Contribución al proceso de consulta pública respecto de la "Segunda Estrategia Nacional de Ciberseguridad"

15 de Febrero de 2023.-

1. Introducción

De acuerdo con el procedimiento de consulta pública establecido en la Resolución 1/2023[1] de la Secretaría de Gabinete de la Jefatura de Gabinete de Ministros sobre la Segunda Estrategia Nacional de Ciberseguridad, la Asociación por los Derechos Civiles[2] (en adelante ADC) presenta a continuación una serie de consideraciones a tener en cuenta durante el mencionado proceso.

La ADC es una organización de la sociedad civil con sede en Argentina que desde 1995 trabaja en la defensa y promoción de los derechos civiles y humanos en Argentina y América Latina.

En primer lugar, se destaca la apertura del proceso de consulta pública del documento y se espera la continuidad de la transparencia en aspectos tales como la publicación de los textos posteriores, permitir comentarios de las partes interesadas con fechas límite razonables y la posibilidad de brindar una retroalimentación sobre los comentarios recibidos. Esta transparencia no sólo es importante en la etapa de consulta de la estrategia, sino también en su implementación y en la continuidad del plan de trabajo que la lleve adelante.

Es positivo, además, que se incorpore entre los principios rectores de la ciberseguridad el respeto por los derechos humanos y los derechos y libertades individuales, de acuerdo a la Constitución Nacional y los Tratados Internacionales.

Se reconoce la legitimidad del Gobierno Nacional para hacer frente a la seguridad digital, enfrentar la cibercriminalidad y proteger las infraestructuras críticas nacionales, pero las acciones a implementar pueden significar la expansión de la vigilancia estatal sin un examen adecuado de su necesidad y proporcionalidad. Esto afectaría los derechos de las personas y en particular los derechos a la libertad de expresión y a la privacidad.

Las políticas de seguridad digital deben estar centradas en el ser humano. Cualquier política de seguridad digital debe tener en su núcleo al individuo y desarrollarse de conformidad con las normas de derechos humanos reconocidas en convenios regionales y en el derecho internacional, e integrar y aplicar una política pública de protección de datos personales[3].

Teniendo en cuenta esto es que realizamos las siguientes observaciones y contribuciones con el fin de otorgar mayor profundidad a ese énfasis, y que no sea una mera declaración de intenciones.

2. Comentarios a la Segunda Estrategia

I. Sobre el término “Ciberseguridad”

En el Anexo de definiciones se define a la ciberseguridad como un “conjunto de políticas, estrategias y acciones orientadas a elevar los niveles de seguridad de las personas físicas y jurídicas frente a incidentes y delitos que utilicen como medio y/o fin un dispositivo informático”. Esta definición vincula de manera inseparable a la ciberseguridad con el cibercrimen y, como resultado, deja de lado cuestiones como el acceso a las herramientas digitales por parte de la ciudadanía.

Una valoración más cercana al enfoque integrador, que relaciona la seguridad digital con el respeto a los derechos humanos, es la desarrollada en 2014 por el grupo de trabajo 1 de la Freedom Online Coalition: “La ciberseguridad es la preservación –a través de políticas, tecnología y educación– de la disponibilidad, confidencialidad e integridad de la información y su infraestructura subyacente, a fin de mejorar la seguridad de las personas tanto online como offline”[4].

Esta definición responde a la importancia de respetar los derechos humanos y considerar el papel de la innovación tecnológica como motor para promover la libre circulación de información en medios digitales. Así, se refuerza la relación entre seguridad digital y derechos humanos como forma de fomentar la libertad y la seguridad[5].

La ciberseguridad no puede ser concebida desde un enfoque exclusivamente punitivista. Las políticas de seguridad en internet no se limitan a desempeñar un papel de “prevención del daño” sino que deben buscar que las personas puedan gozar de manera autónoma de la tecnología. Por lo tanto, la Estrategia debe

servir también como instrumento para reparar desigualdades sociales en materia de conectividad a internet o alfabetización digital, entre otras.

