Naciones Unidas A/HRC/46/37

Asamblea General

Distr. general
25 de enero de 2021
Español
Original: inglés

Consejo de Derechos Humanos
46º período de sesiones
22 de febrero a 19 de marzo de 2021
Tema 3 de la agenda
Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo

La inteligencia artificial y la privacidad, así como la privacidad de los niños

Informe del Relator Especial sobre el derecho a la privacidad, Joseph A. Cannataci* **

Resumen

El presente informe se ha preparado de conformidad con las resoluciones 28/16 y 37/2 del Consejo de Derechos Humanos. El derecho humano a la privacidad no ha sido nunca más importante ni se ha visto más hostigado. Como se presagiaba en 2015, los avances tecnológicos han planteado cada vez más problemas para el goce del derecho a la privacidad. En el presente informe, el informe final del primer mandato del Relator Especial sobre el derecho a la privacidad, se abordan dos problemas distintos: en primer lugar, la inteligencia artificial y la privacidad y, a continuación, la privacidad de los niños, en particular la función de la privacidad en la reafirmación de la autonomía y la participación positiva en la sociedad. Se esbozan orientaciones y recomendaciones, elaboradas mediante consultas e investigaciones, para afrontar esos desafíos. Junto a otras recomendaciones formuladas por el Relator Especial en sus informes anteriores, el presente informe completa el plan de trabajo presentado al Consejo de Derechos Humanos en 2016 (A/HRC/31/64). En los anexos figura una reseña general de las actividades realizadas desde 2015 por el Relator Especial en el marco del mandato.

* Se acordó publicar este informe después de la fecha de publicación prevista debido a circunstancias ajenas a la voluntad de quien lo presenta.

** Los anexos del presente informe se distribuyen tal como se recibieron, únicamente en el idioma en que se presentaron.

I. Recomendaciones sobre la protección de la privacidad en el desarrollo y la aplicación de soluciones de inteligencia artificial

Antecedentes y propósito

1. La finalidad de las presentes recomendaciones es proporcionar directrices sobre el uso de la información personal y no personal en el contexto de las soluciones de inteligencia artificial (IA)[1] desarrolladas como parte de las tecnologías de la información y las comunicaciones (TIC) aplicadas, así como hacer hincapié en la importancia de una base legítima para el tratamiento de datos de IA por parte de los Gobiernos y las empresas en el marco general del derecho humano a la privacidad.

2. Las recomendaciones toman como base la Declaración Universal de Derechos Humanos y reflejan el espíritu y el entendimiento de esa Declaración. Sobre todo, los artículos 7 (no discriminación) y 12 (derecho a la privacidad) son fundamentales para el desarrollo o la aplicación de soluciones de IA. El contenido y los valores de esos artículos se recogen en los artículos 2 y 3 (no discriminación) y 17 (privacidad) del Pacto Internacional de Derechos Civiles y Políticos y constituyen obligaciones contraídas por los Estados que han ratificado este instrumento.

3. Los derechos tienen una importancia crucial en la sociedad de la información. La Asamblea General y el Consejo de Derechos Humanos han confirmado que los derechos de que gozan las personas cuando no están conectadas a Internet también deben protegerse cuando lo están (A/75/62-E/2020/11, párr. 9), como condición para que Internet siga siendo global, abierta e interoperable (resolución 26/13 del Consejo de Derechos Humanos), y en tanto que fuerza motriz para avanzar en el desarrollo en sus diversas formas, incluido el logro de los Objetivos de Desarrollo Sostenible (resolución 73/179 de la Asamblea General).

4. Las recomendaciones se centran en la privacidad de todos los datos[2] que sirven de base para las soluciones de IA. Su objeto es servir de base internacional común para las normas en materia de protección de datos relativas a las soluciones de IA, en especial las que vayan a ser de aplicación nacional. Si bien se reconocen los numerosos beneficios económicos y sociales de las soluciones de IA, las recomendaciones tienen por objeto servir de punto de referencia sobre la manera de proteger el derecho a la privacidad en el contexto de dichas soluciones.

5. La aplicación de las recomendaciones requiere la plena colaboración entre los Gobiernos, la sociedad civil, el sector privado, la comunidad técnica y los círculos académicos, y debe sustentarse en valores humanos comunes, como la inclusividad, el respeto, la consideración central del ser humano, los derechos humanos, el derecho internacional, la transparencia y la sostenibilidad.

6. Las soluciones de IA implican la aplicación de sistemas de IA destinados a guiar, predecir o tomar decisiones que afectan a la vida de todos. Estas soluciones tienen beneficios, así como otros efectos que se están debatiendo actualmente en la sociedad. Se trata de debates en curso sobre cuestiones morales, éticas y sociales relacionadas con derechos humanos como la privacidad, la no discriminación y la libre participación. Todas esas cuestiones están condicionadas por un tratamiento legal desde la perspectiva de la privacidad. Ello es

[1] Hay varias definiciones de inteligencia artificial. El sentido en el que se utiliza en el presente informe es el más común, con arreglo a la definición que figura en *Oxford Reference*: "La teoría y el desarrollo de sistemas informáticos capaces de realizar tareas que normalmente requieren la inteligencia humana, como la percepción visual, el reconocimiento de voz, la adopción de decisiones y la traducción entre idiomas". Esta no es, en absoluto, una lista exhaustiva de las aplicaciones de las tecnologías de la IA.

[2] El Relator Especial establece una vinculación entre la protección de datos y el derecho al respeto de la vida privada recogido en el artículo 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, y aborda la legislación sobre protección de datos como parte de la reglamentación en materia de privacidad. Si bien reconoce que la evolución histórica de Europa ha llevado a la inclusión explícita de la protección de datos en un artículo específico de la Carta de los Derechos Fundamentales de la Unión Europea, remite a los lectores a las referencias históricas.

especialmente necesario habida cuenta de que la mayoría de los datos están en manos de empresas privadas que sacan partido de su valor comercial y combinan diversos conjuntos de datos para aprovechar al máximo su capacidad analítica. Se requiere una respuesta a la creciente preocupación del público sobre la intrusión y el impacto potencial de la recopilación de datos, el riesgo de la vigilancia y el creciente uso de algoritmos que se basan en esos conjuntos de datos para automatizar decisiones que afectan a las vidas de las personas (A/75/62-E/2020/11, párr. 10).

7. El contexto para el despliegue de la IA requiere el funcionamiento efectivo e independiente de un organismo regulador de la privacidad y/o la protección de los datos que supervise la legislación en la materia.

Alcance

8. Las presentes recomendaciones son de aplicación al procesamiento de datos de soluciones de IA en todos los sectores de la sociedad, con inclusión de los sectores público y privado. El procesamiento de datos se refiere a cada etapa del ciclo de vida de una solución de IA en la que intervengan datos, incluidos el diseño, desarrollo, despliegue y desmantelamiento de una solución de IA, así como cualquier iteración o nuevo diseño basado en una solución de IA precedente.

9. Las recomendaciones son de aplicación a todos los gestores de soluciones de IA, ya sean diseñadores, desarrolladores u operadores (responsables autónomos o principales), con arreglo a la función específica que lleven a cabo cada uno de ellos. Se trata de que, en las organizaciones, haya una persona jurídica o física plenamente responsable de cada solución de IA.

10. Las recomendaciones no limitan ni afectan en manera alguna a cualquier legislación que conceda a los titulares de datos derechos, protección y/o recursos más amplios o, en algún otro modo, de mayor calado. No limitan ni afectan de ninguna otra manera a ley alguna que imponga obligaciones a quienes gestionan y procesan los datos, cuando dichas obligaciones sean mayores, más amplias o más estrictas en relación con aspectos de la privacidad de los datos.

11. Las recomendaciones no son de aplicación a las soluciones de IA que puedan aplicar las personas físicas en el contexto de actividades puramente privadas o domésticas.

