Módulo 1: Definiciones

1.1. ¿Qué es la privacidad?

Hola, soy Laura Siri y te agradezco tu interés por el último curso de Vía Libre del año, dedicado a debatir los desafíos actuales en torno a la privacidad, la vigilancia (o, más bien, *vigilantismo*), cómo incide la tecnología en estas cuestiones y qué repercusión tiene todo esto para el ejercicio de los derechos humanos.

¿Qué contestarías si te pregunto qué es la privacidad? Me encantaría que nos dijeras en el foro tu respuesta y, mientras tanto, te cuento que para muchos directivos de grandes empresas tecnológicas la suya parece ser "algo que no existe, que no debe existir y, si existe, ya nos encargaremos de liquidar". Algunos ejemplos:

- En el 2000, el entonces gerente general de la compañía Sun Microsystems, Scott McNeally, dijo: "*la privacidad ha muerto, supérenlo*".
- Larry Ellison, fundador de otra gran tecnológica, Oracle, dijo en 2001: "*Bien, esta privacidad que les preocupa es en gran medida una ilusión. Y todo lo que deben abandonar son sus ilusiones, no su privacidad. Ahora mismo pueden ir a Internet y conseguir un informe de crédito sobre su vecino y averiguar dónde trabaja, cuánto gana, si está al día con su hipoteca y un montón más de información*". Casualmente, Sun Microsystems fue comprada por Oracle, pero eso es otra historia.
- En 2010, el exgerente general de Google, Eric Schmidt, dijo: "*nos das más información sobre ti y sobre tus amigos, y podemos mejorar la calidad de nuestras búsquedas. No necesitamos que tipees nada. Sabemos dónde estás. Sabemos dónde has estado. Podemos saber aproximadamente en qué estás pensando*".
- En el mismo año, el fundador de Facebook, Mark Zuckerberg, sugirió que la privacidad ya no constituye una "norma social".
- Su hermana Randi, exdirectora de marketing de la compañía, fue aún más lejos al año siguiente cuando expresó que: "*el anonimato en Internet tiene que desaparecer*" porque, en su opinión, la gente se comporta mucho mejor si no se le permite ocultar su nombre real.

Generalmente, como ves, no definen qué es esa cosa que debe desaparecer o que ya desapareció. O bien resaltan solo un aspecto de la privacidad, como si ésta no fuera un derecho multidimensional y contextual. La verdad es que existen diferentes formas de privacidad, así como numerosos conceptos vinculados, pero no sinónimos ni antónimos lineales. Por ejemplo, intimidad, secreto y anonimato. Hay un trabajo de la British Royal Academy of Engineering (2007) que, sin ser el único ni necesariamente el mejor, resulta útil para comenzar a hacer distinciones en función de "*aquello que uno quiere mantener privado*". Así, se puede entender la privacidad como:

- ***confidencialidad***: cuando queremos mantener en secreto cierta información sobre nosotros o sobre terceros.
- ***anonimato***: representa la intención de que algunas de nuestras acciones no puedan ser relacionadas con nosotros como individuos específicos. Es muy combatido por las empresas de Internet, que quieren tener datos veraces de todos para poder segmentar publicidad. Y también por las agencias de seguridad que, virtualmente, consideran sospechoso a todo aquel que no quiere aparecer online con su nombre verdadero. Sin embargo, el anonimato online es imprescindible muchas veces para garantizar efectivamente el derecho a la libertad de expresión y el disenso político.
- ***identidad***: podemos querer mantener nuestra identidad desconocida por cualquier razón, incluso cuando queremos separar nuestra identidad personal de la de una función pública. Las discusiones al respecto también surgen en el marco, por ejemplo, de los documentos "de identidad" obligatorios y biométricos (que, en realidad, son de "identificación", que no es lo mismo).
- ***autodeterminación***: podemos considerar que algunas de nuestras acciones, actitudes y comportamientos son asunto nuestro y no incumben a nadie más (esos otros pueden ser desde empleadores hasta el Estado). No necesariamente implica ocultar un secreto (aunque el derecho a tener secretos también debería ser reivindicado).
- ***libertad de "ser dejado tranquilo"***: es una acepción de privacidad muy clásica, ya que fue enunciada de este modo en un famoso ensayo de los jueces Samuel Warren y Louis Brandeis en 1890. Implica poder dedicarnos a nuestros asuntos sin ser escrutados por parte de nadie. Curiosamente, fue motivada por la aparición de un invento técnico: la cámara de fotos personal. Los mencionados juristas de Estados Unidos, con agudeza aún hoy vigente, decían que *"La soledad y la privacidad se han hecho más esenciales para el individuo; pero la empresa moderna y la invención, a través de la invasión de su privacidad, lo han sometido al dolor mental y el stress, mucho más de lo que podría infligir una mera herida corporal"*.
- ***control de los datos personales***: se relaciona con el derecho a controlar la información que circula sobre nosotros (ej.: dónde se almacena, quién la ve, quién se asegura de que sea correcta, etc.). Por ejemplo, todos encontramos perfectamente correcto que nuestro médico conozca qué medicamentos tomamos. Pero muchos encontramos chocante y peligroso que haya empresas dedicadas a transcribir y almacenar en bases de datos, para luego venderlo, el historial de consumo farmacológico de cada ciudadano.