Desde 2016[6] la ADC recomienda que en lugar de ciberseguridad —que responde a una raigambre fuertemente militar y lleva muchas veces a la confusión señalada— se considere la utilización del término "seguridad digital". Dicho concepto tiene un enfoque más integral, que pone en el centro a las personas y a las comunidades, a la vez que busca promover el desarrollo económico y social, respetando las instituciones democráticas, el Estado de derecho y los derechos fundamentales de los individuos.

Sustituir el concepto de ciberseguridad por seguridad digital sería una primera gran oportunidad para situar el discurso en aspectos relevantes del tema. En un sentido sustantivo, la seguridad es un concepto positivo, pues se refiere a la capacidad de una persona a acceder a un recurso fundamental y utilizarlo de acuerdo a sus necesidades y preferencias. Desde la óptica de los derechos humanos, la seguridad se centra en la capacidad de las personas de actuar libre y responsablemente. Las políticas de seguridad en internet no deberían limitarse a desempeñar un papel defensivo sino facilitador.

Así, se potenciaría el bienestar de las personas como eje central. De esta forma, se aseguran soluciones con menos amenazas a los derechos humanos, garantías fundamentales de los sistemas democráticos[7].

II. Transparencia y rendición de cuentas sobre las estrategias que se adopten

Aunque en la introducción de la Segunda Estrategia se afirma que las acciones en el ciberespacio inciden en la actividad de las administraciones gubernamentales permitiéndoles transparentar y comunicar sus acciones de gobierno, es necesario destacar que no se mencionan prácticas de transparencia y rendición de cuentas.

Para comprobar el alcance de las metas asumidas en las políticas públicas sobre seguridad digital es necesario avanzar en la articulación de políticas de transparencia y monitoreo de la gestión sobre este tema. Ello implica verificar si se ha cumplido con lo programado y luego evaluar los resultados obtenidos. Esta mirada retrospectiva permite observar cuál ha sido el punto de partida –es decir, la línea de base– y cuáles han sido los avances logrados[8].

La rendición de cuentas es la herramienta más apropiada para visibilizar las acciones que se toman para articular políticas públicas ante problemas transectoriales en temas de seguridad digital, pues ayuda a prevenir y controlar cualquier abuso, además de que incrementa la seguridad digital de todas las personas[9].

Los indicadores propuestos en las políticas o estrategias de seguridad digital deberán ser medibles y verificables. El cumplimiento de las metas trazadas no debe terminar en una mera declaración de buenas intenciones, sino que sus resultados deben promover la confianza en el ciberespacio.

Como ejemplos concretos, es público conocimiento la cantidad de ataques a sistemas informáticos de reparticiones oficiales que están aconteciendo[10]. Desde el Registro Nacional de Personas[11] y la Dirección Nacional de Migraciones[12] hasta el Ministerio de Salud Nacional[13], entre otros[14], han visto vulnerados sus sistemas. Más allá de lo que surge al momento del hecho, en general brindado por medios de comunicación, no hay datos posteriores al ataque ni rendiciones de cuentas o información detallada para esclarecer las vulneraciones o incidentes.

Las estadísticas sobre vulnerabilidades informáticas deberían ser no sólo públicas, sino también presentadas en términos claros y accesibles para todas las personas. Como ya se mencionó, la rendición de cuentas ayuda a prevenir y controlar cualquier abuso e incrementa la seguridad digital de todas las personas.

III. Auditoría de los sistemas informáticos

La estrategia tiene en cuenta la necesidad de "fomentar y potenciar capacidades tecnológicas precisas para disponer de soluciones confiables que permitan proteger adecuadamente los sistemas frente a diferentes amenazas, promoviendo actividades de investigación, desarrollo e innovación, tanto en el sector académico, organizaciones de la sociedad civil, como en entidades del sector público y privado" (Objetivo 5). A pesar de ello, es fundamental resaltar que también es necesario promover e impulsar mejores sistemas informáticos, resilientes y actualizados que permitan potenciar la seguridad digital en los tres poderes del Estado.

