Technology Workshop. 2006.
- [Hevia 2018], "El Camino hacia la Votación Electrónica Segura en Chile", presentación en Conversatorio "Ciberseguridad, ¿estamos preparados?", A. Hevia. Senado de Chile, 6 de Julio de 2018.
- [Kiayas et al. 2006], "Security Assessment of the Diebold Optical Scan Voting Terminal", A. Kiayias, L. Michel, A. Russell, A. A. Shvartsman, M. Korman, A. See, N. Shashidhar y D. Walluck. (2006). https://web.archive.org/web/20061127175659/http://voter.engr.uconn.edu/voter/Reports_files/uconn-report-os.pdf
- [Lewis 2019], "Ceci n'est pas une preuve: The use of trapdoor commitments in BayerGroth proofs and the implications for the verifiability of the Scytl Swiss Post Internet voting system", S. J. Lewis, O. Pereira y V. Teague. Univ. Melbourne, Australia, 2019.
- [NASEM], "Securing the vote", National Academy of Sciences, Engineering, and Math, 2018.
- [Oostveenet et al. 2009], "Users' experiences with e-voting: A comparative case study", A. M. Oostveen y P. den Besselaar. Journal of Electronic Governance 2, no. 4, 2009.
- [Rivest 2008], "On the notion of 'software independence' in voting systems", R. L. Rivest. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 366, no. 1881, 2008.
- [Rivest 2020], "Cryptographers Panel" en RSA Security Conference, febrero de 2020.
- [Ryan et al. 2009], "Prêt à voter: a voter-verifiable voting system". P. Y. Ryan, D. Bismark, J. Heather, S. Schneider y Z. Xia. IEEE transactions on information forensics and security, 4(4), 2009.
- [Springall et al. 2014], "Security Analysis of the Estonian Voting System", D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine y J. Alex Halderman. CCS 2014 "Independent Report on E-voting in Estonia", https://estoniaevoting.org/ 2014.
- [Wolchok et al. 2010], "Security Analysis of India's Electronic Voting Machines", S. Wolchok, E. Wustrow, J. A. Halderman, H. K. Prasad, A. Kankipati, S. K. Sakhamuri, V. Yagati y R. Gonggrijp. En ACM Conference on Computer and Communications Security, 2010.
- [Wolchok et al. 2012], "Attacking the Washington, DC Internet voting system", S. Wolchok, E. Wustrow, D. Isabel y J. A. Halderman. International Conference on Financial Cryptography and Data Security, Springer, 2012.
- [Zetter 2008], "The Cost of E-Voting", K. Zetter (4 de abril de 2008). https://www.wired.com/2008/04/the-cost-of-e-v/

¿Cree usted que hay temas del mundo digital que deben ser directamente incorporados a una potencial nueva Constitución? ¿Cuáles?

A partir del proceso constituyente recientemente originado, sería un gran aporte si quienes trabajamos en el mundo digital podemos contribuir a pensar qué temas de ese ámbito debieran ir en una (potencial) nueva Constitución. Es por eso que planteamos la interrogante a diversos académicos y profesionales del área. Esperamos que las respuestas recibidas puedan servir como punto de partida para un oportuno debate al respecto.[1]

Comité Editorial
Revista Bits de Ciencia

> Optaría por un documento minimal con flexibilidad para adaptación, junto a formas explícitas de actualización a nuevas versiones. Incluiría puntos relativos a la protección de datos personales, inteligencia artificial, limitaciones a tratamiento de datos en territorio nacional, firma electrónica para todo trámite, transparencia por diseño, plataforma de iniciativa ciudadana de ley *(CrowdLaw)* y asegurar voto en papel.
>
> **Marcelo Aliaga.**
> *Profesor y asesor TI Universidad de Talca.*

> Que la digitalización y automatización (ejecutada por organizaciones nacionales o internacionales) no afecten negativamente el ejercicio de derechos fundamentales que nos permiten tener una vida digna, manteniendo nuestra individualidad mientras somos parte de una sociedad. Pienso en derechos como no ser discriminadxs arbitrariamente, privacidad de la vida/datos, e incluso los neuroderechos.
>
> **Claudia López Moncada.**
> *Académica Universidad Técnica Federico Santa María.*

1 | Por una cuestión de espacio nos es imposible publicar todas las respuestas recibidas, pero las mismas están disponibles de manera pública en: https://www.dcc.uchile.cl/bits-de-ciencia/muro-de-expresion

Tal como ocurre en la actualidad, debe consagrarse el derecho a la protección de los datos personales. Es decir, que tenemos derecho a la protección de los datos personales que nos conciernen, que dichos datos deben procesarse de manera justa para fines específicos y sobre la base del consentimiento, y que toda persona tiene derecho a acceder a los datos que se han recopilado sobre ella.

Sebastián Valenzuela.
Académico Pontificia Universidad Católica de Chile.
Investigador Instituto Milenio Fundamentos de los Datos.

Sí, dos temas independientes pero interrelacionados: 1) País Digital, o la disposición de plataformas integradas para la atención de los servicios públicos, en la Constitución se debiera garantizar el acceso universal a estos servicios en forma digital; y 2) Transparencia, disponer de plataformas que permitan visualizar todos los datos de servicios públicos e incluso privados.

Javier Vidal.
Académico Universidad de Concepción.

Debiese existir a nivel constitucional la obligación del Estado de velar porque no exista (o sea mínima) la brecha digital en cuanto a acceso y conocimiento tecnológico para las personas en nuestro país, principalmente en contextos de educación, biotecnología, comunicación y emprendimiento.

Elson Stuardo.
Académico Universidad de Los Lagos.

Por un lado la información personal debería mantenerse de forma reservada, especialmente cuando pueda usarse para discriminar arbitrariamente (por ejemplo, información médica). Por el otro, uno debería poder acceder a la información que se tiene de uno mismo sin tener que pagar por ella (por ejemplo, reporte de Dicom o certificados que se puedan obtener del Registro Civil).

Rodrigo Paredes.
Académico Universidad de Talca.

Tres derechos de la ciudadanía que deberían ser resguardados por una nueva Constitución: 1) Derecho a la privacidad y protección de datos personales; 2) Derecho a recibir información veraz y precisa (elaborar/difundir información falsa debería ser penalizado), y 3) Derecho a la no discriminación de ningún tipo (ideología, orientación sexual, etc.) tanto en ambientes offline como online.

Magdalena Saldaña.
Académica Pontificia Universidad Católica de Chile.
Investigadora Instituto Milenio Fundamentos de los Datos.

El Estado de Chile debiera definirse como un Estado digital, es decir que hará todos los esfuerzos para digitalizar su relación con las personas, para facilitar la vida de éstos y transparentar su gestión. Así, instituciones con una lógica del siglo antepasado como notarios y conservadores debieran tender a desaparecer o, al menos, focalizarse en trámites especialmente complejos.

Guillermo Cabrera.
Académico Pontificia Universidad Católica de Valparaíso.

Protección de datos; alfabetización digital; delitos informáticos. Sin perjuicio de lo anterior, no se puede obligar a que todas las personas tengan un teléfono propio o cuenten con alfabetización digital: por lo tanto se debe asegurar que todos los ciudadanos cuenten con los mismos derechos, independiente de su condición respecto a los temas de informática.

Julio Águila.
Académico Universidad de Magallanes.

Propiedad de los datos y de la información profesional. El derecho a que la persona sea el dueño único de cualquier dato que se genere sobre sí, y que se deba contar con su autorización expresa para su uso.

Mario Inostroza Ponta.
Académico Universidad de Santiago de Chile.

La integración entre los distintos sistemas computacionales del Estado debe brindar eficiencia para agilizar los trámites para todos los ciudadanos. Para ello es necesaria no solo la disponibilidad de los sistemas, sino también la accesibilidad teniendo en cuenta las brechas. Esto debe analizarse teniendo en cuenta el balance entre la transparencia de los sistemas y la privacidad de las personas.

Cecilia Bastarrica.
Académica Universidad de Chile.

Protección de la privacidad digital de los ciudadanos. Las empresas y los organismos públicos recolectan y comercializan los datos personales de los chilenos. El ciudadano no tiene ningún control sobre la distribución de su información privada, ni puede optar por ser borrado o no compartido de estas bases.

Felipe Guerrero.
Gerente de Informática Maui and Sons.

Privacidad y seguridad: la privacidad debe estar garantizada. No garantizarla afecta la seguridad física y mental de las personas.
Transparencia: se debe asegurar disponibilidad y facilidad de acceso (estándares) a la información pública.
Economía digital: la economía será (ya está siendo) digital. Asegurar suficiente flexibilidad con el fin de agilizar y regular nuevos negocios de base digital.

Miguel Guevara.
Director del Laboratorio de Data Science, DatosLab.cl, Universidad de Playa Ancha.

Es crítico volcar el esfuerzo tecnológico para atender nuestros problemas nacionales: educación, salud, agricultura, desechos, aguas, energía. Debemos fomentar la transferencia efectiva y concreta aquí y el desarrollo de I+D+i con impacto sustantivo en estos sectores y términos; no en otros ajenos a nuestra subdesarrollada realidad.

Pedro Pinacho-Davidson.
Académico Universidad de Concepción.

Chile frente a la vigilancia digital

RENÉ PERALTA ARCAYA

Criptógrafo del Instituto Nacional de Normalización y Tecnología (NIST) de Estados Unidos. Doctor en Computación por la Universidad de California, Berkeley. Ha sido profesor de varias universidades, incluyendo la Universidad Católica de Chile y Yale. Actualmente trabaja en las áreas de aleatoriedad pública, criptografía postcuántica, criptografía de mejora de la privacidad, y complejidad de circuitos.

rene@peralta.one

Este documento fue preparado por René Peralta Arcaya a título personal. Las opiniones aquí vertidas son de exclusiva responsabilidad de su autor, y no reflejan puntos de vista ni de NIST, ni del Departamento de Comercio, ni del Gobierno de Estados Unidos.

Una nueva Constitución chilena sería una oportunidad para enfrentar la vigilancia digital. Estas palabras tienen como objetivo denunciar el fenómeno y llamar a expertos a articular derechos constitucionales que reviertan la precaria situación actual de los ciudadanos chilenos frente al capitalismo de vigilancia.

La vigilancia digital

Mientras camino con mi pareja por el parque, es normal sentirnos dueños de nuestro entorno. En la actualidad, sin embargo, el simple hecho de tener un teléfono con nosotros pone gran parte de este entorno a disposición de intereses ajenos. Nuestra posición geográfica, lo que nos decimos, si nuestros corazones laten lenta o apresuradamente, si nos encontramos con unos amigos, si nos paramos a mirar un árbol o una estatua, si nos abrazamos en el césped... Todo esto es ahora la materia prima de un modelo de despojo y comercialización de nuestras vidas en beneficio de otros.