En general, más allá de qué es lo que "queremos mantener privado", lo importante es que esa voluntad siempre depende de un contexto. En efecto, como dice Helen Nissenbaum en su libro "Privacidad amenazada", una acción o práctica viola nuestra privacidad en función del contexto en el cual la actividad tiene lugar y también según cuál sea el tipo de información en cuestión y los roles sociales en los que las personas están inmersos. Los contextos sociales, tales como los de los servicios de la salud, la educación, el comercio y la religión, se rigen por normas sociales complejas y relaciones de poder. La privacidad, o integridad contextual, tiene que ver entonces con un subconjunto de dichas normas vinculado con los riesgos del traspaso de ciertas "fronteras" informacionales. Este tipo de normas prescriben cómo ciertos tipos de información sobre ciertas

personas específicas, actuando en roles específicos, deben fluir entre las demás personas. Por ejemplo, en un contexto de amistad, los amigos comparten recíprocamente informaciones, no por obligación, sino por elección. Si lo que uno habla con sus amigos saliera de contexto, esas mismas informaciones funcionarían de modo muy distinto. El problema es que hoy en día sí salen de contexto habitualmente, solo que no prestamos atención. Porque, por ejemplo, cuando creemos estar hablando en privado con amigos en Facebook resulta que hay robots de esa plataforma haciendo análisis textual para encontrar piezas de información de valor comercial, y también hay autómatas de organismos de seguridad nacionales y extranjeros tratando de detectar actividad "sospechosa".

Entonces, de acuerdo con la teoría de la integridad contextual de Nissenbaum, las mencionadas normas informacionales establecen expectativas contra las cuales ciertas acciones y prácticas son confrontadas. En particular, brindan una guía para evaluar nuevas prácticas sociotécnicas, cuyo respeto por la integridad contextual de los sujetos involucrados es juzgado de acuerdo con varios factores:

- El contexto que las rige
- Si la nueva práctica cambia los tipos de información en cuestión
- Si la nueva práctica causa un giro en quiénes están involucrados como remitentes, destinatarios o sujetos de la información
- Si los nuevos patrones del flujo de información encajan con los principios relevantes para la transmisión

Entonces, cuando uno tiene la impresión de que ciertas prácticas sociotécnicas son violatorias de la privacidad es porque son percibidas como violatorias de normas informacionales que se asumen como apropiadas en determinado contexto, sostiene Nissenbaum.

Pero los contextos y la consecuente necesidad de repensar qué es la privacidad vienen cambiando a medida que también cambian las posibilidades técnicas:

- En cierto momento, lo "inviolable" (salvo casos especificados por ley y con garantía judicial) era apenas lo que la cuarta enmienda de la constitución de los Estados Unidos predica. Es decir, el domicilio, los papeles privados, las posesiones personales que uno lleva consigo, el cuerpo.
- Warren y Brandeis introdujeron los componentes de autonomía y aislamiento.
- Con el creciente uso de los teléfonos, se comenzó a discutir la privacidad en las telecomunicaciones.
- Las tecnologías de la información, con la posibilidad de confeccionar bases de datos personales, dieron lugar a un nuevo enfoque: la "privacidad informacional".
- Las luchas por los derechos de los gays y a favor de la despenalización del aborto también dieron lugar a argumentaciones basadas en la "privacidad", esta vez ancladas en el derecho de cada uno a hacer lo que quiera con su cuerpo sin que otros se inmiscuyan.
- El clásico "derecho a ser dejado en paz" experimenta una reactualización a medida que las cámaras de vigilancia se vuelven omnipresentes.
- Con la existencia de dispositivos con capacidad de geolocalización, como los modernos