Para ello los sistemas deben ser auditados de forma pública y constante, permitiendo no solo que su código fuente esté disponible a toda la ciudadanía sin trabas legales, sino también el acceso a información acerca de la forma en que se implementa el sistema en cuestión. Esto es beneficioso en tanto alienta a la revelación de vulnerabilidades por parte de aquellas partes interesadas y además beneficia el potencial de aprendizaje sobre seguridad informática.

En el ámbito empresarial es usual que se implementen programas de recompensa por errores para quienes reporten vulnerabilidades de los sistemas informáticos, permitiendo a las empresas reducir la probabilidad de incidentes por debilidades desconocidas[15]. La adopción de prácticas similares por parte de los Estados alentaría y apoyaría el trabajo de investigación sobre seguridad digital.

Las auditorías periódicas evitan pérdidas económicas y de datos, generan confiabilidad, permiten encontrar fallas y reflejan transparencia, aspectos que resultan fundamentales en el ejercicio de la actividad pública.

IV. Seguridad Digital y Datos Personales

Tal como se menciona en la exposición del proyecto de la Segunda Estrategia Nacional de Ciberseguridad, la Resolución N°A/RES/66/290 aprobada por la Asamblea General de las Naciones Unidas (ONU)[16] establece que la seguridad humana “exige respuestas centradas en las personas, exhaustivas, adaptadas a cada contexto y orientadas a la prevención que refuercen la protección y el

empoderamiento de todas las personas y todas las comunidades". Teniendo en cuenta esto, la ADC considera que la protección de los datos personales es un aspecto fundamental bajo el cual considerar la seguridad digital.

En los últimos años ha venido creciendo la cantidad de ataques a los sistemas informáticos de diferentes reparticiones oficiales en las que se comprometen datos personales de la población[17].

Ante esta situación la ADC se manifestó en varias oportunidades solicitando información al respecto a través de pedidos de acceso a la información pública[18]. En dichos pedidos uno de los puntos que se consulta se refiere a las medidas de seguridad digital sobre los datos personales de las y los afectados al momento del incidentes y las adoptadas luego de que ocurrieran. En ninguna de las oportunidades citadas se obtuvo respuesta concreta sobre este aspecto.

Es por eso que es fundamental resaltar la extensión de la protección de los datos personales a la seguridad digital que los resguarda y, por lo tanto, considerar que el acceso a la información concreta sobre dichas medidas de seguridad también se encuentra alcanzada por los derechos consagrados en la Ley N° 25.326[19], específicamente el derecho de acceso a la información.

Estas consideraciones van de la mano con el proceso de reforma de la Ley de Protección de Datos Personales que inició la Agencia de Acceso a la Información Pública, a la que la ADC también realizó contribuciones[20], y la reciente incorporación del Convenio 108+ a nuestro sistema normativo[21].

V. Cifrado

La seguridad y privacidad se refuerzan mutuamente y generan entornos saludables para la confianza de las personas en la red, contribuyendo al florecimiento de una variedad de servicios en internet. La adopción de buenas prácticas en seguridad y privacidad deben incluirse en las políticas o estrategias nacionales de seguridad digital, así como establecer salvaguardas nacionales para la promoción de herramientas de cifrado y otros sistemas de protección para las personas.

El cifrado es el proceso por el que se codifican los datos utilizando algoritmos matemáticos. Esto ayuda a proteger la información de una comunicación o resguardar datos en cualquier dispositivo en que se encuentren[22].

El uso de técnicas de cifrado, tanto en el resguardo de información como en las comunicaciones privadas, tiene como propósito disminuir los riesgos de que los contenidos puedan ser interceptados. Estos riesgos incluyen el acceso a datos sensibles asociados a la ejecución de acciones. Esto puede ser compras por internet, datos médicos, acceso a redes sociales, cuentas bancarias y todo tipo de actividad en línea que suponga el acceso a información y cuya extracción ilegítima pueda revelar detalles sumamente precisos de la vida privada y generar perjuicios[23].