Consideración de aspectos éticos y relacionados con los derechos humanos

12. La sociedad tiene la responsabilidad de desarrollar soluciones de IA dentro de un marco de derechos humanos, y de manera ética y responsable. Las soluciones de la IA afectan en la actualidad a muchas esferas de la vida diaria, y cada vez lo harán más, por lo que tienen una profunda influencia en la vida personal y las situaciones laborales de las personas. En el futuro es probable que las soluciones de IA afecten a una gama más amplia de principios fundamentales que reflejen normas de derechos humanos y cuestiones éticas. Es fundamental la forma en que se utilice esa tecnología.

13. La no discriminación es esencial para evitar la desigualdad, la injusticia y el sufrimiento, que pueden afectar al goce de los derechos humanos, incluidos los derechos económicos, sociales y culturales. Es necesario vigilar estrechamente el uso de soluciones de IA y corregir cualquier caso de discriminación u otros supuestos en que se vulneren los derechos humanos con objeto de evitar consecuencias adversas.

14. En ciertos ámbitos, como las decisiones judiciales o médicas, no debe permitirse el uso de soluciones de IA para la adopción de decisiones finales, sino únicamente como parte del proceso de apoyo a la adopción de estas. Siempre debe hacerse una evaluación desde el punto de vista de los derechos humanos, junto con la evaluación respecto de la protección de datos, a fin de contar con una visión general integral de las condiciones contextuales necesarias.

15. En todo el mundo hay comités que trabajan en la elaboración de marcos normativos y códigos de ética para las soluciones de IA, como es el caso del Comité Especial sobre Inteligencia Artificial del Consejo de Europa. Debe hacerse referencia a su labor, así como a

otras orientaciones pertinentes, como los Principios Rectores sobre las Empresas y los Derechos Humanos.

Inteligencia artificial y privacidad de los datos

16. Los sistemas actuales de inteligencia artificial incluyen o representan una combinación de sistemas de análisis basados en conocimientos especializados formalizados (almacenes de datos, inteligencia comercial) y aprendizaje automático, así como una aplicación selectiva de lo aprendido. Hay una diferencia entre los sistemas algorítmicos previamente programados para la solución de problemas específicos y los sistemas que pueden aprender. Estos últimos están equipados con algoritmos de aprendizaje y tienen que ser entrenados.

17. En el proceso algorítmico de toma de decisiones que se utiliza habitualmente como base para la IA, se hace una evaluación basada en la información, que da lugar a una decisión, un pronóstico o una recomendación respecto de una medida. En el caso del "aprendizaje supervisado", el sistema de IA tiene criterios de solución para resolver un problema específico, mientras que en el caso del "aprendizaje no supervisado", el propio sistema de IA elige o recomienda los criterios de solución pertinentes.

18. Por consiguiente, tanto el tratamiento de los datos como la decisión que se adopte como resultado de ese tratamiento entrañan riesgos potenciales para los titulares de datos.

19. La tecnología de la información clásica, con sus elementos de "introducción de datos" — "tratamiento" — "resultado", se amplía con las capacidades de percibir, comprender, actuar y aprender. Esas actividades, que antes sólo realizaban los seres humanos, las realizan cada vez más las máquinas. El término "comprensión" es un nuevo ámbito en relación con las computadoras y ha de ir acompañado de un examen crítico de la rastreabilidad y el respeto de los derechos humanos y los valores éticos.

20. El aprendizaje automático se refiere, entre otras cosas, a una serie de métodos de optimización de las redes neuronales artificiales. Los sistemas de IA pueden tener estructuras muy complejas entre las capas de entrada y salida. Mediante el mapeo de varias capas de procesamiento jerárquico, el aprendizaje automático puede ser considerablemente más eficiente (aprendizaje profundo). Ello resulta inevitablemente en una reducción de la rastreabilidad de las decisiones de la IA. Debido a la complejidad de los algoritmos y a la multitud de operaciones aritméticas realizadas por la máquina, las capas de procesamiento más profundas (capas ocultas) eluden la transparencia de los criterios de decisión y su ponderación.

21. La divulgación de los algoritmos en los que se basa la IA es una exigencia fundamental en el debate actual sobre la transparencia de esta. No obstante, es probable que, en la práctica, sea difícil la verificación concreta de la lógica de decisión de los sistemas de IA altamente complejos utilizando algoritmos revelados. Tanto si se trata de IA interpretable o explicable, como de otro tipo, cuando hay dudas o un fallo en lo que se refiere al proceso o a los resultados, es necesario obtener pruebas digitales para hacer una reconstrucción de lo que ocurrió y de las razones por las que se aconsejó o se produjo realmente un determinado resultado.

22. La vigilancia externa de los procesos de adopción de decisiones de los sistemas de IA, mediante el examen de las decisiones mismas en relación con un propósito predeterminado del sistema y de la gobernanza ética, tiene muchas ventajas, también desde un punto de vista práctico.

23. Han de identificarse las decisiones de la IA que estén fuera del rango previsto de resultados o decisiones e intervenir al respecto. Previamente, se requiere el desarrollo de herramientas específicas para la detección de resultados imprevistos y para el análisis de las decisiones de la IA. La vigilancia de las máquinas exclusivamente por máquinas aumenta la posibilidad de riesgos imprevistos o "incógnitas desconocidas". Es necesario, pues, partir del principio de que los juicios humanos deben dominar siempre los procesos de vigilancia de la IA.

24. Además de la eficiencia de los mecanismos de aprendizaje, el éxito del aprendizaje automático depende de la cantidad y la calidad de los datos disponibles. El desarrollo de los

macrodatos en la tecnología de la información y la creciente disponibilidad masiva de datos de alta calidad están acelerando de manera significativa el desarrollo de los sistemas de IA.

25. Es probable que los complejísimos procesos psicológicos y emocionales del conocimiento y la toma de decisiones de los seres humanos sigan siendo dominio de los humanos y no de las máquinas. Por consiguiente, al evaluar y sopesar el derecho aplicable en relación con los sistemas de IA y su toma de decisiones, ha de tenerse en cuenta que las decisiones de la máquina se basan en principios y mecanismos diferentes (aunque desarrollados en gran medida por los seres humanos) de los aplicados a las decisiones humanas.

26. Para lograr la seguridad necesaria de los sistemas de IA, ha de aplicarse de manera efectiva una gobernanza ética y jurídica integral de las decisiones de la IA en el entorno de control de una entidad que emplee soluciones de IA. Además, se necesita una mejor cooperación digital en la que múltiples interesados reflexionen sobre la elaboración y aplicación de normas y principios como la transparencia y la imparcialidad de las aplicaciones de IA en diferentes entornos sociales.

A. Principios relativos a la privacidad de los datos para el uso de soluciones de inteligencia artificial

27. Con independencia de la jurisdicción o del ordenamiento jurídico aplicables al gestor responsable, hay ocho principios fundamentales que son consideraciones obligatorias a la hora de planificar, desarrollar y aplicar soluciones de IA. Los principios y su especificación no sustituyen a ninguna otra normativa sobre protección de datos, o a una que sea más estricta, aplicable a quienes trabajan con soluciones de IA. Los principios son los siguientes:

a) Jurisdicción;

b) Base ética y legal;

c) Fundamentos de los datos;

d) Responsabilidad y supervisión;

e) Control;

f) Transparencia y “justificación”;

g) Derechos del titular de los datos;

h) Salvaguardias.

Jurisdicción

28. Para crear certidumbre jurídica y rastreabilidad, lo ideal sería que existiera un marco transnacional que reflejara el consenso internacional y contuviera mecanismos para identificar y regular la responsabilidad en las soluciones de IA y gestionar los riesgos conocidos.

29. En ausencia de ese marco transnacional, una opción es el establecimiento de soluciones y salvaguardias impuestas de manera local. En este supuesto, cuando una solución de IA utilice un mecanismo de toma de decisiones diversificado, ese mecanismo también debe estar en una única jurisdicción.

30. Otras opciones son los acuerdos bilaterales o multilaterales o la reglamentación local dentro de una jurisdicción facilitada por acuerdos transfronterizos; o bien, en los casos en que la IA se siga implementando y sean las fuerzas del mercado y los riesgos los que determinen la reglamentación, mediante el derecho de los consumidores u otras formas de reparación.