teléfonos móviles, aparece el concepto de “privacidad de las ubicaciones” y la controversia acerca de si uno puede o no tener expectativa de privacidad cuando se encuentra en lugares públicos, como la calle.
- La privacidad como confidencialidad resurge en los debates a medida que crece la conciencia de cómo nos espían las redes sociales online y los sitios de comercio electrónico.
- Las historias clínicas digitales también han generado debates, en este caso debido a que ya no solo el médico tratante tiene acceso a los datos de salud.
- Las presiones en distintas partes del mundo para implementar sistemas de voto electrónico dispararon dudas acerca de cómo dichos sistemas podrían comprometer el secreto del sufragio. Esos debates mostraron particularmente cómo la falta de privacidad puede comprometer seriamente la mismísima democracia.
- La privacidad corporal no solo está puesta en cuestión por el creciente uso de biometría y recolección de ADN con diversos fines, sino también con los experimentos que hay en neurotecnología, que hacen abogar por una “privacidad de la mente”.

También hay que tener en cuenta que los riesgos para la privacidad generados por una de las prácticas previamente enumeradas interactúan sistémicamente con aquellos generados por las demás, y que una pieza discreta de información personal, recolectada en determinado momento y contexto, podría perfectamente terminar siendo usada para otros distintos y en combinación con otras piezas de información para conocer aún más íntimamente todas las particularidades de la vida de las personas.

1.2. ¿Por qué es importante que hablemos de privacidad?

La privacidad no necesariamente es un fin en sí mismo, sino que puede ser vista como un medio para obtener un fin. Y dicho fin no tiene por qué ser un beneficio individual, como el enfoque de “dejar tranquilo” podría dejar traslucir. Más bien, la privacidad importa por la función social que cumple para permitir la libertad y la democracia.

Quizá oíste hablar de Edward Snowden, el excontratista de los servicios de inteligencia de Estados Unidos que, en 2013, reveló cómo ese país espía las comunicaciones online de gran parte de la población mundial (y, si no, no te preocupes que volveremos sobre él en otro módulo). Él dijo que hay al menos dos razones para oponerse a la invasión de la privacidad. La primera es que, evidentemente, la gente modera su conducta cuando sabe que la vigilan. “Bajo observación, actuamos de modo menos libre, lo que significa que efectivamente somos menos libres”, dijo. La segunda es que si se están recolectando todos los datos de todos, se están creando registros permanentes de nuestras vidas, aunque no seamos sospechosos de nada. Así, si algún día sí somos objetos de una investigación, ya será abstracto nuestro derecho de no declarar contra nosotros mismos porque nuestro registro ya habrá declarado todo lo declarable, y más. “Quizá no recuerdes dónde fuiste a cenar el 12 de junio de 2009, pero el gobierno sí se acuerda”, ejemplificó Snowden.

Según el libro de Helen Nissembaum que ya citamos, (2010: 98), la privacidad es fundamental para el ejercicio de:

- **La individualidad**: porque la oportunidad de un desarrollo personal satisfactorio, creativo y saludable depende en gran parte de la posibilidad de experimentar sin el temor a la desaprobación, censura o el ridículo y, sobre todo, sin la presión de adecuarse constantemente a las normas convencionales. La exposición exacerbada produce que los individuos repriman actitudes, comportamientos o pensamientos para evitar represalias tales como la pérdida de un trabajo o el aislamiento social.
- **La autonomía**: la privacidad es de hecho una manera de mantener la autonomía con respecto a cierta información que una persona considera que no debe ser revelada a terceros. El valor que ha adquirido la información en la actualidad amenaza directamente la autonomía y por lo tanto la privacidad de las personas, ya que las empresas y los gobiernos manipulan los datos personales sin el consentimiento consciente de los individuos.
- **Las relaciones sociales**: la autonomía de alguien para disponer de los elementos que conforman su vida privada le permite revelar voluntariamente a ciertas personas y en ciertos contextos la información personal que considera oportuna, útil y necesaria.
- **La participación política**: la privacidad es un valor esencial de todo sistema social y político legítimo. Es un valor público en la medida en que es constitutivo de otros derechos tales como la libertad de asociación y de discurso, y sobre todo de la votación secreta sobre la que se funda la democracia. La privacidad además protege a los individuos de intromisiones por parte del gobierno y de las empresas.