La Asamblea General de las Naciones Unidas ha reafirmado que la privacidad es un derecho que habilita el goce de otros derechos, particularmente la libertad de expresión y la libertad de opinión, además de ser la base de una sociedad

democrática. Proteger el derecho a la privacidad implica a su vez salvaguardar un gran abanico de derechos que éste habilita[24].

La seguridad que brinda el cifrado juega un rol fundamental en el desarrollo de nuestra personalidad como individuos. Como bien lo menciona el Relator Especial para la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión de las Naciones Unidas, David Kaye: "La posibilidad de navegar la web, desarrollar ideas y comunicarse en forma segura es tal vez la única manera en que muchas personas pueden explorar aspectos básicos de identidad, como su género, religión, etnia, nacionalidad y sexualidad"[25].

Teniendo en cuenta lo anterior, la promoción del cifrado resulta un principio fundamental a incluir en la Segunda Estrategia Nacional de Ciberseguridad. Este aspecto tampoco fue incluido en la primera estrategia[26] y resulta necesario para el cumplimiento del pleno respeto de los derechos humanos.

VI. Evaluaciones de impacto

Ya se ha rescatado en esta contribución la incorporación como uno de los principios rectores de la seguridad digital del respeto por los derechos humanos y los derechos y libertades individuales.

Para que este principio sea transversal a toda la estrategia es fundamental la incorporación de evaluaciones de impacto anteriores a la implementación de medidas concretas de seguridad digital. Como se mencionó en la introducción, es clara la legitimidad del Gobierno Nacional para hacer frente a la seguridad

digital, enfrentar la cibercriminalidad y proteger las infraestructuras nacionales, pero las estrategias adoptadas no pueden habilitar la expansión de la vigilancia estatal sin un examen adecuado de su necesidad y proporcionalidad.

En aras a la búsqueda de la seguridad de la población, los Estados han adoptado medidas desproporcionadas que pueden afectar los derechos a la privacidad y la protección de datos personales, y garantías constitucionales como la presunción de inocencia y el debido proceso, los derechos a la no discriminación, a la libertad de expresión, de reunión y de asociación.

La utilización de datos biométricos como mecanismo de identificación -que comenzó a ser aplicada con fines de seguridad pública- ya se está efectuando para verificar identidades en programas de seguridad social, responsabilidades impositivas o fiscales, educación, elecciones y deportes. Además, cada vez son más las autoridades gubernamentales que despliegan cámaras de vigilancia en espacios públicos que permiten identificar a las personas por los rasgos de su rostro, generando así importantes riesgos para los derechos de las personas[27].

Un ejemplo de la implementación de estas medidas en los últimos años son los sistemas de reconocimiento facial. Tanto por cuestiones de vigilancia[28], como para habilitar las tarjetas SIM en teléfonos móviles[29], esta tecnología es cada vez más utilizada. En ambas oportunidades la ADC manifestó su preocupación ante la proporcionalidad de los medios utilizados para determinados fines[30]. Esto tiene más peso cuando además se puede afectar a sectores de la población que, por razones inherentes a su identidad o condición, se ven más expuestos a la privación en el ejercicio de sus derechos humanos.

Una evaluación de impacto en derechos humanos debe realizarse en todos los procesos de implementación y ejecución de la estrategia de seguridad digital, tanto a nivel producto como servicio.

En este sentido, es fundamental preguntarse:

- ¿En qué medida podrían contribuir las medidas de seguridad adoptadas a reducir las desigualdades? O por el contrario, ¿en qué medida podría exacerbar estas desigualdades?
- ¿Se han tomado en consideración los derechos humanos en el planeamiento de las medidas de seguridad? ¿En qué grado se verán afectados?
- ¿Qué mediciones pueden verificar si las medidas de seguridad alcanzan por igual a las personas?[31]

Es por ello que previo a la adopción y durante la ejecución de cualquier medida de seguridad digital se debe realizar una evaluación de impacto para determinar las bases y justificación de la necesidad y proporcionalidad de la misma. Y su análisis debe ser realizado bajo una óptica de respeto de los derechos humanos. Es fundamental que está cuestión sea incorporada a la estrategia en análisis.