El rumbo actual de nuestra sociedad es hacia un mundo lleno de sensores. No solo nuestro teléfono, sino nuestro reloj, nuestra ropa, nuestros lentes, y un sinfín de lugares otrora privados son ahora considerados oportunidades de mercado para el capitalismo de vigilancia. Pero no solo nuestros cuerpos. También lo son nuestra casa, nuestros colegios, nuestras calles y parques. En resumen, nuestras vidas. El capitalismo de vigilancia nos despoja de nuestro comportamiento, lo transfiere al mundo digital, y luego trafica esta información en mercados digitales. En estos mercados se lucra, en primera instancia, mediante la predicción algorítmica de nuestro comportamiento futuro en el mercado de bienes y servicios. En segunda instancia el modelo de lucro apunta no solo a predecir, sino que a determinar. Este modelo de intervención en nuestras vidas adopta las técnicas del conductismo de Skinner, expandidas y adaptadas al mundo digital por gurús académicos financiados por el capitalismo de vigilancia. El modelo conductista reduce la persona a su conducta, negando la relevancia de un mundo personal interno que dé sentido a la vida humana. Desde esa perspectiva, no hay un problema ético en el uso de técnicas que modifiquen nuestro comportamiento sin nuestro conocimiento ni permiso. Ni siquiera los más vulnerables entre nosotros, nuestros niños y adolescentes, tienen derecho a santuario. En el libro "The Age of Surveillance Capitalism" [7], Zuboff usa un concepto de Sartre, "la voluntad de ejercer la voluntad", como una condición necesaria de las personas. Si se extingue la voluntad de ejercer la voluntad, se extinguen nuestras vidas. Pero esto es precisamente la meta del conductismo digital. Los dueños del aparato de vigilancia digital nos venden en la medida que nos predicen o determinan. Seres autónomos que reclaman el derecho a ser impredecibles son un obstáculo en los mercados de predicción del comportamiento.

La vida efectiva

Vivir en sociedad es condición necesaria para la vida humana. En la era moderna, esto requiere del acceso a las comunicaciones, al transporte, a la educación, a la información, a la asamblea, al *"chat room"*... Con respecto a esto, es mucho lo que nos ha dado la revolución digital de las últimas décadas.[1] Sin embargo, el capitalismo de vigilancia condiciona el acceso a todo esto a la renuncia de nuestra autonomía y de nuestra privacidad. Vivir sometidos a un régimen de vigilancia corporativa, y acosados por un sinfín de pequeños estímulos conductuales para el lucro de otros, es ahora lo que entregamos en un pacto faustiano para obtener derecho a la vida efectiva. Esta situación global es producto de contingencias históricas (tecnología digital, hegemonía de Estado en el caso de China, globalización, hegemonía del capital consagrada por el neoliberalismo en el caso de Estados Unidos). Distintas contingencias hubieran podido dar otros resultados. En particular, el modelo de negocios basado en la vigilancia no es la única manera de hacer realidad las maravillas de la era digital. La rentabilidad de la vigilancia supera largamente lo necesario para pagar los servicios de información y conectividad de los cuales hemos llegado a depender. El Estado tiene la capacidad de financiar la infraestructura digital y de fomentar un modelo de negocios alternativo, en el cual se respeten los derechos humanos.

A modo de ejemplo, y sin intentar ser exhaustivo, enumero algunos de los principios y derechos que están en juego:

- Acceso a telefonía, y a Internet y sus servicios, sin vigilancia de las corporaciones. La intervención del Estado en estos medios debe ser acorde con derechos humanos y en beneficio de la sociedad y las personas.
- En el hogar y en los lugares sociales, así como en otros entornos del individuo moderno (en la calle, en los buses y autos, en los aviones, en el trabajo), debe ser posible vivir sin vigilancia electrónica.
- La conexión digital de los objetos cotidianos, ya sea entre ellos o con el exterior, no puede ser por defecto. Una vez conectados, la conexión debe ser fácil

1 | Una importante excepción a esta evaluación de lo positivo de la revolución digital, es la deterioración de la información necesaria a los procesos democráticos (ver [3], https://www.newyorker.com/magazine/2019/09/30/the-dark-side-of-techno-utopianism).

de terminar apretando un botón. No es aceptable que tengamos que andar construyendo cajas de Faraday para evitar que los objetos en nuestras casas reporten nuestras conversaciones a terceros.

- Los datos de salud de las personas no pueden ser traficados con fines de lucro.
- Los niños tienen derecho a que sus juguetes no estén conectados a Internet con fines de lucro.
- Los colegios deben ser santuarios adonde no llegue la vigilancia digital ni los estímulos conductuales con fines de lucro. Los modelos en los cuales se le "regala" a un colegio computadores, a cambio de pasarles avisos comerciales y monitorear las comunicaciones de los niños, no tienen lugar en nuestros colegios.
- El uso de técnicas de modificación de la conducta no puede ser en beneficio de intereses comerciales ni políticos. Tampoco pueden tener como objetivo la homogeneidad ni de nuestras conductas ni de nuestro fuero interno. Todo aquello que apunte a extinguir la voluntad de ejercer la voluntad, es un atentado a la persona.
- Estos derechos deben ser inalienables, de manera que el renunciar a ellos no pueda ser condición de acceso a los servicios digitales.

El modelo de negocios del capitalismo de vigilancia

Si compramos un bien de mercado es natural suponer que el dinero que pagamos corresponde al costo de producción y comercialización más un porcentaje de ganancia para el inversor. Pero éste no es el modelo de negocios del capitalismo de vigilancia. Lo ganancia que obtiene Google cuando compramos un Android, se deriva en gran parte del poder de despojarnos de nuestras experiencias de vida para venderlas en un mercado de predicción del comportamiento.[2]

Ahora, ya estamos acostumbrados a la vigilancia. Ésta ya no nos indigna, aunque debiera.

Esta situación es tan inédita que es natural que la persona no comprenda la naturaleza de la transacción. Si hace veinte años nos hubieran dicho que nos dan un teléfono a cambio de grabar nuestras conversaciones privadas y luego lucrar con las inferencias derivables sobre nuestro comportamiento, muchos de nosotros hubiéramos dicho que no. Ahora, ya estamos acostumbrados a la vigilancia. Ésta ya no nos indigna, aunque debiera. Y el individuo ya no puede decir que no, porque ahora esto implicaría renunciar a la vida en sociedad. La única manera de decir que no ahora es a nivel de sociedad y Estado.

También es importante comprender que, habiéndose establecido el modelo de negocios del capitalismo de vigilancia, las corporaciones son ahora prisioneras del modelo. Una empresa como Google no puede, unilateralmente, empezar a respetar los derechos humanos, sin hacerse no-viable comercialmente. La única salida que tenemos, tanto ciudadanos como corporaciones, es establecer la ilegalidad del modelo de vigilancia. Entidades con más poder que el Estado de Chile, por ejemplo la Comunidad Europea, están en eso. Pero las protecciones que los europeos logren establecer no se extenderán automáticamente a los chilenos. La disyuntiva chilena actual ofrece la oportunidad de mejorar la correlación de fuerzas en favor de los derechos humanos de los ciudadanos.

La predicción algorítmica

Hasta hace pocas décadas, la predicción de riesgos, por ejemplo para un seguro de vida, se basaba en no más de unas decenas de datos. El individuo, y las autoridades fiscalizantes correspondientes, tenían acceso a la ecuación que calculaba el riesgo. El capitalismo de vigilancia digital apunta a usar no unas decenas sino miles de datos sobre el individuo. Estos datos, en su mayoría, no son aportados voluntariamente. Ellos incluyen fotos, grabaciones de voz, el entorno del hogar, el historial de localización geográfica, y todo aquello detectable y capturable por el régimen de vigilancia. Los datos ni siquiera son accesibles para el individuo afectado. Además, el cómputo que arroja una medida de riesgo basada en estos datos es usualmente opaco, no solo para el individuo sino también para los mismos dueños de los algoritmos (éste es el caso cuando se usan redes neuronales u otras técnicas de inteligencia artificial [6]). No es posible una fiscalización del cómputo, por ejemplo para hacer respetar principios de equidad. Peor aún, estos algoritmos perpetúan y magnifican sesgos e inequidades [1, 2].

La predicción algorítmica también se usa para "optimizar" sistemas y entornos. Por ejemplo, un colegio "inteligente" del futuro (y también del presente) usaría estas técnicas para "optimizar" la educación de los alumnos. Pero ¿qué es lo que se optimiza? Solo aquello que es factible de expresarse en un número, en una función matemática sobre datos medibles por el régimen de vigilancia. No se puede reducir el bienestar de los individuos ni la salud o efectividad de las instituciones, a lo medible y calculable. Es necesario medir y calcular, pero

2 | Las ganancias de Apple con el iPhone son más complicadas de explicar aquí. Éstas dependen en menor medida, y en forma indirecta (mediante contratos con Google y Facebook), de la vigilancia digital.

sobre aquello es necesario una evaluación no por computadoras sino por personas e instituciones. Tal evaluación debe, además, contextualizarse en una realidad y un marco de valores locales. El capitalismo de vigilancia promueve aplicar la optimización algorítmica a todos los entornos e instituciones sociales, a los colegios, los parques, las ciudades, las comunicaciones, los hospitales... Esto necesariamente lleva a emascular principios y conceptos como equidad, solidaridad, amistad, salud, felicidad. Y, convenientemente para los dueños de los capitales, a elevar la vigilancia como condición necesaria al bienestar humano y social.

Soberanía del Estado sobre la red de Internet

Querámoslo o no, la visión de mundo y sociedad de gran parte de la población está hoy mediada por Internet. La hegemonía de unas pocas corporaciones sobre este medio les otorga un poder inédito sobre el público. Esta asimetría de poder no solo se establece en la relación corporaciones-ciudadanía sino también en la relación corporaciones-Estado. Como lo demostró el caso de Cambridge Analytica (ahora Emerdata), el capitalismo de vigilancia también trafica en influencias sobre los procesos democráticos. No podemos aceptar que una corporación pueda vender al mejor postor un porcentaje posiblemente determinante de votos. El Estado debe tener las atribuciones necesarias para ejercer la soberanía digital en nombre de la ciudadanía. Esto es tanto para proteger la libertad de expresión como para combatir las asimetrías de poder que atenten contra los derechos humanos y los procesos democráticos. Estas asimetrías son enormes. La capitalización de mercado de Alphabet (conglomerado dueño de Google) es varias veces el valor agregado de todas las compañías chilenas. Los estados hacen lo que pueden en defensa de los derechos humanos de sus ciudadanos. Debemos estudiar y aprender de los esfuerzos de instituciones internacionales, como la ONU y la Unión Europea, así como de las denuncias de las organizaciones internacionales de derechos humanos como Amnistía Internacional.[4]

Las redes sociales

La persona moderna requiere de un espacio psíquico privado en el cual forjamos y alojamos nuestra identidad. Este espacio es particularmente vulnerable en la niñez y en la adolescencia, cuando aún no se ha desarrollado la conciencia que una persona tiene de ser ella misma y distinta a las demás. El capitalismo de vigilancia toma por asalto este espacio. El modelo que Facebook ha instalado en las redes sociales apunta a eliminar el espacio privado y sustituirlo por una cara pública (una cara mucho más lucrativa, por cierto). Es en este espacio público donde el adolescente busca la legitimación de su identidad. Los daños que esto causa están ampliamente documentados por psicólogos, sociólogos y filósofos. El poder de quienes controlan este espacio es enorme. ¿De verdad debemos aceptar, por ejemplo, que una corporación trasnacional decida qué nivel de depresión en los jóvenes chilenos es aceptable y compatible con sus ganancias?

Santuario para el hogar

Entre los planes del capital de vigilancia está llenarnos la casa de sensores conectados a sus algoritmos de captura y comercialización de datos. La cocina y el baño son particularmente atractivos para quienes quieren saberlo todo sobre nosotros. Si en un futuro no muy lejano, sentado en el baño de tu casa, el parlante "Google home" te anuncia que, según la taza del baño, tu presión arterial está algo elevada [5], y te recomienda que vayas a tal o cual doctor, ¿cuál será tu reacción? Cuando te expliquen que los sensores del baño tienen como finalidad la protección de tu salud ¿qué pensarás? Es mi esperanza que sientas indignación. Que te preguntes qué cara te habrán visto... Y si tu indignación les resulta incomprensible a tus hijos, ¿qué harás? ■

REFERENCIAS

[1] S. Barocas and A. D. Selbst. Big data's disparate impact. *California Law Review*, 104:671–732, 2016.