La privacidad, por lo tanto, es fundamental para evitar las consecuencias que puedan resultar de los errores deliberados o accidentales que surgen de la acumulación de datos, así como de las malas interpretaciones y prejuicios. También es imprescindible para protegerse de posibles extorsiones y abusos de poder por parte de las personas físicas y jurídicas que acceden a los datos. Y, por qué no, para evitar ser nada más que “prospectos” dentro de un esquema comercial que puede ser muy agresivo, aunque su aspecto sea amigable, como en el caso de las redes sociales online. La falta de privacidad, en suma, amenaza todos los derechos humanos que apreciamos.

1.3. Algunos malentendidos sobre la privacidad: “no tengo nada para ocultar”

El típico argumento “no tengo nada que ocultar” suele expresarse así: “si no tienes nada que ocultar, no tienes nada que temer”. Hay que imaginar que quienes dicen eso en su casa no usan cortinas, o que le dan su número de tarjeta de crédito a todo el mundo. Pero en general se usa a la hora de justificar intromisiones para hacer “prevención” en materia de seguridad. También lo dicen muchos cuando reflexionan “a quién le puede importar lo que diga en las redes sociales un don nadie como yo, si me quieren espiar, adelante”. Lógicamente, si lo que dice online un “don nadie” fuera de tan

poco valor, ¿por qué habrían de espiarlo?

El jurista norteamericano Daniel Solove escribió un maravilloso ensayo en 2011 para refutar el argumento “no tengo nada que ocultar”. Allí señala que obedece a la confusión de suponer que la privacidad supone el derecho de alguien a esconder algo desdoroso sobre su persona. Y, aunque sí es posible que uno tenga tal derecho en muchas situaciones, como hemos visto la privacidad no es eso, o no es solo eso.

Solove también señala que otra falacia es suponer que el interés de la seguridad siempre sobrepasa el interés por la privacidad. Sin embargo, no todas las medidas de seguridad apuntan a prevenir el mismo tipo de amenazas. El terrorismo, por ejemplo, no suele prevenirse apropiadamente por el simple expediente de cercenar la privacidad de la parte mayor posible de la población mundial. Además, también es una falacia el pensamiento de “todo o nada”. Porque es posible respetar salvaguardas como que no todo tipo y cantidad de datos sean almacenados, que no se los almacene por tiempo indeterminado, que se reconozca el derecho de los sujetos a enmendar o eliminar datos innecesarios, que se pueda solicitar informes de qué datos sobre uno tiene una entidad en su poder, o que los datos recolectados para un propósito no sean reutilizados para otro. Nada de esto tiene por qué comprometer ni disminuir la seguridad. Más aún, para garantizar la seguridad de los individuos, muchas veces se necesita implementar mayores medidas de privacidad, no menores. Esto es particularmente cierto en el mundo online, donde una suplantación de identidad podría conducir, por ejemplo, a que otra persona utilice la propia cuenta de banco en Internet o adquiera cosas en eBay.

Ya en 1990, el profesor Gary Marx enumeró una serie de falacias que rodean las discusiones sobre privacidad, vigilancia y tecnología, que conviene recordar, ya que la de “no tengo nada que ocultar” dista de ser la única. He aquí algunas:

- La falacia de pensar que el significado de una tecnología se apoya solamente sobre sus aspectos prácticos o materiales y no sobre su simbolismo social y referentes históricos.
- La falacia «frankensteiniana» de que la tecnología siempre será la solución y nunca el problema.
- La falacia de la tecnología es neutra.
- La falacia de que el consenso y la homogeneidad sociales hacen inexistentes los conflictos y divisiones y que lo bueno para quienes tienen el poder económico y político es bueno para todo el mundo.
- La falacia del consentimiento implícito y la libre elección.
- La falacia legalista de que sólo porque uno tiene derecho legal a hacer algo entonces es correcto hacerlo.
- La falacia de creer que la información personal de clientes y casos en posesión de una compañía es sólo una clase más de propiedad para ser comprada y vendida del mismo modo que los muebles de oficina o los insumos.
- La falacia de no ver los factores sociales y políticos involucrados en la recolección y construcción de los datos.

- La falacia de suponer que, dado que nuestras expectativas sobre la privacidad están históricamente determinadas y son relativas, entonces se harán necesariamente cada vez más débiles a medida que la tecnología se vuelva más poderosa.