31. A menos que se desarrolle un mecanismo específico de derecho internacional *ad hoc* para resolver cuestiones jurisdiccionales en materia de tecnologías de la información y las comunicaciones, especialmente para las soluciones de IA desarrolladas en una jurisdicción pero utilizadas en otra, y hasta que dicho mecanismo se desarrolle, cuando se requiera que

una solución de IA funcione en múltiples jurisdicciones, deberá aplicarse y funcionar como una federación multinacional de soluciones individuales de IA de una jurisdicción.

Base ética y legal

32. Dado que el tratamiento de los datos personales de las personas físicas siempre afecta a los derechos del titular de los datos, el tratamiento de estos en que se base una solución de IA debe tener una sólida base ética y jurídica. Esto es aún más importante si el tratamiento en sí tiene por objeto dirigir la posición o los derechos de titular de los datos o tomar decisiones que los afecten. Independientemente de la jurisdicción o del entorno jurídico individual del gestor, una o más de las hipótesis que se mencionan a continuación pueden proporcionar una base jurídica suficiente para el tratamiento de los datos por un sistema de IA:

a) Cuando se haya elaborado una ley de conformidad con los principios democráticos y los derechos humanos, esta podría constituir una base jurídica específica si aborda el conflicto de intereses entre los gestores y los titulares de los datos y establece salvaguardias adecuadas para la protección de los derechos de dichos titulares;

b) Cuando el uso de la solución de IA sea necesario para el cumplimiento de un contrato con el titular de los datos y cuente con su consentimiento explícito, y siempre que el contrato no perjudique materialmente al titular de los datos ni vulnere los derechos humanos de este o de otras personas;

c) Cuando el interesado haya consentido libremente, con un conocimiento informado que incluya el propósito de la IA, las consecuencias de su uso y los procedimientos para retirar el consentimiento. Dicho consentimiento tendrá que prestarse mediante un acto concreto y el gestor responsable deberá proporcionar un sistema de gestión del consentimiento que permita retirarlo en cualquier momento e incluya la documentación adecuada;

d) Cuando, sobre la base de un interés legítimo y preponderante del gestor y/o de un interés social importante, los titulares de los datos estén debidamente informados antes de que comience el tratamiento de los datos y se les dé la oportunidad de oponerse a este, o tengan derecho, como mínimo, a acceder al mecanismo o los procedimientos establecidos, en un plazo razonable, o a modificar su situación;

e) Cuando toda solución de IA esté vinculada y limitada al propósito para el que fue originalmente diseñada, implementada y correctamente documentada. Si bien ello no impediría otros usos adicionales (como un tratamiento ulterior) o el uso por parte de otro gestor, el uso ulterior tendría que evaluarse de nuevo en lo que respecta a la base jurídica y las medidas de salvaguardia, incluidos los propósitos aparentemente compatibles;

f) Cuando se hayan establecido condiciones especiales para proteger y proporcionar bases jurídicas para la aplicación de soluciones de IA a los titulares de los datos, en especial a los pertenecientes a categorías especiales, sensibles o vulnerables, como los niños, los reclusos u otros grupos.

Fundamentos de los datos

33. La calidad de los datos incluye la consideración de aspectos precisos, como la divisa y la no discriminación, así como la reducción al mínimo necesario y la limitación de los propósitos. Deben abordarse los requisitos de protección de los datos, así como cualquier requisito adicional para el procesamiento de datos específicos, como los relacionados con la salud o los relativos a niños.

Responsabilidad y supervisión

34. Dentro de una organización, cada solución de IA necesita que una persona jurídica o física asuma la plena responsabilidad del tratamiento de los datos y de sus resultados. Ello abarca todos los aspectos de la gestión del proceso y de la tecnología, incluida la legalidad del tratamiento de los datos, su documentación, la adaptación, los resultados, la verificabilidad fiable del conjunto de datos del algoritmo, el tratamiento, la consideración y colaboración en lo que se refiere al planteamiento interno y el respeto de los derechos de los

titulares de los datos. Cuando la solución de IA se distribuye más allá de la organización, es necesario identificar, documentar y acordar las responsabilidades de las partes a las que se distribuye dicha solución.

35. Esas responsabilidades, también en el caso de que haya un procesador de la solución de IA, deben ser transparentes y debidamente accesibles para los titulares de los datos, así como para las autoridades públicas de supervisión y los reguladores.

36. Una gobernanza adecuada, especialmente en el caso de entidades legales de mayor envergadura, puede incluir un encargado de la privacidad de los datos, cuyas responsabilidades y funciones incluyan el asesoramiento sobre el cumplimiento de los requisitos de privacidad de los datos y la supervisión de la aplicación de la solución de IA. El puesto de encargado de la privacidad de los datos debe estar dotado de los recursos y la autoridad necesarios para llevar a cabo esas funciones, y la persona que lo ocupe debe recibir formación completa y adecuada o estar cualificada, ya sea mediante certificación o en razón de la experiencia acumulada, para desempeñar las funciones y tareas de manera efectiva e independiente. Se recomienda vivamente el establecimiento de canales de comunicación efectivos entre quienes desempeñen esa función y el organismo de vigilancia o supervisión pertinente. En los Estados más pequeños y en las empresas de nueva creación, es necesario invertir en la gobernanza de la IA, tanto si ello conlleva la creación de dicho puesto como si no.

37. La información sobre estos acuerdos en materia de responsabilidad debe estar a disposición del público.

38. Es necesaria la supervisión por parte de un regulador independiente y competente, así como que exista la posibilidad de recurrir a la vía judicial en caso de que se infrinja la legislación pertinente.

Control

39. Las soluciones de IA, incluidas las adquiridas a un tercero, han de estar bajo el control pleno del gestor correspondiente. Desde la primera idea respecto del diseño hasta la desconexión y el desmantelamiento final, debe quedar claro qué datos se procesan en la solución de IA, qué parámetros y mediciones de la calidad de los datos sirven de base para la toma de decisiones y cómo se equilibrarán y ponderarán entre sí. Los resultados han de ser controlados de manera continua y corregidos de ser necesario. En el ámbito de las soluciones de toma de decisiones automatizadas, no han de tomarse decisiones basadas en prejuicios conscientes o inconscientes. Han de comprobarse y corregirse los posibles efectos relacionados con los prejuicios y la discriminación antes de poner en marcha un sistema y a intervalos regulares durante su vida útil.

40. En el caso de la IA para sistemas de apoyo a la toma de decisiones, se requiere una serie similar de controles para el encargado de tomar las decisiones.

41. El gestor, junto con los procesadores si fuera necesario, ha de poder detener o modificar el procesamiento en cualquier momento. Han de documentarse los resultados incorrectos, así como las medidas correctoras adoptadas, a fin de mitigar cualquier riesgo para los titulares de los datos. Una vez que se haya completado su uso con fines de identificación, corrección o análisis, los resultados incorrectos han de eliminarse sin demora.

42. Han de establecerse revisiones internas y externas del funcionamiento de dicho control a fin de poder abordar cualquier aspecto crítico de la solución de IA o de sus resultados.

Transparencia y “justificación”

43. Las soluciones de IA han de ser transparentes para el público y los titulares de los datos. La información ha de tener sentido, ser inteligible y abarcar todos los aspectos pertinentes en lo que se refiere a la evaluación de la solución y los posibles derechos de los titulares de los datos. Ello incluye la “justificación” del propósito, las funciones generales, los procesos de apoyo, las fuentes de los datos utilizadas y el alcance del resultado previsto. Esos aspectos pueden incluir:

a) Las fuentes de los datos y los datos utilizados para alimentar y entrenar la solución de IA, además de los datos resultantes de dicha solución;

b) El propósito y la base jurídica del procesamiento;

c) Los parámetros que constituyen la base de las decisiones de la IA y su ponderación;

d) La aclaración de si la solución de IA tiene por objeto preparar las decisiones finales que vayan a tomar seres humanos (apoyo a la decisión) o si se trata de la toma de la decisión final misma (toma de decisiones automatizada);

e) La manera de distribuir las responsabilidades entre el gestor y el procesador, de no ser idénticas, así como la información de contacto y los posibles canales de comunicación;

f) La incorporación de terceros (por ejemplo, otros gestores o procesadores), la transferencia a otros países (de haberla) y el motivo de la incorporación y la transferencia. También se requiere una declaración de que los terceros están obligados a cumplir los mismos requisitos, como los relativos a la protección de datos, que el gestor, y que sus funciones y responsabilidades son similares, con independencia del lugar en que se encuentren;

g) La publicación de la información necesaria, al menos en la política de privacidad de datos relativa a la solución de IA. Dicha información ha de ser accesible, comprensible y pertinente para los titulares de los datos.