[2] F. Z. Borgesius. Discrimination, artificial intelligence and algorithmic decision-making. 2019. Documento del Consejo de Europa.

[3] A. Marantz. The dark side of techno-utopianism. *The New Yorker*.

[4] Amnistía Internacional. Gigantes de la vigilancia: La amenaza que el modelo de negocios de Google y Facebook representa para los derechos humanos. 2019.

[5] US Patent Office. Patente US 10064582 B2, de Google: Noninvasive determination of cardiac health and other functional states and trends for human physiological systems. 2018.

[6] A. Selbst and S. Barocas. The intuitive appeal of explainable machines. *FORDHAM L. REV.*, 87:1085–1139, 2018.

[7] S. Zuboff. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. 1st edition, 2018.

El sistema constitucional de protección de la privacidad en el derecho chileno

Foto: Harold Castillo

DANIEL ÁLVAREZ VALENZUELA

Académico de la Facultad de Derecho de la Universidad de Chile. Coordinador Académico del Centro de Estudios en Derecho Informático y socio de Ciberseguridad Humana. Licenciado en Ciencias Jurídicas y Sociales, Magíster en Derecho Público y candidato a doctor en derecho, todo por la Universidad de Chile.

En Twitter lo encuentras como @simenon.

Introducción

Para muchos resulta evidente que el debate público sobre el derecho a la privacidad y sus límites, llegó para quedarse entre nosotros. La discusión constitucional que se aproxima, en caso que se apruebe el plebiscito convocado para abril de 2020, es muy buen contexto para revisar la forma en que la Constitución chilena protege la privacidad de las personas.

Tradicionalmente en el derecho chileno los antiguos textos constitucionales protegían objetos tan disímiles como el hogar, los efectos personales —aquellas cosas que la personas traen consigo—, los papeles y la correspondencia privada. No fue sino recién en la Constitución de 1980, cuando se reconoció un derecho especial que protege este ámbito esencial de la vida de las personas, que se ha ido transformando en unos de los derechos fundamentales de la vida contemporánea.

En las siguientes líneas quiero explicar que en el derecho constitucional chileno existe un conjunto de derechos explícitos que amparan aquello que intuitivamente denominamos como privacidad, de una forma mucho más amplia y comprensiva que como tradicionalmente se ha analizado. Esta manera de entenderlo resulta fundamental si queremos utilizar el derecho a la privacidad como una de las defensas frente a las amenazas y riesgos que ha supuesto y supone el uso intensivo de tecnologías digitales en la vida cotidiana de las personas, especialmente frente a usos corporativos, comerciales y gubernamentales vinculados al perfilamiento, el marketing, la seguridad y la vigilancia masiva, entre otros usos.

Derecho a la privacidad

Comprendido como un sistema, el derecho a la privacidad está compuesto por la suma de los derechos amparados bajo las normas de los numerales 4º y 5º del artículo 19 de la Constitución, a saber:

a. el derecho a la vida privada;
b. el derecho a la protección de datos personales;
c. el derecho a la inviolabilidad del hogar;
d. el derecho a la inviolabilidad de las comunicaciones privadas; y,
e. el derecho a la inviolabilidad de los documentos privados

Estos derechos, junto a las normas pertinentes de los tratados internacionales sobre derechos humanos suscritos y ratificados por Chile y que se encuentren vigentes[1], forman parte de lo que hemos denominado *sistema constitucional* de protección de la privacidad, que debiera servir a varios propósitos. Por una parte, servir de mandato constitucional para el legislador al momento de desarrollar, en el nivel legal, la protección efectiva de estos derechos; mandato para el juez al momento de interpretar y aplicar los derechos protegidos constitucionalmente; mandato para las autoridades públicas en el desempeño de sus funciones; entre otros.

Cuando comprendemos las normas de protección de la privacidad en el derecho constitucional chileno como un sistema, podemos apreciar que, a pesar de las obvias diferencias entre los distintos derechos que conforman el sistema, al aplicar sus disposiciones sobre hechos u objetos específicos, evidenciaremos que existen zonas donde éstos se entrecruzan o se superponen.

Veamos un ejemplo. En el proceso de comunicación privada que se verifica mediante el uso de plataformas de mensajería instantánea como WhatsApp, Signal o Telegram, existen varios objetos de protección que superan al mero derecho a la inviolabilidad de las comunicaciones privadas del numeral quinto del artículo 19, que ampara el acto comunicativo en sí mismo. Los metadatos asociados al proceso comunicativo reciben, al menos, una doble protección. Por una parte, se consideran que son elementos que forman parte del acto comunicativo, pero además son informaciones que dan cuenta de nuestras preferencias (con quién, por cuánto tiempo y con qué regularidad nos comunicamos) protegidos entonces por el derecho a vida privada propiamente tal. Además, como son datos personales aptos para el procesamiento, de los cuales se pueden inferir u obtener datos personales sensibles, serán objeto de protección del derecho a la autodeterminación informativa. Por último, sus respaldos electrónicos, celosamente guardados en nuestros teléfonos, por aplicación de las disposiciones sobre equivalencia normativa entre el documento en formato papel y el documento electrónico[2], serán objeto de protección del derecho a la inviolabilidad de los documentos privados, sin duda alguna.

¿Qué significa todo esto? Varias cosas. Primero, que las normas fundamentales comprendidas de manera sistémica operan reforzándose recíprocamente, entregando un nivel de protección constitucional más alto que si fueran consideradas individualmente. Segundo, que para que exista una intromisión legítima de la autoridad o de un tercero, se deben cumplir con las habilitaciones constitucionales establecidas para

1 | Véase los artículos 12 de la Declaración Universal de Derechos Humanos; 17 del Pacto Internacional de Derechos Civiles y Políticos; 11 del Pacto de San José de Costa Rica; y V, IX y X de la Declaración Americana de Derechos y Deberes del Hombre.

2 | Norma contenida en el artículo 3º de la Ley Nº19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.

cada disposición, algunas de las cuales además están establecidas en normas de carácter legal, las cuales también habrá que examinar para determinar si fueron dictadas cumpliendo con las exigencias que impone la Constitución.

El amparo a los documentos privados debe ser repensado completamente, a partir del feroz proceso de digitalización de la vida cotidiana de las personas.

Debo advertir que comprender las normas de protección de la privacidad como un sistema constitucional no supone, en ningún caso, desdibujar los contornos de las normas que lo integran. Al contrario, una mejor aplicación de esta teoría del sistema constitucional de protección de la privacidad requiere que el ámbito de aplicación, el contenido y los límites de cada derecho estén claramente identificados, de manera de precisar de mejor manera las zonas de superposición o reforzamiento recíproco.

Como se aprecia en la Figura 1, es posible explorar distintas formas de superposición entre dos o más derechos o, incluso, entre todos ellos:

A continuación, revisaremos cada uno de los cinco derechos que conforman el sistema constitucional de protección de la privacidad, a fin de determinar su contenido esencial.

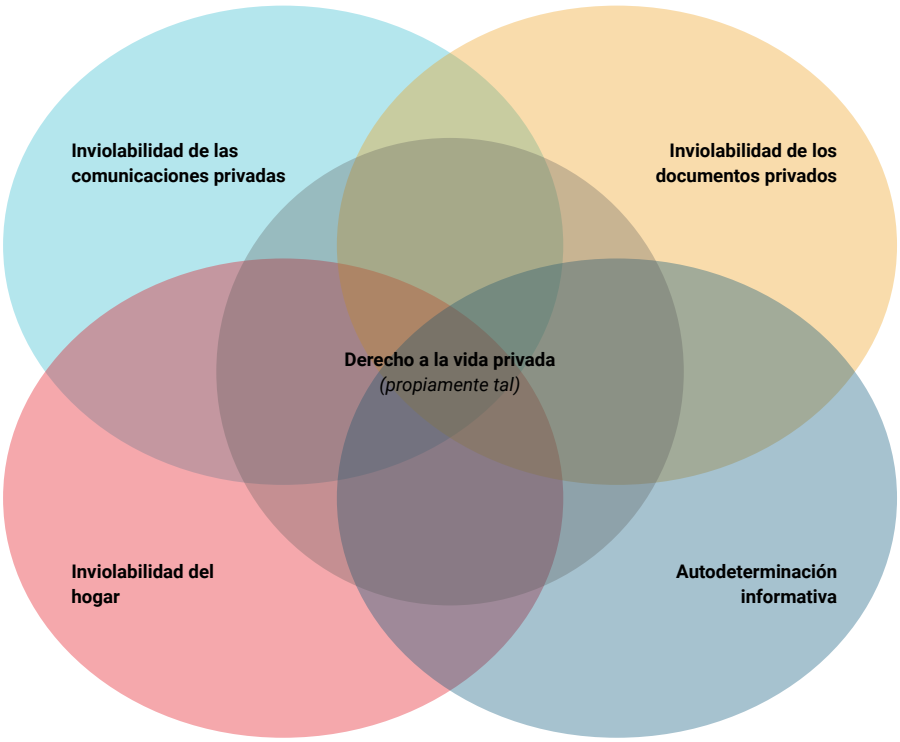


Figura 1. Superposición entre los diversos derechos amparados por el sistema constitucional de protección de la privacidad.

El derecho a la vida privada

Responder la pregunta acerca de qué es la privacidad, en general, suele sacarnos a pasear por consideraciones de tipo social, cultural, históricas, antropológicas e, incluso, religiosas.[3] Lo mismo sucede cuando nos preguntamos por el contenido del derecho a la vida privada. Una somera revisión de la doctrina nacional relativa al derecho consagrado en el numeral 4º del artículo 19, permite constatar el consenso que existe respecto a la dificultad de precisar qué se entiende por "vida privada". Diversos autores coinciden en que, por tratarse de un concepto de contornos indeterminados, de carácter cultural, variable en el tiempo y en el espacio, la determinación de su alcance y la identificación de sus límites, es una labor que le corresponde esencialmente a la jurisprudencia, sin perjuicio que algunos pocos de ellos se aventuran en la tarea de formular una definición más precisa.[4]

Existen, al menos, dos formas distintas de comprender el concepto de privacidad y, consecuentemente, el derecho que lo protege. En la primera, la vida privada es entendida como secreto, como aquello que un sujeto no desea que sea conocido por terceros. La segunda comprende la vida privada como expresión de autonomía y libertad personal. En la literatura nacional es posible encontrar autores y autoras que sostienen alguna de estas diversas posturas.

3 | (Corral Talciani, 2000; Figueroa, 2014; Novoa Monreal, 1979).

4 | (Barros Bourie, 2010; Figueroa, 2014; Tapia, 2008).

En trabajos previos, he considerado que se puede conceptualizar el derecho a la vida privada como aquel derecho que ampara los ámbitos de la vida de un sujeto determinado que, por su decisión o por mandato de la ley, quedan fuera del conocimiento o alcance de terceros y del Estado.[5] Así, sus preferencias sexuales, políticas o religiosas, sus hábitos personales, sus decisiones de consumo, su cuerpo y las decisiones que sobre él recaen, por mencionar algunos aspectos, se encuentran fuera del conocimiento general o de la intervención estatal.

El derecho a la autodeterminación informativa

Luego de la reforma constitucional de junio de 2018, se consagró la protección de datos personales como un nuevo derecho fundamental explícito de la Constitución, sumándose a la tendencia regulatoria comparada, principalmente de países de América Latina y Europa.