En síntesis, no se trata de defender paranoicamente la privacidad como una esfera de privilegio individual, sino de destacar que sin ella no hay posibilidad de ejercer otros derechos humanos ni de vivir en democracia.

1.4. La tensión entre privacidad y seguridad

Básicamente, la seguridad involucra, en primer lugar, la protección de las personas contra daños o muerte por parte de otras personas y, en segundo lugar, la protección de los objetos y propiedades contra hurto, daño o destrucción ilegales. Como se supone que estas protecciones actúan a favor de la sociedad como un todo, suele argumentarse que valen más que el respeto por la simple privacidad del individuo, en especial si se tiene en cuenta la seriedad atribuida a ciertas amenazas actuales.

Sin embargo, proteger la privacidad de los individuos, como hemos ya argumentado, genera externalidades positivas para toda la sociedad, no solamente para los sujetos directamente afectados. Así lo explica Daniel Solove en el artículo que ya hemos citado:

"E*l valor de proteger al individuo es social. La sociedad involucra una gran dosis de fricción y estamos constantemente chocando unos con otros. Parte de lo que hace a una sociedad un buen lugar para vivir es cuánto permite a la gente tener libertad contra la intrusión de otros. Una sociedad sin protección de la privacidad sería sofocante y podría no ser el lugar donde la mayoría querríamos vivir*".

Otra cuestión que debemos resaltar es que, muchas veces, privacidad y seguridad no solo no son antagónicos, sino que son casi sinónimos. Ya en 1994 el investigador Roger Clarke subrayó que "*la visibilidad creciente de los hábitos y movimientos de la gente crea oportunidades para los ladrones y los extorsionadores, secuestradores y asesinos para realizar sus delitos con un riesgo mínimo para sí mismos*". No hay, por lo tanto, seguridad personal sin privacidad.

Del mismo modo, cuando la seguridad personal de jefes de estado, embajadores y otros funcionarios gubernamentales se ve comprometida por una incursión contra su privacidad (por ejemplo, por un acceso ilegítimo en sus comunicaciones), también puede verse afectada la seguridad nacional. Es otro ejemplo de que menos privacidad puede conducir a menos seguridad, en este caso no solo para el individuo afectado. De hecho, defender la privacidad puede ayudar mucho en el mantenimiento de la seguridad.

Por lo tanto, es falaz oponer genéricamente los valores de la privacidad y de la seguridad. Más aún, siempre es crucial identificar con precisión el tipo y la gravedad de la supuesta amenaza a la seguridad en juego e identificar apropiadamente los riesgos para el ejercicio democrático y los derechos humanos que la solución propuesta pudiera implicar. También es preciso no confundir

entre tipos de seguridad muy diferentes, como la seguridad nacional, la seguridad personal y la prevención del crimen. Por ejemplo, una intromisión en la privacidad que pudiera ser inevitable y necesaria en caso de una emergencia epidemiológica grave sería mucho más difícil de justificar solo para prevenir el crimen común. Y también sería muy cuestionable si, una vez solucionada esa eventual epidemia infecciosa, los datos personales recolectados con el fin de eliminarla se reutilizaran para usos comerciales o de prevención criminal, entre otros posibles.

La metáfora del "balance"

Es fundamental desarticular la idea, comúnmente enunciada al debatir estos temas, de que "hay que encontrar un balance entre seguridad y privacidad". O, como expresó el presidente de Estados Unidos, Barack Obama en un intento de defender el programa de espionaje masivo PRISM de la NSA: "*es importante reconocer que uno no puede tener un 100 por 100 de seguridad y también un 100 por 100 de privacidad, con cero inconveniencias. Vamos a tener que hacer algunas elecciones como sociedad*".

Una aguda refutación de esta manera de pensar se encuentra en el artículo "After Snowden: Rethinking the Impact of Surveillance", de Zygmunt Bauman, Didier Bigo, David Lyon y otros coautores. Allí establecen que:

"No se trata de una elección entre mercaderías en un mercado. Las invocaciones retóricas a un balance simplemente oscurecen y amenazan lo que ocurre con lo que puede ser el lugar más importante e intenso, pero desatendido, de la práctica democrática moderna. Se abre luego el camino para reinvindicaciones de facto de que las responsabilidades de la soberanía están en quienes están a cargo de nuestra seguridad y que el espacio de negociación abierto para aquellos presuntamente asegurados debe reducirse".