Derechos del titular de los datos

44. Las personas o grupos de personas cuya información personal o identificable sea procesada por la solución de IA (titulares de los datos) tendrán derecho a:

a) Comprender y consultar, para poder verificarlo de manera inteligible, si los datos personales se almacenan en archivos automatizados de datos y, en caso afirmativo, con qué finalidad, y qué autoridades públicas o personas u organismos privados controlan o pueden controlar sus archivos;

b) Retirar el consentimiento sin consecuencias negativas en cualquier momento del procesamiento, si ese consentimiento fue dado y utilizado como base legal para dicho procesamiento;

c) Oponerse al procesamiento de los datos por motivos justificados en cualquier momento si el procesamiento se basa en un interés legítimo;

d) Obtener información sobre el cumplimiento de todos los requisitos de privacidad de los datos enumerados en la presente sección;

e) Obtener acceso proporcionado a sus datos con una información completa por escrito sobre sus datos personales, el uso y el procesamiento de estos, así como los resultados y la manera en que esos resultados pueden afectar a su posición y a sus derechos individuales;

f) Solicitar que sea un ser humano el que adopte la decisión si tiene dudas razonables de que la decisión propuesta o tomada por la solución de IA no es precisa o correcta;

g) Corregir los datos si son inexactos;

h) Presentar una reclamación y recibir una reparación si se estima la reclamación;

i) Borrar y depurar los datos si el propósito de la solución de IA deja de existir o si los datos ya no son necesarios para otra finalidad legal.

45. Estos derechos no dejan sin efecto otros derechos ni van más allá de aquellos de que gocen los titulares de los datos en virtud de la legislación aplicable en una jurisdicción determinada.

Salvaguardias

46. Las soluciones de IA deben funcionar de manera sólida y deben estar aseguradas contra los riesgos mediante salvaguardias apropiadas, utilizando métodos que fomenten la confianza y la comprensión de todas las partes implicadas, incluidos los titulares de los datos y el público. Antes de su despliegue, todas las soluciones de IA, aunque sea a modo de prueba, han de someterse como mínimo a una evaluación inicial de los riesgos para los derechos humanos y la protección de los datos que identifique los riesgos y puntos críticos específicos asociados a la solución prevista. En función del resultado de esa evaluación inicial, puede ser necesaria una nueva evaluación de los derechos y de los riesgos.

47. Utilizando un enfoque de "privacidad por diseño", han de evaluarse individualmente las salvaguardias técnicas y organizativas para mitigar los riesgos identificados. Ello debe incluir medidas como la anonimización o seudonimización, el cifrado, la separación de clientes, la gestión del acceso (limitación), la política de eliminación de datos y la supervisión de los registros y actividades.

48. Durante la evaluación de los riesgos han de examinarse nuevos riesgos y desafíos resultante de los avances tecnológicos, arquitectónicos y/o estructurales, como la informática distribuida.

49. La mitigación de los riesgos puede basarse en normas internacionales, como las publicadas conjuntamente por la Organización Internacional de Normalización y la International Electrotechnical Commission en la serie ISO/IEC 27000 (sistemas de gestión de la seguridad de la información). En particular, la norma ISO/IEC 27701 contiene ampliaciones sobre la privacidad de los datos que establecen, como mínimo, medidas de:

a) Protección: controles para proteger contra los efectos de los riesgos evaluados;

b) Detección: controles para detectar las anomalías lo antes posible;

c) Respuesta: controles para contener y eliminar el riesgo de eventos anormales y garantizar que los procesos empresariales básicos puedan seguir funcionando hasta que se encuentre la solución global y la situación vuelva a la normalidad.

B. Evaluación de la criticidad de las soluciones de inteligencia artificial

50. Las medidas que se adopten han de estar centradas en el ser humano y ser proporcionales a los riesgos de vulneración de los derechos humanos, en especial la discriminación, y la protección de datos, así como a la complejidad o criticidad de una solución de procesamiento de datos. A continuación se enumeran algunos enfoques adecuados.

Evaluación de los derechos humanos en la fase de planificación

51. Todas las soluciones de IA han de respetar la primacía de la ley, los derechos humanos, los valores democráticos y la diversidad. Así pues, toda solución de IA planificada, también los algoritmos, debe someterse a una evaluación oportuna de los derechos humanos, incluidas evaluaciones en relación con la ética y la igualdad. El derecho a la igualdad de trato no ha de ser vulnerado por la solución de IA prevista. Por ejemplo, las soluciones de IA que utilicen información que refleje un sesgo inconsciente conducirán a resultados que podrían discriminar a determinadas personas o grupos de la sociedad. Además, una solución de IA alimentada con la información "correcta" puede conducir a resultados "erróneos", ya que el aprendizaje de la solución de IA derivado de la información recogida podría llevar a suposiciones erróneas por parte de dicha solución.

52. La privacidad por diseño y por defecto requiere una evaluación en la fase de planificación de cómo los derechos humanos, incluido el derecho a la privacidad, podrían verse afectados por la aplicación de la solución de IA.

Fase de pruebas y correcciones – supervisión

53. Tras la fase de planificación y la evaluación inicial de los derechos humanos, las condiciones marco identificadas han de tenerse en cuenta en la fase de desarrollo posterior. Durante la fase de implementación y antes de la puesta en marcha, las soluciones de IA deben someterse a una fase de prueba intensiva, con datos de prueba en un entorno independiente y autónomo, al objeto de evaluar si los supuestos generales subyacentes no sólo se tienen en cuenta, sino que se cumplen. Sólo si el gestor responsable puede estar seguro de que la solución de IA funciona correctamente, debe ponerse dicha solución en marcha para un funcionamiento real.

54. Durante todo el tiempo en que esté en funcionamiento la solución de IA, hasta la desconexión final, los resultados producidos por ella han de ser supervisados teniendo en cuenta los requisitos fundamentales definidos en la fase de planificación.

55. Las dificultades para controlar todos los aspectos de las operaciones de los algoritmos y el cambio constante de estos durante el tiempo de funcionamiento de una solución de IA hacen que sea esencial verificar constantemente los resultados teniendo en cuenta el objetivo inicial de la solución de otra forma viable para proporcionar un elemento de comparación. Si se sospecha o se observa una desviación, la alimentación de datos para la solución de IA debe adaptarse en consecuencia o detenerse la solución.

56. Para obtener los beneficios de los nuevos enfoques creativos y ampliar el horizonte del desarrollador y del gestor, es necesario tener en cuenta, en el desarrollo, las pruebas y el seguimiento de las soluciones de IA, las aportaciones y los comentarios de las comunidades de usuarios, sociedad civil, sectores interrelacionados y del ámbito privado. Ha de establecerse un mecanismo de prueba para las soluciones de IA listas para la puesta en funcionamiento, por ejemplo, con la instalación de una denominada caja negra en Internet en la que la solución, por separado y de manera autónoma, esté abierta a que terceros introduzcan datos para comprobar el tipo de resultados que producirá dicha solución, o bien con la implementación por parte de los reguladores de campos de pruebas en el seno de las organizaciones que participen en la introducción de soluciones de IA.

Evaluación de la criticidad basada en el uso de diferentes tipos de datos

57. Además de la planificación, la realización de pruebas y la implementación adecuadas, la criticidad de los datos y la finalidad prevista también son aspectos necesarios a tener en cuenta para un procesamiento adecuado.