VII. Perspectiva de género

Resulta alentadora la inclusión como parte del objetivo 1 (Concientización, Capacitación y Educación en el uso responsable del ciberespacio y promoción

para la formación de especialistas en Ciberseguridad) de desarrollar iniciativas con perspectiva de género que fomenten la capacitación en la materia. La ADC viene señalando desde 2019[32] que existe una cultura laboral extendida en el tiempo que expulsa a las mujeres del rubro tecnológico.

La baja proporción de mujeres en carreras de grado en informática repercute en el posterior acceso al mercado laboral y en la ocupación de áreas jerárquicas del sector. Entre las razones que se citan para explicar la pérdida progresiva de las estudiantes en el sector podemos encontrar, en particular, los estereotipos culturales en relación con las capacidades de las niñas y mujeres para desenvolverse en áreas como tecnología, informática, ciencia y matemática.

El problema de una industria tecnológica donde la mayoría son hombres es que la misma genera productos que, concebidos desde una perspectiva masculina hegemónica, son ofrecidos a un mundo en el cual al menos no se ajusta.

En el caso de la creación de soluciones en seguridad digital que no consideren diferencias fundamentales entre modelos de riesgo resulta peligrosa para las más desprotegidas y vulnerables. Los modelos de riesgo son diversos y responden a las necesidades particulares y actividades de cada persona, y difieren de manera fundamental entre mujeres y varones.

Como consecuencia de lo anterior, es necesario que el fomento de la capacitación en materia de ciberseguridad con perspectiva de género dentro de la estrategia se materialice posteriormente en iniciativas concretas, tales como:

- la elaboración de programas dirigidos a niñas y adolescentes en las escuelas que apunten a romper con los mitos de las carreras en ciencia y matemática;
- la promoción de becas para estudiantes universitarias mujeres;
- incentivos a empresas de tecnología, para la elaboración de protocolos de género y guías de buenas prácticas con el fin de erradicar la expulsión de mujeres en esos rubros;
- ampliación de licencias por paternidad, por maternidad y por enfermedad de hijas e hijos, que favorezcan la corresponsabilidad para incentivar una distribución más justa de las tareas de cuidado familiar.

Con mucho agrado el equipo de la ADC queda a disposición de la Secretaría de Innovación Pública, de la Jefatura de Gabinete de Ministros, así como de las múltiples partes interesadas, para contribuir en futuros aportes y, en caso de ser necesario, profundizar las contribuciones del presente documento en la elaboración de la Segunda Estrategia Nacional de Ciberseguridad.