El derecho a la autodeterminación informativa es resultado de un doble proceso de transformación social y jurídica. Por una parte, la creciente utilización de tecnologías informáticas y digitales por parte de órganos del Estado, del sector privado y de la propia ciudadanía, para la captura, procesamiento y transmisión de información personal, levantó varias alarmas respecto al impacto que este tipo de herramientas podía tener en la protección de los derechos fundamentales de las personas.

Esto llevó a la doctrina y jurisprudencia a identificar cuál era la respuesta que se podría ofrecer desde el derecho para controlar o dar legitimidad al proceso de captura, procesamiento y transmisión de datos personales, que permitiera, por una parte, el flujo de información imprescindible para el funcionamiento de una sociedad moderna e informatizada y, por otra, garantizara la no afectación de los derechos fundamentales de las personas.

La constitucionalización del derecho a la protección de datos personales tiene efectos prácticos importantes. Por ejemplo, significa que la regulación sobre el "tratamiento" y la "protección" de datos personales deberá siempre adoptar la forma de una ley, excluyéndose la vía reglamentaria u otras normas menores como las ordenanzas municipales. Esto resulta especialmente importante si pensamos en iniciativas en materia de seguridad pública que implican tratamientos de datos personales de manera intensiva, como son las tecnologías de videovigilancia mediante cámaras estáticas, globos

5 | (Álvarez Valenzuela, 2018).

La Constitución protege por igual una comunicación privada donde se expongan aspectos sensibles de la vida de las personas o aquellas donde se expongan nimiedades o asuntos sin importancia.

y drones, las cuales usualmente son reguladas en normas de jerarquía inferior a la ley, por lo cual podrían devenir en inconstitucionales.

El derecho a la inviolabilidad de las comunicaciones privadas

En obras previas he sostenido que el derecho a la inviolabilidad de las comunicaciones privadas es un derecho de carácter autónomo e independiente de la protección que la Constitución reconoce al derecho a la vida privada analizado precedentemente.[6] El derecho a la inviolabilidad de las comunicaciones es el derecho que protege, por una parte, la libertad de comunicarse, en cualquier forma, con personas determinadas y, por la otra, resguarda dichas comunicaciones de la interferencia de terceros, sin que sea relevante el contenido de la comunicación transmitida, la que puede o no formar parte de la vida privada de las personas.

La regla vigente recoge la experiencia acumulada en más de doscientos años de historia, ampliando el ámbito de aplicación al concepto genérico de «comunicación privada» que reconoce al acto comunicativo en sí mismo como objeto de amparo constitucional, con independencia del soporte utilizado para materializar tal acción comunicativa y, lo que resulta más importante, con prescindencia del contenido de la comunicación. La Constitución protege por igual una comunicación privada donde se expongan aspectos sensibles de la vida de las personas o aquellas donde se expongan nimiedades o asuntos sin importancia.

El derecho a la inviolabilidad de los documentos privados

La evolución histórica del derecho a la inviolabilidad de los documentos privados ha avanzado, principalmente, de la mano del derecho a la inviolabilidad de la correspondencia. Así, por ejemplo, en los textos constitucionales de 1812 y 1818 se protegían la seguridad de "los papeles y efectos" de los ciudadanos o se declaró que "los papeles de cada individuo son sagrados", respectivamente. El vocablo "papeles" utilizado por estos textos cubría los documentos personales, profesionales o contables, además de la correspondencia privada que se encontrare entre dichos documentos.[7]

En mi opinión, el amparo a los documentos privados debe ser repensado completamente, a partir del feroz proceso de digitalización de la vida cotidiana de las personas, que ha significado que buena parte de lo que tradicionalmente considerábamos como documentos privados, dejaron de ser papeles guardados en cajones en nuestras casas, oficinas o bodegas y hoy están representados por archivos digitales contenidos en computadores, teléfonos u otros tipo de dispositivos que solemos portar (los cuales podrían calificar como efectos personales también) pero también que suelen ser almacenados en servidores computacionales mediante servicios basados en tecnologías de cloud computing, las cuales son difíciles de localizar territorial y jurisdiccionalmente.

El derecho a la inviolabilidad del hogar

La garantía de inviolabilidad del hogar es una garantía de larga data en el derecho constitucional chileno. Casi todos los textos constitucionales de la historia de Chile reconocían alguna forma de protección de la casa o el hogar de los ciudadanos.

Evans señala que la expresión "hogar" equivale a "recinto privado" y abarca, por tanto, no solo la vivienda de la familia, sino que también las oficinas, los hoteles, y toda edificación o predio que no tenga el carácter de abierto al acceso público o de bien nacional de uso público. Es así como el hogar es un concepto amplio y es el lugar donde la familia y sus integrantes pueden estar en intimidad. La idea del constituyente fue garantizar que la persona fuera respetada en sus actividades básicas y donde estuviere iniciando su acción exterior o desarrollando sus actividades más personales.[8]

Ante el surgimiento de un sinfín de dispositivos electrónicos, informáticos o digitales que permiten una intromisión ilegítima en el hogar de una persona, sin suponer allanamiento físico, cabe preguntarse cómo operaría la garantía de inviolabilidad. Como hemos señalado previamente, el hogar es una construc-

6 | (Álvarez Valenzuela, 2019).

7 | (Álvarez Valenzuela, 2019).

8 | (Evans Espiñeira, 2014).

ción jurídica basada en la idea de control de un espacio determinado, que la Constitución protege especialmente por ser uno de los espacios esenciales donde se llevan a cabo actos que esperan estar sustraídos de la observación ajena. De ahí que podemos comprender que los actos de intromisión en ese espacio de control no se limitan únicamente al allanamiento físico, sino que deben considerar las intromisiones intermedias por tecnologías. En caso contrario, el mero desarrollo tecnológico supondría una reducción del ámbito de protección de las garantías fundamentales, cuestión que no resulta razonable.

Como dice Frosini, debemos comprender a las tecnologías como instrumentos de "desarrollo de las libertades, esto es, las libertades han podido desarrollarse y expandirse notablemente a través de nuevas fronteras del actuar humano gracias precisamente al progreso tecnológico".[9]

REFERENCIAS

- Álvarez Valenzuela, D. (2016). Acceso a la información pública y Protección de Datos Personales. ¿Puede el Consejo para la Transparencia ser la autoridad de control en materia de protección de datos? *Revista de derecho (Coquimbo), 23*(1), 51–79.
- Álvarez Valenzuela, D. (2018). Privacidad en línea en la jurisprudencia constitucional chilena. *Revista de Derecho Público, 89*, 11–32.
- Álvarez Valenzuela, D. (2019). *La inviolabilidad de las comunicaciones privadas electrónicas* (1a edición). LOM ediciones.
- Anguita, P. (2007). *La protección de datos personales y el derecho a la vida privada.* Jurídica de Chile.
- Barros Bourie, E. (2010). *Tratado de Responsabilidad Extracontractual* (1a edición). Jurídica de Chile.
- Bascuñán Rodríguez, A. (1996). *La intimidad de la telecomunicaciones.* 26.
- Camacho, G. (2014). La protección de datos como frontera del derecho de acceso a la información en la legislación chilena. *Revista de Gestión Publica, 3*(1), 73–93.
- Cerda Silva, A. (2012). *Legislación sobre el protección de datos de las personas frente al tratamiento de sus datos personales* (p. 42) [Separata]. Centro de Estudios en Derecho Informático, Universidad de Chile.
- Corral Talciani, H. (2000). Configuración jurídica del derecho a la privacidad I: Origen, desarrollo y fundamentos. *Revista Chilena de Derecho, 27*(1), 51–79. https://dialnet.unirioja.es/servlet/articulo?codigo=2650211
- Covarrubias Cuevas, I. (2013). *La vida privada de las figuras públicas. El interés público como argumento que legitima la intromisión en la vida privada.* (1a edición). Legal Publishing Chile.
- Evans Espiñeira, E. (2014). La inviolabilidad del hogar y de la correspondencia: Nuevas perspectivas dogmáticas y jurisprudenciales. *Revista de Derecho. Universidad Finis Terrae, Segunda época*(II).
- Figueroa, R. (2014). *Privacidad.*
- Frosini, T. E. (2003). Nuevas tecnologías y constitucionalismo. *Revista Derecho del Estado, 15.* https://revistas.uexternado.edu.co//index.php/derest/article/view/798
- Nogueira Alcalá, H. (2013). *Derechos fundamentales y garantías constitucionales.* (4o edición, Vol. 1). Librotecnia.
- Novoa Monreal, E. (1979). *Derecho a la vida privada y libertad de información. Un conflicto de derechos*. (1a). Siglo XXI.
- Pastén, D. (2005). *Régimen jurídico de las medidas de interceptación de las comunicaciones telefónicas previstas en el Código Procesal Penal.* Universidad de Valparaíso, Escuela de Derecho.
- Tapia, M. (2008). Fronteras de la vida privada en el derecho chileno. *Revista Chilena de Derecho Privado, 11*, 117–144. https://dialnet.unirioja.es/servlet/articulo?codigo=3266922
- Vial Solar, T. (2000). Hacia la construcción de un concepto constitucional del derecho a la vida privada. *Revista Persona y Sociedad, XIV*(No3), 47 a 68.
- Viollier, P. (2017). *El estado de la protección de datos personales en Chile* (p. 52). ONG Derechos Digitales. https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf
- Vivanco, Á. (2006). *Curso de derecho constitucional. Aspectos dogmáticos de la Carta Fundamental de 1980: Vol. II* (2a edición). Ediciones Universidad Católica de Chile.

9 | (Frosini, 2003).

Computadores: ¿amigos o enemigos?

Informática en la violación y la defensa de los derechos humanos en Chile, 1973-1989

JUAN ÁLVAREZ RUBIO

Académico del Departamento de Ciencias de la Computación de la Universidad de Chile. Master of Mathematics (Computer Science), University of Waterloo. Ingeniero de Ejecución en Procesamiento de la Información, Universidad de Chile. Junto a su labor como docente, trabaja en reconstruir la historia de la computación en Chile.

jalvarez@dcc.uchile.cl

RESUMEN: "Computadores: ¿amigos o enemigos?" fue el título de un artículo escrito en 1978 que advertía que en los computadores "las posibilidades de mal uso son graves, incluyendo el uso para fines represivos por parte del Estado" [1]. Transcurridos cuarenta y dos años ese mismo título sirve para contrastar los usos de la tecnología computacional por parte de la dictadura en el período 1973-1989, para gestionar los datos de la represión de sus opositores, con los esfuerzos informáticos de algunas instituciones no gubernamentales para apoyar la defensa de los derechos de las personas en Chile.

Introducción

El golpe de Estado del 11 de septiembre de 1973, derrocó al Gobierno del Presidente Salvador Allende quien fue elegido en septiembre de 1970 y debía terminar su período constitucional en noviembre de 1976. Se inició entonces una larga dictadura de las fuerzas armadas y carabineros que violó sistemáticamente los derechos humanos, y que ha sido ampliamente estudiada por periodistas de investigación, historiadores y cientistas sociales y políticos.

El uso de la tecnología computacional durante la dictadura se produjo en el contexto del desarrollo del área en el país. De hecho, a comienzos de la década del setenta el Estado contaba con computadores en la Empresa Nacional de Computación (ECOM), en la Universidad de Chile y en algunos servicios y empresas del Estado. En las fuerzas armadas, la aviación y la marina disponían de computadores transistorizados IBM-1401 (de segunda generación) y el ejército contaba con un computador IBM-360 (de tercera generación). Posteriormente, en los años ochenta, en los ámbitos público y privado, se difundió el uso de los computadores personales y comenzó el uso de las redes computacionales antecesoras de Internet.