Por supuesto, quienes están a cargo de la seguridad pública también tienen muchas maneras de resaltar algunas supuestas amenazas por sobre otras, y así seguir naturalizando la también supuesta necesidad de un "balance" o negociación entre derechos. Todo esto en un creciente marco de secreto para quienes ejercen el poder, mientras se incrementa la transparencia para los ciudadanos comunes, cuando debería ser exactamente al revés. El lenguaje metafórico del "balance", por lo tanto, como es común en el lenguaje metafórico en general, tiende a naturalizar una asimetría de poder impropia de lo que se supone que es la democracia, bajo la forma de una asimetría de información. Es una forma de hablar cuya conclusión evidente es que la privacidad es intrínsecamente insegura, que es un obstáculo para la plena seguridad. Y a la hora de definir políticas concretas seguramente la carga de la prueba estará a cargo de quienes abogan por el respeto a la privacidad. Deberán demostrar que, en una situación dada, el respeto por la privacidad no afecta la seguridad.

Finalmente, señalan Bauman, Bigo *et al*. en el artículo antes citado, están los problemas prácticos que debe enfrentar cualquiera que intente empíricamente "balancear" la seguridad y la privacidad de una manera que no sea ni arbitraria ni subjetiva. Por ejemplo:

- ¿Qué unidad de medida comparable debería asignarse a cada concepto?

- ¿Dichos valores se incrementarían o decrecerían a tasas constantes?
- La utilidad que asignemos a los cambios en cada concepto, ¿permanece constante independientemente del nivel de seguridad y privacidad que haya en el estado inicial y el final?
- ¿Permanece constante la naturaleza y el valor de dichos bienes durante y después del acto de "balanceo"?
- ¿Cuántas unidades de seguridad equivalen a cuántas unidades de privacidad?

Como queda claro, el concepto de "balance" entre privacidad y seguridad carece de ninguna regla o fórmula clara, consistente y no controversial para resolver situaciones prácticas, ni queda claro quién ni cómo debe llevar a cabo legítimamente dicha negociación.

1.5. El derecho a la privacidad en los tratados internacionales de Derechos Humanos

La privacidad, al menos bajo algunas de sus modalidades, es un derecho humano fundamental reconocido en diversos tratados internacionales. Por ejemplo, el artículo 12 de la **Declaración Universal de Derechos Humanos** de 1948, dice que:

Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Por otra parte, el **Pacto Internacional de Derechos Civiles y Políticos**, que entró en vigor en 1976, dice en su artículo 17:

1. *Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.*
2. *Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.*

En Europa, rige un **Convenio para la Protección de los Derechos Humanos y de las libertades fundamentales** que, en su artículo 8, dice:

1. *Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.*
2. *No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.*

La **Convención Americana sobre Derechos Humanos**, más conocida como **Pacto de San José de Costa Rica**, de 1969, dice en su artículo 11 que:

1. *Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.*
2. *Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.*
3. *Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.*

Con respecto a la privacidad en menores de 18 años, la **Convención Internacional sobre los Derechos del Niño** de 1989, en su artículo 16, establece que:

1. *Nadie tiene derecho a invadir, sin una razón legal, tu privacidad, es decir, tu vida privada o tu vida familiar. Tu casa, tu correo, así como tu honor y tu reputación, constituyen tu privacidad y están igualmente protegidos.*
2. *El estado debe crear leyes que protejan todos los aspectos de tu privacidad.*

Señalemos también la **Convención internacional sobre la protección de los derechos de todos los trabajadores migratorios y de sus familiares**, de 1990, que dice en su artículo 14:

Ningún trabajador migratorio o familiar suyo será sometido a injerencias arbitrarias o ilegales en su vida privada, familia, hogar, correspondencia u otras comunicaciones ni a ataques ilegales contra su honor y buen nombre. Todos los trabajadores migratorios tendrán derecho a la protección de la ley contra tales injerencias o ataques.