Notas

1. Resolución 1/2023 del 2 de enero de 2023, Boletín Oficial de la República Argentina. Disponible en: https://www.boletinoficial.gob.ar/detalleAviso/primera/279103/20230105
2. Asociación por los Derechos Civiles. (2023, 11 enero). https://adc.org.ar/
3. OEA: Declaración de sociedad civil latinoamericana sobre seguridad digital. (2022, 7 noviembre). *Asociación por los Derechos Civiles.* https://adc.org.ar/2016/04/06/oea-declaracion-sociedad-civil-latinoamericana-seguridad-digital
4. Freedom Online Coalition. (s.f.). WG 1 – An Internet Free and Secure. Disponible en https://freedomonlinecoalition.com/working-groups/working-group-1/
5. Asociación por los Derechos Civiles (ADC). (2018). Derechos Humanos y Seguridad Digital: Una pareja perfecta. https://adc.org.ar/wp-content/uploads/2019/06/034-derechos-humanos-y-seguridad-digital-una-pareja-perfecta-1-01-2018.pdf
6. OEA: Declaración de sociedad civil latinoamericana sobre seguridad digital. (2022, 7 noviembre). *Asociación por los Derechos Civiles.* https://adc.org.ar/2016/04/06/oea-declaracion-sociedad-civil-latinoamericana-seguridad-digital/; Asociación por los Derechos Civiles (ADC). (2016). Ciberseguridad en la era de la vigilancia masiva. Descubriendo la agenda de ciberseguridad de América Latina: el caso de Argentina. https://adc.org.ar/wp-content/uploads/2019/06/013-A-ciberseguridad-en-la-era-de-la-vigilancia-masiva-05-2016.pdf
7. Asociación por los Derechos Civiles (ADC). (2018). Derechos Humanos y Seguridad Digital: Una pareja perfecta. https://adc.org.ar/wp-content/uploads/2019/06/034-derechos-humanos-y-seguridad-digital-una-pareja-perfecta-1-01-2018.pdf
8. Asociación por los Derechos Civiles (ADC). (2018). *Derechos Humanos y Seguridad Digital: Una pareja perfecta.* https://adc.org.ar/wp-content/uploads/2019/06/034-derechos-humanos-y-seguridad-digital-una-pareja-perfecta-1-01-2018.pdf
9. Asociación por los Derechos Civiles (ADC). (2018). *Derechos Humanos y Seguridad Digital: Una pareja perfecta.* https://adc.org.ar/wp-content/uploads/2019/06/034-derechos-humanos-y-seguridad-digital-una-pareja-perfecta-1-01-2018.pdf
10. Cronista (2022). El gobierno reconoce que se duplicaron los intentos de hackeos y robo de datos: quiénes están en peligro. https://www.cronista.com/infotechnology/mundo-cio/el-gobierno-reconoce-que-se-duplicaron-los-intentos-de-hackeos-y-robo-de-datos-quienes-estan-en-peligro/
11. El Cronista (2021). Hackean RENAPER: habló el hacker y asegura tener copia de los datos, planea venderlos y filtrarlos. https://eleconomista.com.ar/tech/hackean-renaper-hablo-hacker-asegura-tener-copia-datos-planea-venderlos-filtrarlos-n47003
12. Clarín (2020) . Ciberataque a Migraciones: qué información robaron y publicaron los ciberdelincuentes. https://www.clarin.com/tecnologia/ciberataque-migraciones-informacion-robaron-publicaron-ciberdelincuentes_0_Pfe1OVNlI.html