58. Esto es de aplicación a los datos generales, como la información personal general o los datos en el contexto de los servicios de telecomunicaciones o de la salud. Los datos relacionados con la salud y algunos otros tipos de información, como los contenidos de las telecomunicaciones, tienen que ser tratados con más rigor que la información personal menos sensible. Esto significa que, en relación con otros supuestos, han de reforzarse las medidas técnicas y organizativas pertinentes, como la limitación estricta del propósito y la minimización de los datos, el cifrado, la seudonimización, el acceso restringido y la eliminación temprana o la anonimización.

59. El uso previsto de los datos desempeña un papel fundamental a la hora de determinar el nivel de protección necesario. Si la información personal se procesa únicamente con fines de almacenamiento, esto podría ser menos crítico que los usos para la elaboración de perfiles. La legitimidad del propósito y las medidas de salvaguardia han de evaluarse con sumo cuidado.

60. Estas medidas han de ser adoptadas y documentadas en todas las evaluaciones de riesgo.

Realización de la evaluación periódica de los sistemas de inteligencia artificial, registro de esta y mantenimiento de datos a disposición de auditorías externas y organismos reguladores

61. La evaluación valora el sistema en cuanto a:

a) Resultados previstos o no previstos;

b) Equidad, parcialidad y discriminación en relación con personas y grupos;

c) Compensaciones y mitigaciones.

C. Consideraciones adicionales

Auditorías externas y certificación

62. Las auditorías y los sistemas de certificación deben tener acceso a toda la documentación interna pertinente, como los registros de evaluación, a fin de supervisar el cumplimiento de los sistemas de IA con normas de ingeniería y ética elaboradas mediante enfoques multilaterales y multisectoriales.

63. Se debe considerar la certificación externa de un auditor homologado en materia de privacidad de datos que también sea reconocido formalmente como experto en IA. Esto puede ser útil para disipar las inquietudes del público y de los titulares de los datos. Puede ser de especial aplicación en el caso de soluciones de IA que podrían dar lugar a resultados adversos importantes y a una pérdida de confianza por parte del público y/o de la comunidad reguladora.

Cambios en la legislación y la normativa

64. En todo el mundo se están estudiando cambios en la legislación y la normativa que afectarán a la mayoría de las soluciones de IA. Su observancia dependerá en gran medida de:

a) El cumplimiento de las normas nacionales e internacionales en vigor y de las que se adopten;

b) La certificación por una autoridad de certificación apropiada que actúe en el marco de un acuerdo nacional o internacional.

Participación en los debates

65. Los responsables de estrategias de IA y/o de soluciones operativas de IA, así como los que supervisan sus usos, deben participar en debates sobre la IA y las nuevas cuestiones éticas y técnicas.

Educación y sensibilización

66. La IA es un tema complejo, y el despliegue de los datos en los sistemas de IA y su uso en las soluciones de IA requiere explicaciones claras y exhaustivas a los usuarios y los proveedores de datos, así como a los ejecutivos, gestores y otras personas que participan en las decisiones sobre soluciones de IA y el funcionamiento de estas. La publicación de algoritmos por sí sola es insuficiente.

II. Principios y recomendaciones sobre el derecho a la privacidad de los niños

67. Los niños, como todas las personas, son titulares de derechos humanos y libertades. Instrumentos jurídicos internacionales y regionales desarrollan el derecho a la privacidad y el derecho de los niños a la privacidad[3].

68. Los principales instrumentos que consagran los derechos del niño son la Declaración Universal de los Derechos Humanos y la Convención sobre los Derechos del Niño, que ha logrado una aceptación casi universal con la ratificación de 193 partes.

[3] Entre ellos figuran instrumentos regionales, como la Carta Africana sobre los Derechos y el Bienestar del Niño (1990) y el Convenio Europeo sobre el Ejercicio de los Derechos de los Menores (1996), así como mecanismos regionales, como el mecanismo interamericano de protección de los derechos humanos.

69. El artículo 16 de la Convención dispone que:

1) Ningún niño 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 a su reputación.

2) El niño tiene derecho a la protección de la ley contra esas injerencias o ataques.

70. Este artículo ha de interpretarse de manera amplia para dar cabida en toda su extensión a las experiencias de los niños en relación con la privacidad[4].

71. Los derechos del niño son universales, indivisibles e interdependientes y están relacionados entre sí[5]. El derecho del niño a la privacidad le permite acceder a otros derechos fundamentales para el desarrollo de la personalidad y la persona[6], como el derecho a la libertad de expresión[7] y de asociación y el derecho a la salud, entre otros. La privacidad de los niños está relacionada con su integridad física y psíquica, su autonomía para tomar decisiones, su identidad personal, su privacidad en relación con la información y su privacidad desde el punto de vista físico y espacial.

72. Las bases de la vida intelectual, emocional y sexual futura se desarrollan en la infancia y la adolescencia, ayudadas por las condiciones de una vida privada[8]. En todo el mundo, las experiencias de la infancia y el derecho a la privacidad difieren[9]. Hay factores interseccionales, como la raza, que afectan a la construcción de la infancia[10].

73. Por lo general, los ámbitos decisivos para la formación de la personalidad de los niños son la familia y la vida en el hogar, la escuela y las redes sociales. Al igual que los derechos del niño, esos ámbitos están interrelacionados y reflejan factores estructurales subyacentes.

74. Los niños sin hogar y sin familia, como los no acompañados, los que viven en la calle, los que están bajo el cuidado de un centro de acogida, los que se encuentran en zonas de conflicto y los que están en otras situaciones vulnerables, tienen muchas más dificultades para disfrutar de sus derechos humanos[11].

75. Si bien la privacidad significa cosas diferentes para cada persona, el Relator Especial hace hincapié en el aspecto positivo y facilitador del derecho a la privacidad que va a la dignidad innata de la persona y facilita el disfrute de otros derechos humanos[12].

76. La “autodeterminación” se define como la capacidad de la persona para decidir si divulga, y en qué medida, aspectos de su vida personal[13]. La autonomía se entiende como la capacidad de autodirección en el pensamiento, los sentimientos y las acciones. El término “niño” hace referencia a una persona menor de 18 años.

[4] John Tobin y Sarah M. Field, “Article 16: The right to protection of privacy, family, home, correspondence, honour, and reputation”, en *The UN Convention on the Rights of the Child: a commentary*, John Tobin, ed. (Oxford, Oxford University Press, 2019).

[5] Comité de los Derechos del Niño, observación general núm. 16 (2013), párr. 12.

[6] Documento de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH), Oficina Regional para Oriente Medio y Norte de África (no se ha dado autorización para publicar el documento).

[7] Documento de la Federación Internacional de Asociaciones de Bibliotecarios y Bibliotecas, pág. 2. En los casos en que se concedió la autorización, la información recibida por el Relator Especial en respuesta a sus consultas se publicará en www.ohchr.org/EN/Issues/Privacy/SR/Pages/CFI_Privacy_and_Children.aspx.

[8] Documento de Belgian Disability Forum, pág. 2.

[9] Documentos de InternetLab y Alana Institute; Office of the Victorian Information Commissioner, Australia.

[10] Rebecca Epstein, Jamila Blake y Thalia González, “Girlhood interrupted: the erasure of black girls’ childhood”, Georgetown Law Center on Poverty and Inequality, 2017.

[11] Documento de Maat for Peace, Development and Human Rights, pág. 7.

[12] Véase resolución 68/167 de la Asamblea General, resolución 20/8 del Consejo de Derechos Humanos y A/HRC/13/37.

[13] Resumen de la sentencia del Tribunal Constitucional Federal alemán de 15 de diciembre de 1983, 1 BvR 209, 269, 362, 420, 440, 484/83 [CODICES].

Identificación de las víctimas

Intereses en tensión

77. Considerar de qué manera el derecho a la privacidad y a la personalidad de los niños remite a la autonomía es examinar las tensiones y las diferentes perspectivas en las que se apoyan esos derechos.

78. La Convención sobre los Derechos del Niño otorga a los Estados partes y a los padres la capacidad y la obligación, cuando sea necesario, de decidir sobre el disfrute de los derechos del artículo 16 por parte de los niños, en función de la evolución de su capacidad (art. 5), a fin de garantizar el interés superior del niño (art. 3)[14].