Finalmente, es interesante citar el artículo 14 de la **Declaración Internacional sobre los Datos Genéticos Humanos**, de 2003:

a) Los Estados deberían esforzarse por proteger la privacidad de las personas y la confidencialidad de los datos genéticos humanos asociados con una persona, una familia o, en su caso, un grupo identificables, de conformidad con el derecho interno compatible con el derecho internacional relativo a los derechos humanos.

b) Los datos genéticos humanos, los datos proteómicos humanos y las muestras biológicas asociados con una persona identificable no deberían ser dados a conocer ni puestos a disposición de terceros, en particular de empleadores, compañías de seguros, establecimientos de enseñanza y familiares de la persona en cuestión, salvo por una razón importante de interés público en los restringidos casos previstos en el derecho interno compatible con el derecho internacional relativo a los derechos humanos o cuando se haya obtenido el consentimiento previo, libre, informado y expreso de esa persona, siempre que éste sea conforme al derecho interno y al derecho internacional relativo a los derechos humanos. Debería protegerse la privacidad de toda persona que participe en un estudio en que se utilicen datos genéticos humanos, datos proteómicos humanos o muestras biológicas, y esos datos deberían revestir carácter confidencial.

c) Por regla general, los datos genéticos humanos, datos proteómicos humanos y muestras

biológicas obtenidos con fines de investigación científica no deberían estar asociados con una persona identificable. Aun cuando estén disociados de la identidad de una persona, deberían adoptarse las precauciones necesarias para garantizar la seguridad de esos datos o esas muestras biológicas.

d) Los datos genéticos humanos, datos proteómicos humanos y muestras biológicas obtenidos con fines de investigación médica y científica sólo podrán seguir estando asociados con una persona identificable cuando ello sea necesario para llevar a cabo la investigación, y a condición de que la privacidad de la persona y la confidencialidad de los datos o las muestras biológicas en cuestión queden protegidas con arreglo al derecho interno.

e) Los datos genéticos humanos y los datos proteómicos humanos no deberían conservarse de manera tal que sea posible identificar a la persona a quien correspondan por más tiempo del necesario para cumplir los fines con los que fueron recolectados o ulteriormente tratados.

Como es evidente, cualquier excepción permitida por ley al ejercicio de un derecho humano debe darse solamente con un objetivo legítimo y solamente para cumplir dicho objetivo. No debe existir otra alternativa menos intrusiva para alcanzarlo y, por supuesto, debe haber garantía judicial ante cualquier interferencia estatal sobre la vida de los ciudadanos. Con respecto a las interferencias originadas en empresas privadas, el Estado debería ejercer su rol de garante de los derechos humanos y establecer políticas para impedirles hacer lo que quieran con los datos personales.

¿Qué ocurre si la vulneración de la privacidad no se orienta hacia un individuo en particular, por ejemplo alguien imputado de un delito, sino que es masiva e indiscriminada? Claramente, eso constituye una violación masiva de los derechos humanos. Así lo expresó el relator especial sobre contra terrorismo y derechos humanos de Naciones Unidas, Ben Emmerson, en un informe formal ante la Asamblea General de la ONU:

"La dura verdad es que el uso de la tecnología de vigilancia masiva suprime efectivamente el derecho a la privacidad de las comunicaciones en Internet por completo [Con la vigilancia masiva] *"las comunicaciones de literalmente cada usuario de Internet están potencialmente abiertas para la inspección de agencias legales y de inteligencia de los Estados concernidos"* […] *"los individuos tienen derecho a compartir información e ideas con otros sin la interferencia del Estado, con la certeza de que sus comunicaciones serán leídas sólo por sus destinatarios".*

Luego de que Edward Snowden revelara los programas de vigilancia global masiva llevados a cabo por los servicios secretos de Estados Unidos, Reino Unido, Australia, Nueva Zelanda y Canadá, la Asamblea General de las Naciones Unidas aprobó el 18 de diciembre de 2013 una resolución donde se reconocía el respeto a la privacidad como parte de los derechos humanos, sin la cual tampoco es posible ejercer otros derechos, como la libertad de expresión. El carácter extraterritorial de este tipo de vigilancia fue señalado como un aspecto particularmente preocupante de la cuestión porque, normalmente, los estados se consideran garantes de hacer cumplir los derechos humanos hacia adentro de sus jurisdicciones, y se habla poco de que puedan tener la misma obligación frente a los ciudadanos de otros estados. Así que la resolución los instaba a respetar la privacidad y revisar sus procedimientos, prácticas y legislaciones, de un modo que permita establecer mecanismos

independientes y efectivos para asegurar la transparencia y la responsabilidad de cada estado.