En este artículo se presenta un aspecto desconocido por gran parte de la ciudadanía: el uso de la tecnología computacional por parte del Estado para apoyar la represión y, por contraparte, la utilización de la informática en la defensa de los derechos de las personas en instituciones no gubernamentales.

Computación en la violación de los derechos humanos

El golpe de Estado afectó al área de computación principalmente con la intervención de ECOM y el consiguiente despido y degradación de directivos y funcionarios y la cancelación de algunos proyectos, entre ellos el emblemático proyecto Synco o Cybersyn [2]. Por otra parte, las universidades fueron intervenidas militarmente, se nombraron rectores uniformados y se suspendieron temporalmente carreras. En el caso de la Universidad Técnica del Estado (hoy USACH), después de ser ocupada militarmente, se detuvo, encarceló y expulsó a profesores, estudiantes y funcionarios.

La utilización de la tecnología computacional durante la dictadura, en desmedro de los derechos de las personas, solo se pudo constatar por las evidencias que se han conocido en tiempos de democracia. Al respecto, se analizará las huellas del uso de computadores en SENDET, en los servicios de "seguridad nacional" (DINA, CNI), y en la "Red Cóndor" de coordinación con organismos similares de algunos países sudamericanos.

Secretaría Ejecutiva Nacional de Detenidos (SENDET)

La primera señal del uso de computadores se encuentra en la "Relación de Prisioneros" (décima versión) del Fondo Ministerio del Interior y la Subsecretaría del Interior, confeccionado el 12 de noviembre de 1973 por la Secretaría Ejecutiva Nacional de Detenidos (SENDET), que fue creada en octubre de 1973. La cantidad de detenidos hizo necesario el uso de un computador para producir las nóminas, lo que se refleja en el tamaño del listado (cerca de 200 páginas y 12.000 personas) y el ordenamiento alfabético por sexo y por nacionalidad (ver Tabla 1). Por cada persona se consignó el nombre, la nacionalidad, la actividad o profesión, el campamento y las circunstancias de la detención, y la acción posterior.

Género	Páginas	Personas	Chilenos	Extranjeros	Países	Campamentos
Hombres	188	11.159	10.522	637	40	20
Mujeres	10	667	589	78	19	14
Total	198	11.826	11.111	715	41	20

Tabla 1. Listado de Detenidos N°10 (SENDET, noviembre de 1973).

Los campamentos corresponden a lugares de detención en Iquique, Pisagua, Tocopilla, Antofagasta, Calama, Copiapó, Guardia Vieja, La Serena, Estadio Nacional, Puente Alto, Buin, Rancagua, Valparaíso, Concepción, Talcahuano-Tomé, Valdivia, Llanquihue y Punta Arenas. La mayoría corresponde a regimientos y recintos militares. El Estadio Nacional aparece con la mayor cantidad de detenidos (9.440), seguido de Rancagua (578) y el buque Lebu en Valparaíso (438).

A fines de septiembre de 1973, Augusto Pinochet reunió a los jefes de los servicios de inteligencia militar (SIM), de la aviación (SIFA), armada (SIN), carabineros (SICAR) e investigaciones. En esa ocasión el coronel del ejército Manuel Contreras propuso una organización que comenzó a operar como dependencia del SENDET para efectuar la clasificación de los detenidos, los "interrogatorios" y la coordinación de "las tareas de inteligencia" [3].

Dirección de Inteligencia Nacional (DINA)

El 14 de junio de 1974 fue creada oficialmente la Dirección de Inteligencia Nacional (DINA) a cargo de Manuel Contreras con dependencia directa de la Junta de Gobierno. El Decreto Ley N° 521 de 1974 en su artículo 1° estableció que "*Créase la Dirección de Inteligencia Nacional, organismo militar de carácter técnico profesional, dependiente directamente de la Junta de Gobierno y cuya misión será la de reunir toda la información a nivel nacional, proveniente de los diferentes campos de acción, con el propósito de producir la inteligencia que se requiera para la formulación de políticas, planificación y para la adopción de medidas que procuren el resguardo de la seguridad nacional y el desarrollo del país.*"

La estructura de la DINA, en 1975 según el Departamento de Defensa de Estados Unidos , contó con una sección de Computación dependiente del subdirector logístico [4]. En otros momentos contó con unidades de documentación, de análisis, de archivo de microfichas, de telecomunicaciones, incluyendo "inteligencia electrónica". Adicionalmente, la Escuela Nacional de Inteligencia (ENI) dictó cursos de criptografía entre otros destinados a "perfeccionar" a su personal.

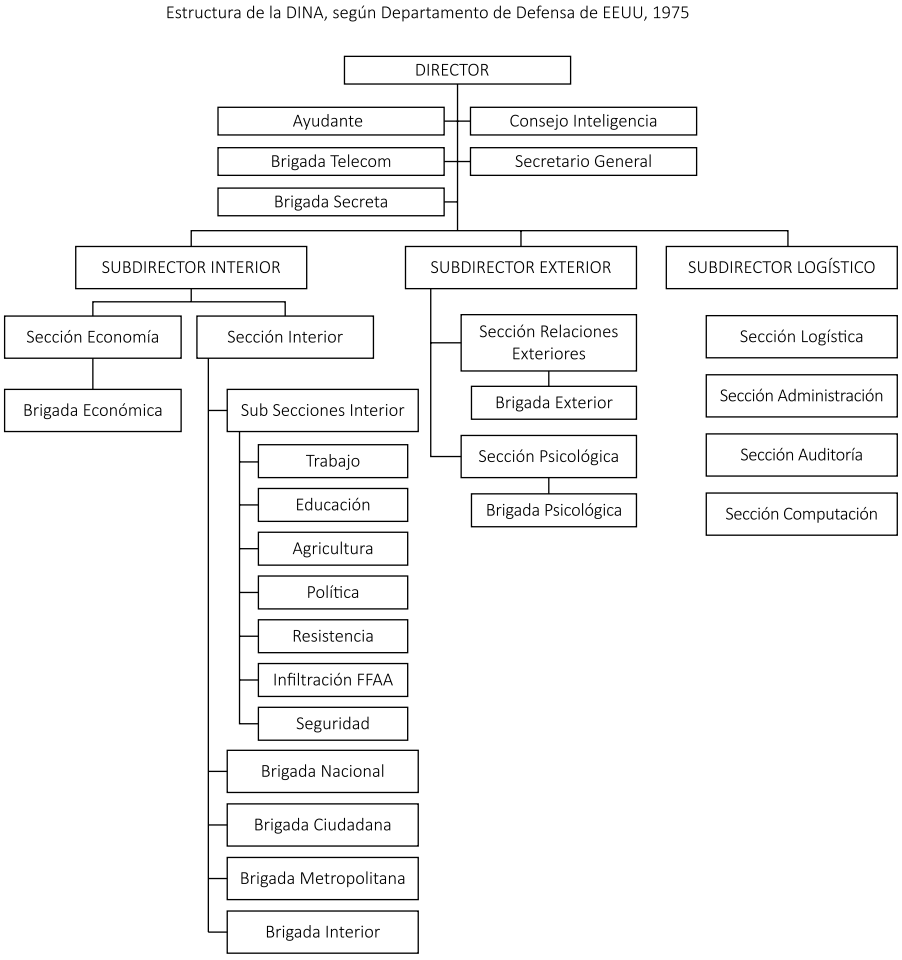


Figura 1. Estructura de la DINA.

Considerando sus objetivos de "reunir y procesar información" la DINA utilizó computadores. Prueba de ello es que en uno de los libros de Manuel Contreras [5] se incluyeron varios listados confeccionados por computador (ver Tabla 2). Cabe señalar que las nóminas "Relación de prisioneros" corresponden al listado n° 12 del 29 de diciembre de 1973 de SENDET e incluyen un total de 15.162 personas, tres mil personas más que en el listado n° 10 del 12 de noviembre.

Red Cóndor

Los orígenes del denominado "Plan Cóndor" u "Operación Cóndor" se encuentran en el "Primer Seminario de Policía sobre la lucha antisubversiva en el Cono Sur", efectuada en febrero de 1974 en Buenos Aires con la asistencia de representantes de Argentina, Bolivia, Brasil, Chile, Paraguay y Uruguay. En la ocasión se analizó establecer una coordinación para intercambiar datos sobre personas. Los acuerdos iniciales le permitieron a la DINA montar, entre otras

acciones, la Operación Colombo o "caso de los 119" (¡11-9!) que la prensa chilena difundió en julio de 1975 con los nombres de detenidos y desaparecidos en Chile supuestamente muertos en enfrentamientos fratricidas en Argentina.

Entre los días 25 y 29 de noviembre de 1975 la DINA organizó secretamente la "Primera Reunión de Trabajo de Inteligencia Nacional" [6] a la que asistieron los encargados de los servicios de inteligencia de Argentina, Bolivia, Paraguay y Uruguay. La convocatoria afirmaba que "*para enfrentar esta Guerra Psicopolítica hemos estimado que debemos contar en el ámbito internacional no con un mando centralizado en su accionar interno, sino con una coordinación eficaz que permita un intercambio oportuno de informaciones y experiencia además con cierto grado de conocimiento personal entre los jefes responsables de la seguridad*".

La DINA propuso un Sistema de Coordinación y Seguridad con un Banco de Datos y una Central de Informaciones (ver Figura 2). El Banco de Datos consistió de un archivo centralizado de antecedentes de personas manejado, financiado y alimentado por los Servicios de Seguridad de los países interesados. Por otra parte, la Central de Informaciones debía "*contar con un Sistema de Comunicaciones moderno y ágil, que permita cumplir con los principios de rapidez y oportunidad en la entrega de información y debía conformarse a base de: trasmisión por Télex, Medios de Criptografía, teléfonos con inversores de voz y correos*". Por todas estas características, el sistema de coordinación constituía una verdadera Red

Listado	Personas
Relación de prisioneros (mujeres)	902
Relación de prisioneros (hombres)	13.527
Relación de prisioneros extranjeros (mujeres)	77
Relación de prisioneros extranjeros (hombres)	656
Listado nacional de personas buscadas (31/XII/1976)	607
Listado nacional de peligrosos	2.488
Militantes de los partidos marxistas comunista, socialista, Mapu y otros que se integraron al ejército guerrillero	3.173
Fuerzas guerrilleras del MIR considerando a los militantes, ayudistas y simpatizantes	1.482

Tabla 2. Listados de personas en libro de Manuel Contreras.