13. Infobae (2022). Hackearon el sistema informático del Ministerio de Salud de la Nación. https://www.infobae.com/salud/ciencia/2022/10/23/hackearon-el-sistema-informatico-del-ministerio-de-salud-de-la-nacion/
14. TN (2022). Ahora el CONICET sufrió un ciberataque: secuestraron datos de la sede central del organismo. https://tn.com.ar/sociedad/2022/04/22/ahora-el-conicet-sufrio-un-ciberataque-secuestraron-datos-de-la-sede-central-del-organismo/
15. Asociación por los Derechos Civiles (ADC). (2018). Derechos Humanos y Seguridad Digital: Una pareja perfecta. https://adc.org.ar/wp-content/uploads/2019/06/034-derechos-humanos-y-seguridad-digital-una-pareja-perfecta-1-01-2018.pdf
16. Organización de las Naciones Unidas (ONU). Resolución N° A/RES/66/290. 2012. Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/476/25/PDF/N1147625.pdf?OpenElement
17. TELAM (2022). Hubo un fuerte incremento en la fuga de datos personales a través de sistemas digitales. https://www.telam.com.ar/notas/202209/605547-fuerte-incremento-fuga-datos-personales-sistemas-digitales.html
18. Asociación por los Derechos Civiles (ADC). (2022). Nuevo pedido de acceso a la información ante el hackeo al Ministerio de Salud de la Nación. https://adc.org.ar/2022/10/26/nuevo-pedido-de-acceso-a-la-informacion-ante-el-hackeo-al-ministerio-de-salud-de-la-nacion/
19. Ley N. 25.326 del 2000. Ley de Protección de los Datos Personales. 30 de octubre del 2000. Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm
20. Asociación por los Derechos Civiles (ADC). (2022). El proyecto de Ley de Protección de Datos Personales presentado por la AAIP incorpora aportes de la ADC. https://adc.org.ar/2022/11/28/el-proyecto-de-ley-de-proteccion-de-datos-personales-presentado-por-la-aaip-incorpora-aportes-de-la-adc/
21. Se convirtió en Ley la adhesión de Argentina al Convenio 108+. (2022, 12 diciembre). *Argentina.gob.ar.* https://www.argentina.gob.ar/noticias/se-convirtio-en-ley-la-adhesion-de-argentina-al-convenio-108
22. Asociación por los Derechos Civiles (ADC). (2018). Derechos Humanos y Seguridad Digital: Una pareja perfecta. https://adc.org.ar/wp-content/uploads/2019/06/034-derechos-humanos-y-seguridad-digital-una-pareja-perfecta-1-01-2018.pdf
23. Derechos Digitales. Tecnologías para la privacidad y la libertad de expresión: Reglas sobre el anonimato y cifrado, (2017). https://www.derechosdigitales.org/wp-content/uploads/anonimato-y-cifrado.pdf
24. Asociación por los Derechos Civiles (ADC). (2016). Defendiendo los Derechos Humanos en la era digital. El rol del cifrado. https://adc.org.ar/wp-content/uploads/2019/06/022-Defendiendo-los-derechos-humanos-en-la-era-digital-El-rol-del-cifrado-12-2016.pdf
25. Reporte del Relator Especial para la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión, ONU, A/HRC/29/32, 2015,

http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A_HRC_29_32_en.doc
26. Primera Estrategia Nacional de Ciberseguridad. 2019. Disponible en: https://www.argentina.gob.ar/sites/default/files/infoleg/res829-01.pdf
27. Asociación por los Derechos Civiles (ADC), (2021). Tecnologías de vigilancia en Argentina. https://adc.org.ar/wp-content/uploads/2021/12/ADC-Tecnologias-de-Vigilancia-en-Argentina.pdf
28. Reconocimiento facial: el gobierno de la Ciudad recusó al juez Roberto Gallardo | Buenos Aires Ciudad - Gobierno de la Ciudad Autónoma de Buenos Aires. (s. f.). Gobierno de la Ciudad de Buenos Aires. https://buenosaires.gob.ar/jefaturadegabinete/noticias/reconocimiento-facial-el-gobierno-de-la-ciudad-recuso-al-juez-roberto
29. Página 12. (2023, 12 enero). Las telefónicas tendrán que requerir reconocimiento facial para cambiar tarjetas SIM. PAGINA 12. https://www.pagina12.com.ar/515029-las-telefonicas-tendran-que-requerir-reconocimiento-facial-p
30. Avanza la regulación del reconocimiento facial en la Legislatura porteña. (2020, 21 septiembre). Asociación por los Derechos Civiles. https://adc.org.ar/2020/09/18/avanza-la-regulacion-del-reconocimiento-facial-en-la-legislatura-portena/
31. Asociación por los Derechos Civiles (ADC), (2020), ¿Cómo implementar la debida diligencia en derechos humanos en el desarrollo de tecnología? https://adc.org.ar/wp-content/uploads/2020/10/Guia-Debida-Diligencia-DDHH-Analisis-de-Impacto-en-Privacidad.pdf
32. Asociación por los Derechos Civiles (ADC). (2019). *La deserción de las mujeres en la industria informática: el caso de la ciberseguridad. Otra dimensión del acceso a las TIC.* https://adc.org.ar/informes/la-desercion-de-las-mujeres-en-la-industria-informatica-el-caso-de-la-ciberseguridad/