79. Tradicionalmente, el derecho a la privacidad de los niños se ha considerado una cuestión que deben determinar los adultos. No obstante, las necesidades de privacidad de los niños difieren de las de los adultos y pueden entrar en conflicto con ellas[15]. Por ejemplo, la divulgación de información sobre los hijos puede hacer que entre en conflicto el derecho a la libertad de expresión de los padres con el derecho a la privacidad de sus hijos[16].

80. Las interpretaciones de los adultos sobre las necesidades de privacidad de los niños pueden impedir el desarrollo saludable de la autonomía y la independencia, y restringir la privacidad de los niños en nombre de la protección[17]. La utilización por los adultos de la vigilancia para proteger a los niños es un ejemplo de ello. Limita los derechos de los niños a la privacidad y la autonomía, y sin embargo los niños están cada vez más sometidos a vigilancia tecnológica por parte de los Gobiernos, el sector privado, los padres, la familia y los compañeros[18]. La vigilancia de los padres aumenta, en lugar de disminuir, con la edad del niño, es decir, cuando los jóvenes son (o deberían ser) más independientes[19]. Los padres y cuidadores de niños con necesidades adicionales están a favor de posturas aún más protectoras que implican configuraciones de privacidad por defecto elevadas, así como la capacidad de determinar la privacidad en línea de los niños[20].

81. El comportamiento de los padres puede estar en contradicción con las preocupaciones que estos declaran. Según los informes, el 57 % de los padres de adolescentes de entre 13 y 17 años se preocupan por el hecho de que sus hijos reciban o envíen imágenes explícitas[21], y al 85 % le preocupa la privacidad digital de sus hijos. No obstante, menos de uno de cada tres padres utiliza la configuración parental en el dispositivo de sus hijos, y el 81 % deja que sus hijos utilicen YouTube para el público general sin supervisión[22].

82. Una investigación reciente que indica que los adultos que no han sufrido daños en línea, como amenazas violentas o troleo, son más proclives a restringir el acceso a la información y el anonimato en línea, pone de manifiesto la necesidad de evaluaciones de riesgos, políticas y reglamentaciones centradas en los niños[23].

---

[14] Tobin y Field, “Article 16”.

[15] Documentos de Parental Rights Foundation; Action Canada for Sexual Health and Rights, pág. 4; Commission Nationale de l’Informatique et des Libertés (CNIL), pág. 11.

[16] Documento de South Australia Commissioner for Children and Young People (en el que el término “sharenting” se explica como la creciente tendencia de los padres y futuros padres a utilizar Internet para publicar información sobre sus hijos en línea, lo que conforma una identidad en línea del niño mucho antes de que éste tenga capacidad para dar su consentimiento o comience a crear su propia huella digital), pág. 3.

[17] Documento de International Child Rights Center y MINBYUN.

[18] *Ibid.*; Jane Bailey y Valerie Steeves, *Defamation Law in the Age of the Internet: young people’s perspectives* (Law Commission of Ontario, Canadá, 2017); Documento de Ariel Foundation International.

[19] Documento de South Australia Commissioner for Children and Young People.

[20] Véase www.ofcom.org.uk/__data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf.

[21] Monica Anderson “A majority of teens have experienced some form of cyberbullying”, Pew Research Center, 27 de septiembre de 2018.

[22] Documento de ACT/The App Association.

[23] BT/DEMOS, “Online harnesses: a snapshot of public opinion” (2020). Puede consultarse en https://demos.co.uk/wp-content/uploads/2020/10/Online-Harms-A-Snapshot-of-Public-Opinion-1.pdf.

83. A medida que maduran, los niños quieren y requieren privacidad, no solo en relación con las escuelas, las empresas y los gobiernos, sino también con sus padres[24]. Esa necesidad aumenta cuando los niños van creciendo. Mientras que los niños de entre 5 y 7 años no consideran en general que la vigilancia de sus actividades en línea por parte de los padres constituya una vulneración de la privacidad, los adolescentes de entre 15 y 17 años suelen estar preocupados por la vigilancia de que son objeto por parte de los padres y de la escuela[25]. Los adolescentes creen que la privacidad y los espacios privados alejados de los juicios y la vigilancia les permiten explorar ideas y expresiones creativas y desarrollar opiniones independientes[26]. Los controles parentales han de ser proporcionales a la evolución de la capacidad y las opiniones del niño[27].

Identidad personal

84. Los niños de hoy son la primera generación que nace en la era digital[28], y sus padres son los primeros en criar "niños digitales"[29].

85. Cada vez más, la identidad de un niño comienza antes de su nacimiento, con imágenes en el útero compartidas por padres y familias en la web. Muchas de esas imágenes incluyen información personal.

86. La formación de la identidad digital de los niños continúa en gran medida a través de acciones de la familia durante toda la infancia: el 80 % de los niños que viven en los países occidentales desarrollados tienen una huella digital antes de los 2 años[30]. También se han utilizado sin consentimiento imágenes de niños para recaudar fondos con fines benéficos[31].

87. Los niños participan ahora en línea de múltiples maneras y a edades más tempranas que antes[32]. Su uso de las redes sociales experimenta un cambio sustancial entre los 9 a 10 años y los 11 a 12 años, cuando pasa del 34 % al 69 %[33]. El número de contactos en línea que tienen los niños se duplica entre el primero y el último curso de la enseñanza secundaria[34]. Muchos niños menores de 13 años tienen perfiles en las redes sociales (el 38 % de los niños de entre 9 y 12 años, según estudios europeos)[35] y la mayoría tiene entre dos y cinco perfiles[36]. La pandemia de enfermedad por coronavirus (COVID-19) ha incrementado esa tendencia; así las cuentas activas diarias de Messenger Kids de Facebook han crecido un 350 % de marzo a septiembre de 2020[37].

88. Cada vez más, la autoestima y el autoconcepto, necesarios para la formación de la personalidad y la identidad, se construyen digitalmente[38]. Los niños utilizan Internet como un informe continuo de sus vidas, y los corazones y los pulgares arriba en las redes sociales

[24] Documentos de Future of Privacy Forum; Ariel Foundation International.
[25] Documento de Global Privacy Assembly, Digital Education Working Group, pág. 25.
[26] Documento de Office of the Victorian Information Commissioner, Australia.
[27] Documento de CNIL, pág. 11.
[28] Documento de la Comisión de Derechos Humanos de Australia, pág. 2.
[29] Danah Boyd, "Social network sites as networked publics: affordances, dynamics, and implications", en *A Networked Self: Identity, Community, and Culture on Social Network Sites*, Zizi Papacharissi ed. (Routledge, 2011).
[30] Documento del Organismo Nacional de Protección de Datos y Libertad de la Información de Hungría, pág. 42.
[31] Documentos de International Child Rights Center y MINBYUN; Defensoría de la Infancia de Croacia, pág. 3.
[32] Documentos de Information Commissioner's Office, Reino Unido; CNIL; Comisionado de Información y Protección de Datos de Albania.
[33] Documento de la Comisión Económica para América Latina y el Caribe (CEPAL).
[34] Documento del Organismo Nacional de Protección de Datos y Libertad de la Información de Hungría, pág. 29.
[35] *Ibid.*, pág. 53.
[36] Documento del Comisionado de Información y Protección de Datos de Albania, pág. 14.
[37] Documento de Facebook.
[38] Documentos de Anna Bunn, pág. 11; Office of the Victorian Information Commissioner, Australia, pág. 2.

se convierten en apéndices de sus pensamientos[39]. No obstante, les preocupa perder el control de la información que hay sobre ellos en línea[40].

89. La violencia, el abuso sexual y el ciberacoso están presentes en la vida digital, especialmente en el caso de los jóvenes pertenecientes al colectivo de personas lesbianas, gais, bisexuales, transgénero, queer e intersexuales (LGBTQI) (véase A/HRC/43/52). Alrededor del 25 % de los adolescentes de entre 13 y 17 años han comunicado haber recibido imágenes explícitas sin su consentimiento[41]. Un 29 % de las chicas y un 20 % de los chicos han comunicado haber recibido imágenes explícitas no solicitadas. La recepción y distribución no deseada de imágenes, incluso cuando no son objetivamente dañinas, ofensivas o vergonzosas, puede afectar al desarrollo de la autoestima, la autonomía y las relaciones del niño, así como a su desarrollo psicosocial[42].