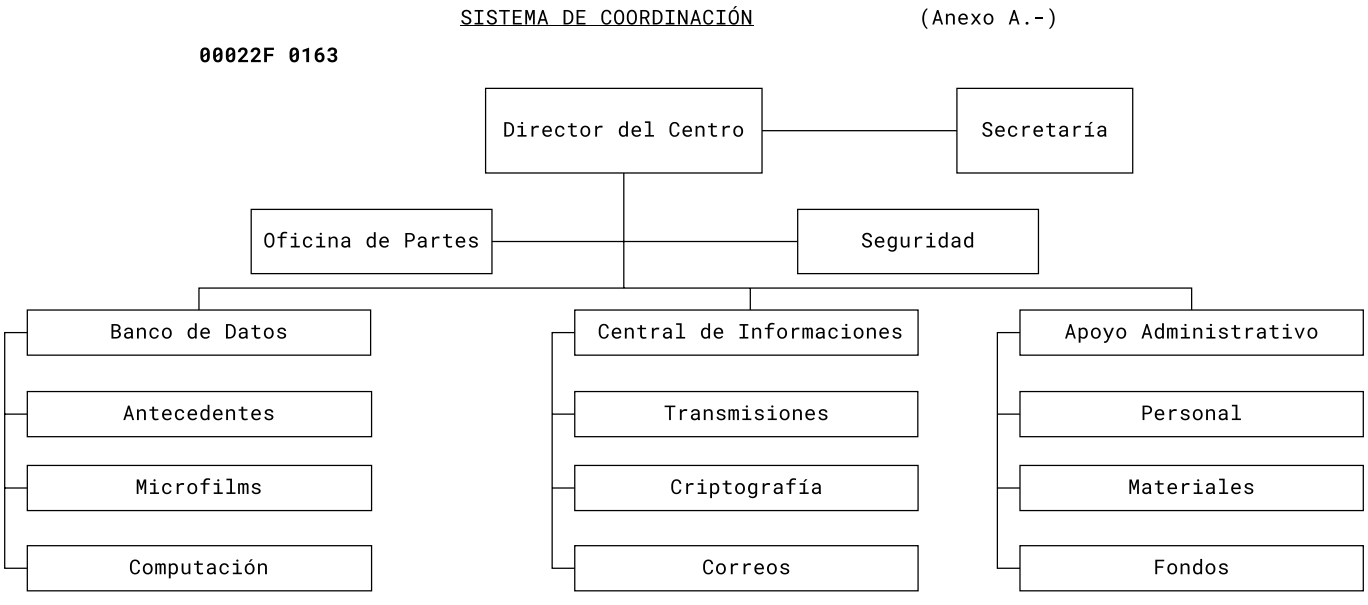


Figura 2. Estructura organizacional de la Red Cóndor.

de tecnología y de personas, y el nombre "Cóndor" fue sugerido por el representante de Uruguay como reconocimiento a Chile como país organizador y coordinador.

Respecto del uso de un computador en el banco de datos el funcionario del FBI Robert Scherrer afirmó que *"la CIA le había facilitado a la DINA sistemas computarizados y capacitación que presumiblemente se habrían aplicado al banco de datos Cóndor"* [7]. Por su parte, dos funcionarios de la CIA, que trabajaron muchos años en Latinoamérica, afirmaron que el apoyo habría sido provisto por una empresa externa contratada por la CIA. Otra fuente afirma que, con la ayuda de la Agencia Internacional de Desarrollo, se adquirió y utilizó un computador IBM-370/145 (el más poderoso de la época).

La red de télex, denominada "Condortel", estaba compuesta por los terminales Cóndor1 (oficina central en Chile), Cóndor2 (Argentina), Cóndor3 (Uruguay), Cóndor4 (Paraguay) y Cóndor5 (Bolivia). Más tarde Brasil, Ecuador y Perú se unieron a la red como Cóndor 6, 7 y 8 respectivamente (ver Figura 3). Inicialmente los mensajes vía télex se transmitían en un código primitivo, que era una simple sustitución de letras (ver Figura 4). Más adelante se instaló un dispositivo de encriptación automática en todos los terminales de télex. Por otra parte, las comunicaciones también se efectuaban usando una poderosa red de radio de alcance continental, cedida por el ejército estadounidense, cuyo transmisor central estaba en la zona del Canal de Panamá.

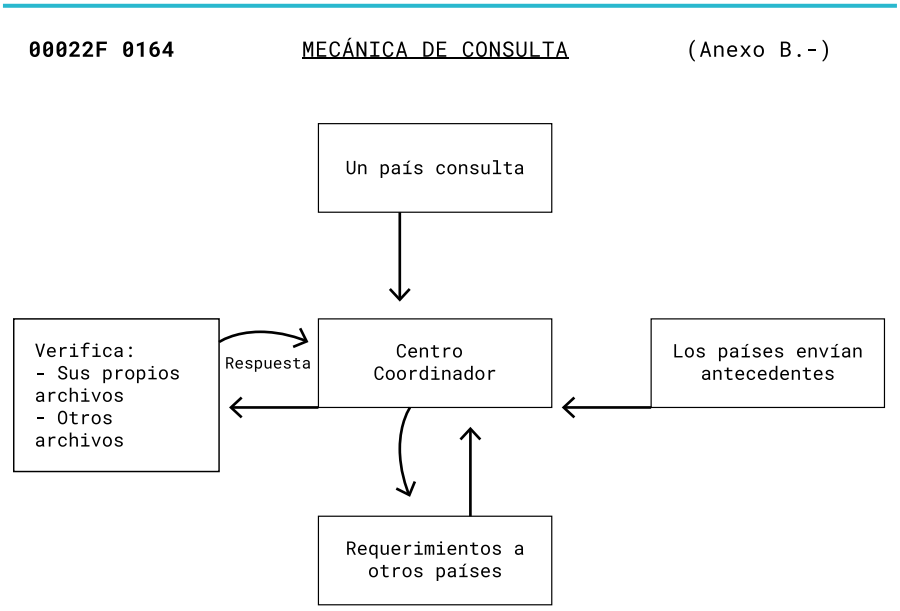


Figura 3. Sistema de consulta de la Red Cóndor.

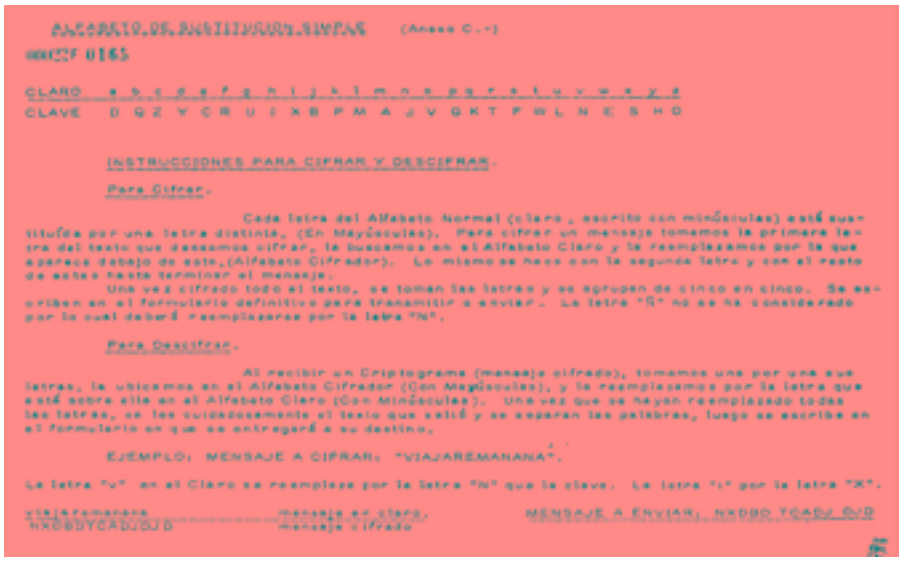


Figura 4. Algoritmo de criptografía de mensajes.

Central Nacional de Informaciones (CNI)

Debido a las repercusiones internacionales por el asesinato de Orlando Letelier (ex ministro de Allende) en Estados Unidos ocurrido en septiembre de 1976, el 12 de agosto de 1977 se derogó el decreto de creación de la DINA considerando "*La conveniencia de estructurar de acuerdo a las actuales circunstancias del acontecer nacional las atribuciones de un Organismo creado en situación de conflicto interno ya superada*" [8]. En su reemplazo se creó la Central Nacional de Informaciones (CNI) prácticamente con los mismos objetivos de la DINA pero con dependencia del ministerio del Interior. Su primer Director fue Manuel Contreras quien fue reemplazado en noviembre de 1977 por el general en retiro Odlanier Mena (su curioso nombre corresponde a Reinaldo escrito al revés).

La llegada del General Mena transforma la sección de Computación en un centro de apoyo a la gestión de la Dirección con un fuerte respaldo financiero para

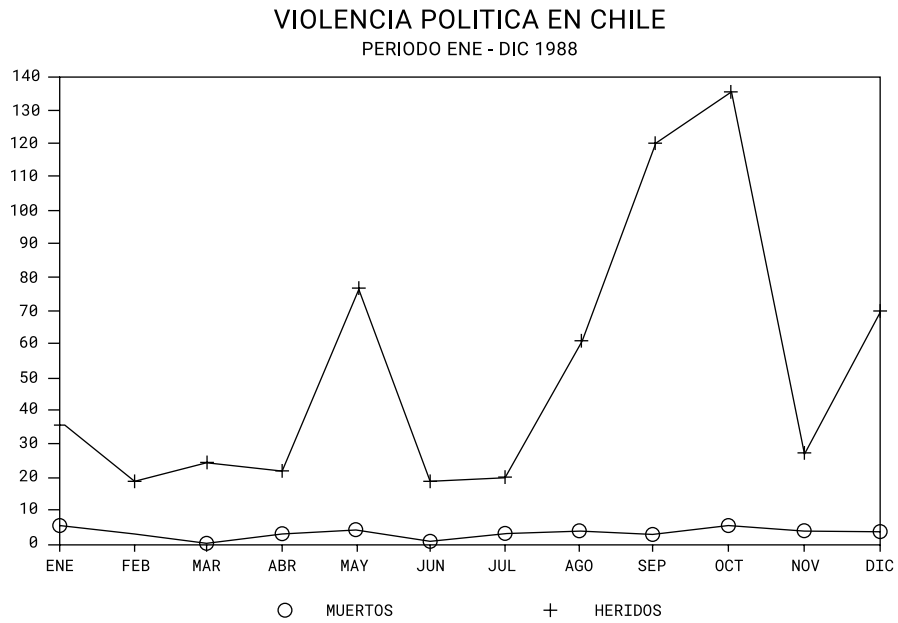


Figura 5. Estadísticas confeccionadas por la CNI.

equipamiento y contratación de personal. Según testimonio de Luz Arce, una ex detenida obligada a convertirse en agente, la sección se traslada a Vicuña Mackena N°69 y "se dotó a L-5 con un equipo más grande, que fue adquirido en la empresa COMDAT, representantes de la BASIC FOUR. Esta empresa además capacitó al personal de L-5" [9].

En 1985, se registra una nueva estructura organizacional de la CNI que incluye una División de Informaciones de la que depende una Brigada Informática que a su vez incluye una Unidad de Computación y una Unidad de Programadores [8]. De esta época hay evidencias del uso de los computadores en los archivos desclasificados [10] en diversos cuadros estadísticos, anuales e históricos, fueron realizados por computadores de los servicios de inteligencia, abarcando hasta el año del plebiscito de 1988 que marcó el comienzo del fin de la dictadura (ver Figura 5).

Adicionalmente, la computación también fue utilizada para impedir el ingreso de chilenos exiliados que se habían visto obligados a abandonar el país. Inicialmente, en los aeropuertos y puntos de entrada al país, se disponía de listados computacionales con la nómina de los chilenos con prohibición de ingreso. Posteriormente, debido a su tamaño y a la dificultad de su lectura, los listados fueron reemplazados por terminales conectados a un computador que disponía del archivo con las personas impedidas de ingresar. De hecho, al retornar la democracia, en las oficinas del Registro Civil se encontró una oficina con terminales que eran utilizados exclusivamente por agentes de la CNI [11].

Recién en el año 2013 se pudo conocer la nómina del personal de los servicios de Inteligencia [12]. En la DINA aparecen 1.131 personas: 1.050 hombres y 81 mujeres. Respecto de la CNI se consignan 2.073 personas: ejército (638), armada (29), aviación (33), carabineros (124), investigaciones (40), civiles (1.151), brigada Lautaro (40), grupo Delfín (18). Para gestionar esta información la CNI desarrolló un sistema computacional de administración del personal.