El Consejo de Derechos Humanos de las Naciones Unidas, compuesto por 47 estados elegidos por la Asamblea General, también se ocupó del tema. En particular, en la agenda de la vigésimo cuarta sesión, llevada a cabo en septiembre de 2013. Allí, el Alto Comisionado hizo notar que la amenaza de la vigilancia masiva para los derechos humanos se encuentra entre las más acuciantes situaciones de la actualidad. Muchos representantes presentes en dicha sesión se refirieron a un informe del 16 de mayo de 2011 del Relator Especial de las Naciones Unidas para la promoción del derecho a la libertad de opinión y expresión, por entonces Frank La Rue, donde ya se habían delineado los peligros de la vigilancia indiscriminada.

El 24 de marzo de 2015 se publicó la resolución de Naciones Unidas titulada "El derecho a la privacidad en la era digital", que establece que el marco legal para la vigilancia debe estar claro y ser públicamente accesible y considera la intercepción de los metadatos de las comunicaciones un acto intrusivo. También solicita al Consejo de Derechos Humanos de las Naciones Unidas la creación de un Relator Especial para el Derecho a la Privacidad.

1.6. Los límites prácticos de las acciones individuales para la defensa de la privacidad

Hay analistas que son pesimistas ante la posibilidad de una solución puramente legal al problema de los archivos informáticos y la intimidad. David Lyon, por ejemplo, escribió en su libro "El Ojo Electrónico", de 1995:

"No sería sincero si ocultara mi opinión de que lo que puede lograrse por medio de medidas legales tiene limitaciones crónicas, no sólo en el sentido de que tales medidas pueden ser «demasiado escasas, demasiado tardías», sino también en el sentido de que el propio derecho es inadecuado para la tarea de regular la vigilancia electrónica. Los enfoques sociales, culturales y políticos, aunque menos tangibles, pueden ser más apropiados".

Algo similar podría decirse de los esfuerzos en el marco de las Naciones Unidas. Es excelente que existan, es mucho mejor que existan que lo contrario, es muy bueno que estas cosas se empiecen a discutir en ámbitos internacionales, pero igual con solo invocar derechos, tratados y leyes, no es de esperar que uno pueda confiar en que estados y empresas los cumplan solo porque existan. Pensar lo contrario implica desconocer las raíces profundas de las crecientes tendencias mundiales a invadir la privacidad y avanzar hacia la vigilancia masiva. Para comenzar a pensar en dichas razones, te recomiendo este artículo de Evgeny Morozov que, entre otras cosas, dice que:

Tanto el capitalismo como la administración burocrática se acomodaron fácilmente al nuevo régimen digital; ambos prosperan muy bien con los flujos de información, cuanto más automatizados, mejor. Ni las leyes, ni los mercados ni las tecnologías obstaculizarán o reconducirán la demanda de datos, puesto que, de entrada, los tres tienen un papel en el

mantenimiento del capitalismo y la administración burocrática. Hace falta otra cosa: política.

Esa es la clave: política. Lo cual excluye especialmente las soluciones individualistas. No es cuestión de que yo diga “no uso Facebook para que no me vigile”. Es cuestión de que ese tipo de empresas privadas se vean presionadas por la acción pública para no incurrir en prácticas cuestionables. También uno puede utilizar distintos sistemas de encriptación y mejorar su prácticas de seguridad informática. Pero, del mismo modo, aunque recomendamos hacerlo, quien crea que es la panacea puede encontrarse con desagradables sorpresas.

Además, aunque un individuo pueda elegir no usar Facebook, Whatsapp o el servicio que más le preocupe desde el punto de vista de la privacidad, ¿qué puede hacer con respecto a la vigilancia estatal? No es tan fácil elegir no relacionarse con las agencias impositivas, por ejemplo, que crecientemente recolectan datos muy personales sobre consumos, sin que se sepa mucho qué hacen con ellos y por cuánto tiempo los conservan. Sería mejor, entonces, un activismo participativo que exigiera transparencia y respeto por los derechos humanos a tanto a empresas como a dependencias estatales, en lugar de tratar de escapar cada cual como pueda de la situación o, peor, abandonarse a un fatalismo paralizante.

Puede decirse que las revelaciones de Snowden no solo mostraron un declive de la soberanía democrática popular, sino de la política misma. Porque, como dijo el filósofo Giorgio Agamben en 2013, con la excusa de la seguridad hoy los estados han virado de la política a la policía, y de gobernar a administrar por medio de sistemas de vigilancia electrónicos. Lo cual mina la posibilidad misma del ejercicio de la política. La política, pensada en este sentido, quizá podría regresar, con la condición de que la cultura de la vigilancia deje de parecernos inocua.