90. El abuso sexual infantil, ya sea en línea o fuera de ella, es una vulneración de la integridad corporal y de la autonomía de decisión. Tiene consecuencias a largo plazo en la personalidad y la capacidad; y la constante existencia en línea de material relacionado con el abuso sexual infantil agrava esas consecuencias. Las formas y consecuencias de los abusos están arraigadas en la forma en que la sociedad ve a los niños y los cuerpos de estos[43]. La lucha contra esos abusos requiere estrategias basadas en los derechos humanos[44]. La inmersión de los jóvenes en la creciente gama de tecnologías digitales produce un flujo continuo de datos, recogidos y mejorados por la inteligencia artificial, las aplicaciones de aprendizaje automático y las tecnologías de reconocimiento facial y de reconocimiento de voz. Los niños y sus datos alimentan el negocio del mundo digital[45]. El valor del mercado de la publicidad en línea para niños podría ascender a 1.700 millones de dólares en 2021, y la cifra de los datos recogidos por las empresas de publicidad en línea sobre cada niño antes de cumplir los 13 años podría superar los 72 millones[46].

91. Los operadores de mercado llegan a los jóvenes, influyen en estos y forjan relaciones continuas con ellos. Los niños más pequeños son especialmente vulnerables a la publicidad dirigida, ya que no diferencian entre la publicidad y el contenido o entre la ficción y la realidad, ni comprenden la naturaleza persuasiva de la publicidad[47]. La tecnología que incorpora técnicas de comportamiento (diseño persuasivo/prácticas oscuras) aprovecha al máximo la vinculación, desencadena comportamientos impulsivos, influye en la toma de decisiones, despierta el miedo a la exclusión y anula la preocupación por la privacidad[48].

92. La elaboración de perfiles de los niños limita su potencial de autodesarrollo en la infancia, la adolescencia y, posiblemente, la edad adulta, ya que las predicciones de comportamiento y las técnicas de incentivo pueden predeterminar opciones y elecciones. Las ofertas tecnológicas han de evaluarse teniendo en cuenta los derechos y el interés superior del niño[49], habida cuenta de que el procesamiento de los datos personales del niño puede:

a) Vulnerar la privacidad y la protección de datos, y provocar una pérdida de autonomía y daños a la reputación personal;

[39] Documento de Ariel Foundation International.

[40] Documentos de C. Mahieu; Office of the Victorian Information Commissioner, Australia; CNIL.

[41] Monica Anderson “A majority of teens have experienced some form of cyberbullying”.

[42] Documento de Bunn; Mahieu.

[43] Documento de InternetLab y Alana Institute.

[44] Comité para la Eliminación de la Discriminación contra la Mujer, recomendación general núm. 38 (2020); Documento de Maat for Peace, Development and Human Rights, pág. 7.

[45] Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books, 2019); documento de InternetLab y Alana Institute.

[46] Documento de CNIL, pág. 3.

[47] Documentos de Campaign for Commercial-Free Childhood y Center for Digital Democracy; InternetLab y Alana Institute; CNIL.

[48] Documentos de Information Commissioner’s Office, Reino Unido; Office of the Victorian Information Commissioner, Australia; Mahieu. Jonathan Crock y otros, American University; CNIL; CEPAL.

[49] Documentos de Comisión de Derechos Humanos del Canadá, pág. 2.; Office of the Victorian Information Commissioner, Australia; Campaign for Commercial-Free Childhood y Center for Digital Democracy.

b) Afectar a la salud mental y emocional del niño, así como a su bienestar físico;

c) Dar lugar a daños económicos o a la explotación comercial[50].

93. Los niños y jóvenes buscan respuestas que reduzcan al mínimo el acceso y el uso de sus datos por parte de las empresas[51], una zonificación de la actividad comercial y mecanismos para proteger su interés superior, incluida la posibilidad de borrar el material publicado[52]. Los niños creen que deberían poder ejercer el derecho a pedir a cualquier empresa una copia de sus datos personales, alrededor del 40 % piensa que deberían poder presentar solicitudes de acceso a los datos o de eliminación de estos a cualquier edad, y el 21 % dice que deberían poder hacerlo con 13 años o menos. Sólo el 13,5 % considera que es necesario tener 18 años o más para presentar una solicitud de acceso a los datos o de eliminación de estos[53].

94. La era digital beneficia el desarrollo de los niños. No obstante, los niños han de poder disfrutar, sin que las prácticas comerciales lo impidan, de sus derechos al libre desarrollo de la personalidad.

95. Desde Sudamérica se ha informado de la utilización de tecnologías de vigilancia y rastreo biométrico para identificar y controlar a los niños sospechosos de cometer infracciones, así como de la falta de protección de la privacidad de los niños durante los procesos judiciales[54]. La identificación de niños de interés para las autoridades policiales o de hijos de padres encarcelados o asociados al terrorismo infringe la privacidad, conduce a la estigmatización y la discriminación y afecta al desarrollo de la personalidad[55]. El desarrollo puede verse afectado también cuando esos niños no están identificados por los servicios de apoyo pertinentes[56], aunque el intercambio de datos puede ser problemático, especialmente con personal de seguridad[57].

Sexualidad, género, integridad corporal y autonomía física

96. Los niños difieren enormemente en su capacidad física, intelectual, social y emocional. Las diferencias son especialmente pronunciadas en la adolescencia, un período caracterizado por rápidos cambios físicos, cognitivos y sociales, incluida la maduración sexual y reproductiva[58].

97. La expresión sexual, la integridad corporal y la autonomía física forman parte del entramado de la intimidad de los niños, y también de su libertad de expresión[59]. Los adolescentes necesitan poder tomar decisiones sobre su bienestar y su cuerpo, y explorar su sexualidad de forma segura y privada a medida que maduran[60], ya sea en línea o fuera de ella[61].

[50] Documento de Information Commissioner's Office, Reino Unido.
[51] Valerie Steeves, "Young Canadians in a wired world, phase III: trends and recommendations", MediaSmarts, 2014.
[52] Documento de Death Penalty Project.
[53] Documento de Global Privacy Assembly, pág. 24.
[54] Documento de InternetLab y Alana Institute.
[55] Comité de los Derechos del Niño, observación general núm. 24 (2019).
[56] Documento de Children of Prisoners Europe; Families Outside; International Coalition for the Children of Incarcerated Parents; Oficina Cuáquera ante las Naciones Unidas.
[57] Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), *Handbook on Children Recruited and Exploited by Terrorist and Violent Extremist Groups: The Role of the Justice System* (Viena, 2017) págs. 138 y 139; Naciones Unidas, Oficina de Lucha contra el Terrorismo, *Children affected by the foreign-fighter phenomenon: ensuring a child rights-based approach* (2019), pág. 103.
[58] Comité de los Derechos del Niño, observación general núm. 4 (2003).
[59] Documentos de Matimba; Consejo de Europa; Comisión de Derechos Humanos de Australia.
[60] Documento de Center for International Human Rights.
[61] Documento de ParentsTogether.