Computación en la defensa de los derechos humanos

Las acciones de defensa de los derechos de las personas comenzaron inmediatamente después del golpe de Estado. Posteriormente, y dada la magnitud de la represión y de la información relacionada, surgió la necesidad de utilizar la computación para apoyar las gestiones judiciales de defensa. Primero fue la Vicaría de la Solidaridad y seguidamente otras instituciones de defensa de los derechos humanos, las que llegaron a constituir la "Red de Informática de Instituciones de Derechos Humanos".

Vicaría de la Solidaridad

La fuerte represión posterior al 11 de septiembre de 1973 motivó la creación del "Comité de cooperación para la paz en Chile" ("Comité Pro Paz"), que realizó las primeras acciones de amparo y defensa de los derechos de las personas. El Comité, que agrupó a distintas iglesias, fue creado el 4 de octubre de 1973 y fue copresidido por el obispo católico Fernando Ariztía y por el obispo luterano Helmut Frenz. La dictadura forzó el fin del Comité que se vio obligado a dejar de funcionar el 31 de diciembre de 1975. En 1976, la Iglesia Católica creó la Vicaría de la Solidaridad para continuar con la labor que realizaba el Comité Pro Paz [13].

La Vicaría atendió a miles de personas generándose documentos con las denuncias y con las gestiones judiciales asociadas. El volumen de información motivó a la Vicaría a microfilmarla y a utilizar un computador para registrarla y gestionarla. En 1978 se inició un proyecto de sistematización y estandarización de los documentos a cargo de dos sociólogos. Los documentos fueron codificados en el plazo de un año por un equipo

de doce personas y digitados por cuatro personas durante tres meses. Los datos fueron finalmente traspasados desde diskettes hacia cintas magnéticas.

Al año siguiente, en 1979, un ingeniero informático desarrolló un sistema computacional para procesar la información. El alto costo de los computadores de la época obligó a arrendar horas de servicio en el Centro de Computación de la Universidad de Chile. Usando una estación de trabajo, conectada a un computador IBM-370/145 con sistema operativo VM/CMS, se desarrollaron programas en el lenguaje PL/I que validaron, depuraron y ordenaron la información. A comienzos de 1980, y en sesiones nocturnas "clandestinas", se emitieron las estadísticas iniciales y los primeros listados que se utilizaron para apoyar el trabajo jurídico y de análisis.

En 1981, y por razones económicas y de seguridad, la Vicaria adquirió un microcomputador Vector3 con memoria de 64K, una unidad para dos diskettes de 5.25 pulgadas y una impresora Centronics-739 (ver Figura 6). Usando el sistema operativo CP/M y el software dBase se agilizó el ingreso, la actualización y la consulta de la información. La Vicaría fue una de las primeras instituciones en adoptar la tecnología de microcomputadores en Chile, y en 1983 creó una unidad informática ("Procesamiento y Archivo") [14] a cargo de José Manuel Parada Maluenda (ver Figura 7), que fue asesinado por uno de los "Servicios de Inteligencia" en marzo de 1985.

En 1982, la Vicaría contrató un estudiante de último año de ingeniería en computación que se tituló al año siguiente en la Universidad de Chile con la versión en línea del sistema computacional [15]. En la memoria de título, el sistema se presentó de manera genérica de modo que pudiera ser aplicado en otros contextos, pero principalmente para evitar las posibles consecuencias represivas. En 1983 se desarrolló un sistema para la información sobre el exilio y se inició la entrega regular de informes sobre la represión. En 1986, el microcomputador Vector3 fue sustituido por un computador IBM/AT con 60 Mb de memoria en disco.

La Vicaría continuó su labor durante todo el período dictatorial y cerró sus puertas en 1992. Por su labor humanitaria recibió reconocimientos internacionales: premio Príncipe de Asturias de la Concordia (1986) y premio Simón Bolívar de la UNESCO (1988). A partir de 1990 sus archivos fueron utilizados para elaborar diversos informes que permitieron reparar en parte a las víctimas y sus familias por las violaciones a sus derechos por parte del Estado. Finalmente, en agosto de 1992, fue creada la "Fundación de Documentación y Archivo de la Vicaría de la Solidaridad" con el propósito de mantener y custodiar los documentos que forman parte de la memoria histórica nacional.

Red Informática de Instituciones de Derechos Humanos (RIIDH)

En los años ochenta otras organizaciones no gubernamentales de defensa de los derechos humanos comenzaron a usar computadores para apoyar su labor. Fue el caso de la "Fundación de Ayuda Social de las Iglesias Cristianas" (FASIC) creada en 1975 y en 1985 desarrolló un sistema computacional relacionado con los exiliados y sus familias y en 1986 un sistema de registro de los casos sobre presos políticos [11].

Figura 6. Microcomputador Vector3 como el utilizado en la Vicaría de la Solidaridad.

Figura 7. José Manuel Parada Maluenda (1950-1985).

Posteriormente, la "Comisión Chilena de Derechos Humanos" (CCHDH), creada en 1978, incorporó el computador en 1987 y desarrolló un sistema para registrar denuncias. El sistema fue construido aplicando una metodología desarrollada en la misma institución [16]. Por otra parte, el "Comité de Defensa de los Derechos del Pueblo" (CODEPU), creado en 1980, comenzó un proceso de computarización a fines de los años ochenta [17].

Desde 1984 comenzó a funcionar la "Red Informática de Instituciones de Derechos Humanos de Chile" (RIIDH) integrada por la Vicaría, FASIC, Comisión Chilena, CODEPU y otros organismos con el propósito de compartir hardware y software, cursos de capacitación y la realización de proyectos conjuntos. A través de los años la Red contó con el siguiente parque de computadores: 1 entre 1982 y 1984 (Vector3 de la Vicaría), 2 en 1985, 4 en 1986, 15 en 1987, 25 en 1988 y 30 en 1989 (16 computadores personales IBM, 13 compatibles y 1 no compatible). En total se disponía de 21 Mb de memoria RAM y 945 Mb en disco. Respecto del personal, en 1989 trabajaban 2 ingenieros, 4 analistas, 14 operadores y 22 digitadores [11].

Como parte del trabajo de coordinación y colaboración, la Red elaboró un "Glosario de definiciones operacionales de las violaciones a los derechos humanos" [18]. La cantidad y diversidad de vulneraciones a los derechos motivó la elaboración de una ontología (ver Figura 8) con una recomendación de su uso informático para poder compartir información y elaborar informes y estadísticas estandarizadas. Dada su trascendencia, la segunda edición

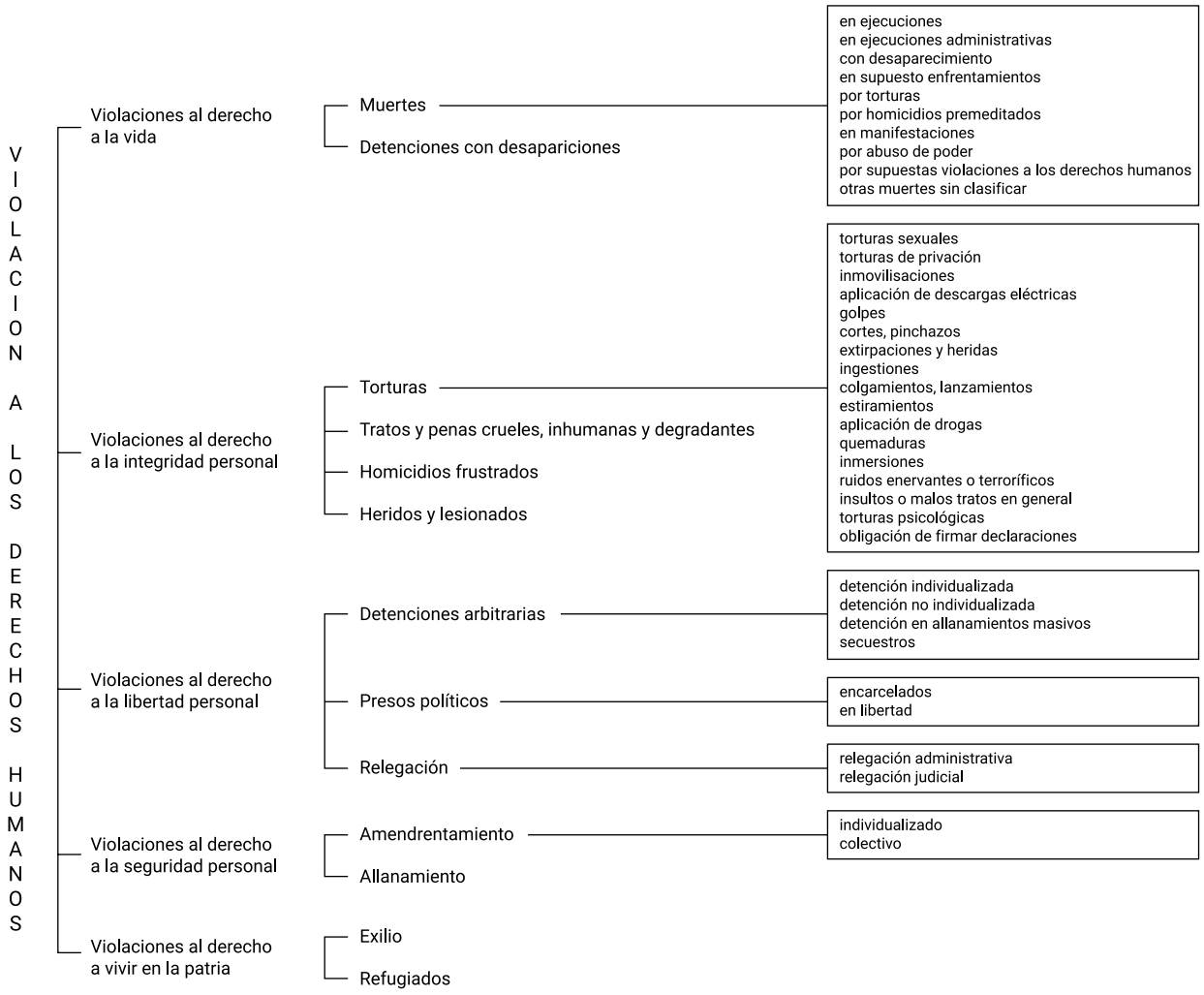


Figura 8. Ontología de Violaciones a los Derechos Humanos elaborada por RIIDH.

Figura 9. Seminario Latinoamericano de Derechos Humanos e Informática (septiembre de 1989).

del glosario incluyó versiones en los idiomas inglés y francés [19].

Seminario Latinoamericano de Derechos Humanos e Informática

En septiembre de 1989, FASIC organizó el "Primer Seminario Latinoamericano de Derechos Humanos e Informática" (ver Figura 9). El Seminario fue denominado "Jecar Neghme" en homenaje a un dirigente político que fue asesinado por esos mismos días a pocas cuadras del lugar del evento. El país aún vivía en un contexto de inseguridad casi un año después de que la dictadura había perdido el plebiscito que propiciaba su continuidad y cerca de la elección democrática de presidente y de parlamentarios.

El seminario contó con 22 delegados extranjeros de 9 países latinoamericanos. Por Chile participaron 67 personas de todas las instituciones de la Red chilena. El evento incluyó cuatro clases magistrales de destacadas personalidades chilenas: "La reconstrucción de la verdad" de Andrés Domínguez de la Comisión Chilena de Derechos Humanos, "Los registros de informaciones personales como violaciones al derecho a la vida privada" de Eduardo Novoa, "Información y desarrollo del movimiento de DH" de Hugo Früling de la Academia de Humanismo Cristiano, y "La comunicación humana y las redes tecnológicas" de Gabriel Rodríguez del Instituto Latinoamericano de Tecnología. Por otra parte, se presentaron 33 ponencias que fueron clasificadas y presentadas como investigaciones, demostraciones, e informes regionales, nacionales e institucionales. Por países, se presentaron 13 trabajos de Chile, 10 de Argentina, 2 de México, 2 de Perú, y 1 de Bolivia, Brasil, Costa Rica, Guatemala, Salvador y Uruguay (ver Tabla 3).

El Seminario alcanzó plenamente los objetivos iniciales: aprobar la creación de un banco de software, iniciar el proceso para crear una red de comunicaciones, preparar un libro que divulgue las ponencias, preparar un estudio que sintetice la experiencia regional en el uso de la computación en la defensa de los derechos humanos, impactar a la sociedad chilena sobre el tema de los derechos humanos [20]. La realización del Seminario solo fue informada por los escasos medios de prensa opositores en los últimos años de dictadura: los diarios Fortín Mapocho [21] y La Época [22].

Conclusiones

Durante el período de la dictadura chilena, entre los años 1973 y 1989, se registró una gran cantidad de violaciones a los derechos humanos que afectó a decenas de miles de personas. El gran volumen de información involucrada obligó a utilizar procedimientos informáticos y computadores, tanto en los servicios de seguridad del Estado, como en las instituciones no gubernamentales que defendieron los derechos de las personas.

País	Título	Autores	Institución
Argentina	Ventajas en el uso de formatos estándares	Daniel Frontalini	CELS
Argentina	Proyectos de investigación “vigencia de la memoria”	Ricardo Snitcofsky Enrique Fernández Graciela Fernández	APDH
Argentina	Sistema de archivo documental	Enrique Fernández R.Ilribarne Ricardo Snitcofsky	APDH
Argentina	Documentación del sistema de clasificación para el archivo periodístico	Daniel Frontalini	CELS
Argentina	El centro de documentación e información del Movimiento de DDHH	Berta Arroyo	MEDH
Argentina	Área de Informática del Equipo de Antropología forense	Rafael Mazzella Daniel Bustamante	Antrop. Forense
Argentina	Sistemas de búsquedas de datos genéticos	Rafael Mazzella	Plaza de Mayo
Argentina	Documentación bibliográfica	Juan J. Fariña	CEDDI
Argentina	Apuntes para un sistema de referencias y comunicación	Daniel Frontalini	CELS
Argentina	DH y la transición democrática	Rafael Mazzella	
Bolivia	Base de datos para juicios de responsabilidades	Waldo Berríos	CESEM
Brasil	El uso del computador en DDHH	Ricardo Brito	GAJOP
Chile	Los sistemas de información y las organizaciones de DDHH	Óscar Montealegre	CCHDH
Chile	Glosario de definiciones operacionales de las violaciones a los DDHH	Cecilia Jarpa	CODEPU, RIIDH
Chile	Proposición de una metodología para desarrollo de sistema de información	Óscar Montealegre	CCHDH
Chile	Descripción general de un sistema de información para el registro de las violaciones a DDHH	Óscar Montealegre Elena Fouquet	CCHDH
Chile	Automatización de la información sobre legislación y sentencias judiciales	Juan G. Hurtado	Vicaría
Chile	Utilización de Redes: la experiencia de organizaciones no gubernamentales	Alberto Cabezas	ILET
Chile	La red de información sobre Chile	Steve Anderson	CHIP
Chile	Guía de organizaciones de DDHH de AL y el Caribe	Juanita Chacón Patricio Orellana Gloria Alberti	FASIC FASIC AHC
Chile	El uso de la informática en la defensa de los DH en América Latina	Patricio Orellana	FASIC
Chile	Informática y DDHH, el caso de Chile	Patricio Orellana	FASIC
Chile	Registro e informática en fundación de “Protección a la Infancia Dañada por los Estados de Emergencia”	PIDEE	PIDEE
Chile	Experiencia de la Vicaría de la Solidaridad en la sistematización y procesamiento de la información	Carmen Garretón	Vicaría
Chile	Los formatos estándar de HURIDOCS para registro de información sobre violaciones a DDHH	Ricardo Cifuentes	HURIDOCS
Costa Rica	Uso de la informática en la defensa de los DDHH en Centroamérica	Florencia Castellanos	CODEHUCA
Guatemala	Integración de la informática en el trabajo de DDHH	Antonio Andrade	CDHG
México	HURIDOCS, Sistema Internacional de Información y Documentación sobre DDHH	Aída M. Noval	HURIDOCS
México	Informe de México	Aída M. Noval	AMDH
Perú	Informe del Centro de Estudios y Acción para la Paz	Mariella Ruiz	CEAPAZ
Perú	Uso de la Informática en la Asociación Pro DDHH	Rosario Narváez	APRODEH
Salvador	Labor de investigación, documentación y denuncia de la CDHES	Joaquín Cáceres	CDHES
Uruguay	La informática en la lucha por Verdad y Justicia	Adrián Manera	SERPAJ

Tabla 3. Ponencias presentadas en el Seminario de Derechos Humanos e Informática (septiembre de 1989).

Los servicios de seguridad del Estado (SENDET, DINA, CNI) utilizaron poderosos computadores para registrar la información de los prisioneros y de las personas buscadas por razones políticas. Adicionalmente, y considerando que varios países de Sudamérica tenían también dictaduras militares, la DINA organizó y coordinó tempranamente la "Red Cóndor" que utilizó un banco de datos, una red de télex y un gran computador central con el propósito de compartir la información de personas y facilitar la realización de operaciones fuera de los países.

Las organizaciones no gubernamentales de defensa de los derechos humanos se vieron también en la necesidad de utilizar computadores para registrar y analizar la información y apoyar las acciones de defensa de las personas. La Vicaría de la Solidaridad fue inicialmente usuaria de un servicio computacional público donde desarrolló un primer sistema de información. Posteriormente, con la llegada de los primeros "microcomputadores" al país, la Vicaría, el FASIC, la Comisión Chilena, el CODEPU y otras instituciones adquirieron y utilizaron computadores para desarrollar sus sistemas de una manera más segura y económica. La necesidad de coordinación llevó a crear una Red Informática donde compartieron recursos, participaron en la elaboración de un glosario y presentaron ponencias en el Primer Seminario Latinoamericano de Derechos Humanos e Informática.

En síntesis, más que computadores "amigos y enemigos", hubo instituciones y personas que utilizaron la tecnología informática computacional para apoyar la represión o la defensa de los derechos humanos. Terminada la dictadura chilena la información generada por los sistemas computacionales "amigos" sirvieron para reparar en parte a las víctimas y a sus familias por la vulneración que sufrieron de sus derechos [23] [24]. ▪

Acto Informática y Derechos Humanos en Chile, 1973-1989

El 9 de septiembre de 2019 en el Museo de la Memoria y los Derechos Humanos, se realizó el acto "Informática y Derechos Humanos en Chile, 1973-1989" (ver Figura 10) con el propósito de conocer y reconocer la labor de las instituciones y las personas que valiente y anónimamente utilizaron la tecnología informática para apoyar la defensa de los derechos humanos. Participaron como panelistas Carmen Garretón, Marco A. Montecinos, Patricio Orellana y quien escribe, Juan Álvarez, como moderador (ver Figura 11).

Figura 10. Acto Museo de la Memoria.

Figura 11. Juan Álvarez, Marco A. Montecinos, Carmen Garretón y Patricio Orellana.

REFERENCIAS

[1] Piquer, Alfredo. "Computadores: ¿Amigos o enemigos?". Revista Mensaje. Diciembre 1978.

[2] Álvarez, Juan. "Empresa Nacional de Computación e Informática (ECOM), 1971-1973". Revista Bits N°13. 2016. https://www.dcc.uchile.cl/Bitsdeciencia13.pdf

[3] Salazar, Manuel. "Las letras del horror – Tomo I: La DINA". Editorial LOM. 2014.

[4] Soto, Hernán; Villegas, Sergio. "Archivos secretos: documentos desclasificados de la CIA". Editorial LOM.

[5] Contreras, Manuel. "La verdad histórica – El ejército guerrillero". Ediciones Encina. 2000.

[6] "Primera Reunión de trabajo de inteligencia nacional". En archivos encontrados en Paraguay. Octubre 1975.

[7] Dinges, John. "Operación Cóndor". Ediciones B Chile. 2004.

[8] Salazar, Manuel. "Las letras del horror – Tomo II: La CNI". Editorial LOM. 2014.

[9] Arce, Luz. "El infierno". Planeta. 1993.

[10] Doeart, Carlos; Weibel, Mauricio. "Asociación ilícita – Los archivos secretos de la dictadura". Ceibo ediciones. 2012.

[11] Orelllana, Patricio. "Informática y Derechos Humanos: el caso de Chile". Documentos Primer Seminario Latinoamericano de Derechos Humanos e Informática". Ediciones FASIC. 1991.

[12] Escalante, Jorge; Guzmán, Nancy; Rebolledo, Javier; Vega, Pedro. "Los crímenes que estremecieron a Chile". Ceibo ediciones. 2013.

[13] Gutiérrez, Paulina. "Institución, derechos humanos y dictadura: Vicaría de la Solidaridad del Arzobispado de Santiago de Chile". Tesis Maestría Psicología Social, Universidad Autónoma Metropolitana. México, 1997.

[14] Garretón, Carmen. "Experiencia de la Vicaría de la Solidaridad en la Sistematización y Procesamiento de la Información". Documentos Primer Seminario Latinoamericano de Derechos Humanos e Informática". Ediciones FASIC. 1991.

[15] Mejías, Rodolfo. "Sistema de Ingreso y validación en línea y construcción de un banco de datos como aplicaciones de un microcomputador". Memoria Ingeniería de Ejecución en Procesamiento de la Información. U. de Chile. 1983.

[16] Montealegre, Hernán. "Proposición de una Metodología para utilizar en el desarrollo de sistemas de información". Documentos Primer Seminario Latinoamericano de Derechos Humanos e Informática". Ediciones FASIC. 1991.

[17] Montecinos, Marco A. "Informática en el Comité de Derechos del Pueblo". Presentación en el Acto "Informática y Derechos Humanos en Chile, 1973-1989". Septiembre de 2019.

[18] Jarpa, Cecilia. "El Glosario de definiciones operacionales de las violaciones a los derechos humanos". Documentos Primer Seminario Latinoamericano de Derechos Humanos e Informática". Ediciones FASIC. 1991.

[19] Red de Informática de instituciones de Derechos Humanos de Chile. "Glosario de definiciones operacionales de las violaciones a los derechos humanos". Ediciones FASIC. 1991.

[20] Orelllana, Patricio. "Saludo de clausura". Documentos Primer Seminario Latinoamericano de Derechos Humanos e Informática". Ediciones FASIC. 1991.

[21] "La computación ayuda a respetar derechos humanos". Diario Fortín Mapocho. 10/9/1989.

[22] "Es vital computarizar defensa de los derechos humanos, afirma seminario". Diario La Época. 10/9/1989.

[23] "Informe Rettig: Informe de la Comisión Nacional de Verdad y Reconciliación". 1991. https://bibliotecadigital.indh.cl/handle/123456789/170

[24] "Informe Valech: Informe de la Comisión Nacional sobre Prisión Política y Tortura". 2005. https://bibliotecadigital.indh.cl/handle/123456789/455

¿Quieres recibir un ejemplar de Revista Bits de Ciencia?

Escríbenos a revista@dcc.uchile.cl con los datos de envío.

También puedes acceder a la versión digital en
https://www.dcc.uchile.cl/bits-de-ciencia

REVISTA DEL DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN DE LA UNIVERSIDAD DE CHILE

Bits DE CIENCIA