98. No obstante, los derechos del niño a la autonomía y la integridad corporal se ven vulnerados por acciones de Gobiernos, entidades comerciales, profesionales de la salud y de otros ámbitos, padres y compañeros. Entre las vulneraciones identificadas cabe mencionar[62]:

a) Niñas objeto de mutilación genital femenina; matrimonios forzados; sexo forzado; embarazo y maternidad forzados; pruebas de embarazo forzadas; esterilizaciones forzadas; denegación de información y servicios en materia de salud sexual y reproductiva; notificación y/o consentimiento obligatorio de los padres para la prescripción de anticonceptivos y la realización de abortos; terapias de "conversión"; sanciones penales por realizar una actividad sexual consentida con un compañero, incluido el intercambio de mensajes de texto de contenido sexual; abusos sexuales en línea y fuera de ella; asesinatos "por cuestiones de honor"; y "calificación de las chicas como prostitutas" ("slut shaming");

b) Niños objeto de mutilación genital; matrimonios forzados; sexo forzado; esterilizaciones forzadas; denegación de información y servicios en materia de salud sexual y reproductiva; terapias de "conversión"; sanciones penales por realizar una actividad sexual consentida con un compañero, incluido el intercambio de mensajes de texto de contenido sexual; abusos sexuales en línea y fuera de ella; acoso; y castigos corporales;

c) Niños y niñas con diversas identidades de género, orientaciones y expresiones sexuales, así como variaciones en las características sexuales que son objeto de violencia; discriminación y acoso; tratamiento de la identidad de género o del cuerpo como si fuese una patología; tratamiento médico innecesario; publicación de detalles relativos a los genitales; estigmatización; violación "instructiva"; terapias de "conversión"; denegación de servicios sanitarios específicos, incluidos información y servicios sexuales reproductivos y de atención a la salud; denegación del acceso al historial médico; sanciones penales por realizar una actividad sexual consentida con un compañero o compañera, incluido el intercambio de mensajes de texto de contenido sexual; abusos sexuales en línea y fuera de ella; y no reconocimiento legal del género.

99. Las vulneraciones de la privacidad corporal afectan a otros derechos, como los consagrados en los artículos 3, 6, 8, 12, 16, 19 y 29, párrafo 1, de la Convención sobre los Derechos del Niño. Así, por ejemplo[63]:

a) Las pruebas de embarazo obligatorias vulneran los derechos de las niñas a la dignidad, la igualdad y la autonomía;

b) Los estudios para identificar a los alumnos con sexo/género diverso vulneran el derecho a la no discriminación y, cuando sirven de base para expulsar a esos alumnos, vulneran el derecho de estos a la educación;

c) Las pruebas de virginidad "voluntarias", a menudo impuestas por los padres, vulneran los derechos de las niñas a la dignidad, la igualdad y la autonomía;

d) Los procedimientos muy medicalizados que implican una intervención quirúrgica para el reconocimiento legal del género afectan al derecho a la salud[64];

e) La notificación o el consentimiento obligatorio de los padres para la prestación de servicios de salud sexual o reproductiva afectan al derecho a la salud, la identidad, la vida, la protección contra daños y el respeto del interés superior del niño.

100. Los niños necesitan y tienen derecho a recibir orientación sobre relaciones sexuales saludables, consentimiento y prácticas seguras[65]. Una educación sexual integral puede ayudar

[62] Documentos de Crock y otros; Human Rights Watch; ILGA-Europa, Transgender Europe y The International Lesbian, Gay, Bisexual, Transgender, Queer and Intersex Youth and Student Organisation; NNID (Organización neerlandesa para la diversidad sexual); Choice for Youth and Sexuality; OutRight Action International; Comisión de Derechos Humanos de Australia; Center for International Human Rights; Consejo de Europa.

[63] Documento de Intersex International Europe.

[64] Documentos de Matimba; A. McCarthy.

[65] Comité de los Derechos del Niño, observación general núm. 15 (2013); Comité de Derechos Económicos, Sociales y Culturales, observación general núm. 22 (2016); Documentos de la Comisión de Derechos Humanos del Canadá; Mahieu; Center for Reproductive Rights, pág.1.

a los niños a proteger y desarrollar su intimidad, independencia y autonomía[66], así como facilitar el bienestar, en particular en el caso de los jóvenes pertenecientes al colectivo LGBTQI[67]. En países de todo el mundo, como el Brasil, la República Dominicana, Ghana, Kenia y Polonia, ha habido reacciones contrarias al ofrecimiento de una educación sexual integral a niños y adolescentes[68].

Reconocimiento de la identidad

101. Todas las personas tienen derechos precisamente en razón de su identidad inherente e igual en tanto que seres humanos[69]. Los datos y los sistemas de registro de datos establecen la identidad oficial[70], pero rara vez permiten a los niños adoptar decisiones en relación con los datos que se refieren a ellos.

102. La identidad oficial comienza con la inscripción del nacimiento. No obstante, muchos niños en todo el mundo y, de manera desproporcionada, en el caso de las comunidades aborígenes e indígenas, no están inscritos[71]. La falta de reconocimiento legal afecta al acceso a muchos derechos necesarios para la autonomía, como la educación.

103. Los certificados de nacimiento pueden plantear dificultades para lograr la dignidad, la identidad, la privacidad y el desarrollo en el caso de los niños transgénero e intersexuales, los niños nacidos en el contexto de acuerdos internacionales de maternidad subrogada, los niños desaparecidos, los niños refugiados no acompañados y los niños en régimen de acogida fuera del hogar, entre otros[72].

Educación y escolarización

104. El propósito de la educación es desarrollar la personalidad, las aptitudes y la capacidad mental y física del niño hasta el máximo de sus posibilidades[73]. La educación es un derecho humano y el principal vehículo para que los niños tengan una vida digna. Con ella, se empodera a los niños, individual y colectivamente, protegiéndolos de la explotación. El derecho a la educación requiere que los Estados lo respeten, lo protejan y lo hagan efectivo, eliminando los obstáculos a la educación, como la violencia y las prohibiciones en relación con el género[74].

105. Las escuelas desempeñan un papel destacado en la forma en que los niños experimentan la privacidad en el día a día. Cuando se declaró la pandemia de COVID-19, el 1 de abril de 2020, 193 países habían cerrado las escuelas, lo que afectó aproximadamente al 90 % de la población escolar mundial[75].

106. En razón de la educación en línea, las descargas de aplicaciones educativas aumentaron un 90 % en comparación con la media semanal a finales de 2019[76]. El cambio a la educación en línea hizo mayores los desequilibrios de poder existentes entre las empresas de tecnología de la educación y los niños, así como entre los Gobiernos y los niños y padres, y varios Gobiernos suspendieron la aplicación de las disposiciones legislativas en vigor sobre privacidad de datos de los niños. En Gales, por ejemplo, el Gobierno dejó de aplicar el

[66] Documentos de Action Canada for Sexual Health and Rights; ILGA-Europa, Transgender Europe y The International Lesbian, Gay, Bisexual, Transgender, Queer and Intersex Youth and Student Organisation.

[67] Documento de McCarthy.

[68] Documento de Human Rights Watch, párr.18.

[69] Dinah Shelton, "On identity", *The George Washington International Law Review*, vol. 39 (1999).

[70] Documento de Rights in Records by Design, Monash University y Federation University; *D. Z. c. los Países Bajos* (CCPR/C/130/D/2918/2016).

[71] Documento de la Comisión de Derechos Humanos del Canadá.

[72] Documentos de la Comisión de Derechos Humanos de Australia; Rights in Records by Design, Monash University y Federation University; Kathryn Allan and David Lacey, "Identity management in disaster response environments: a child exploitation mitigation perspective", *Australian Journal of Emergency Management*, vol. 33, núm. 3 (julio de 2018).

[73] Convención sobre los Derechos del Niño, art. 29, párr. 1 a).

[74] Resolución 75/166 de la Asamblea General.

[75] Documento de ParentsTogether.

[76] Documento de Human Rights Watch, párr.44.

requisito del consentimiento de padres y alumnos[77]. En otros lugares no existe una protección del derecho a la privacidad de los niños en las escuelas públicas[78]. No obstante, agentes no estatales controlan sistemáticamente los expedientes educativos digitales de los niños[79].

107. La digitalización y el almacenamiento de los datos de aprendizaje de los niños incluyen las características del pensamiento, la trayectoria del aprendizaje, la puntuación del compromiso, los tiempos de respuesta, las páginas leídas y los vídeos vistos[80]. La mayoría de los niños y los padres no tienen posibilidad de oponerse a los acuerdos de privacidad de las empresas de tecnología educativa o de negarse a proporcionar datos, ya que la educación es obligatoria[81].

108. La selección de aplicaciones y herramientas de aprendizaje basadas en la web por parte de las escuelas ha tenido en cuenta consideraciones curriculares y financieras más que de privacidad[82]. En septiembre de 2020, un análisis de 496 aplicaciones de tecnología educativa en 22 países puso de manifiesto que muchas de ellas recogían identificadores de dispositivos, 27 tomaban datos de localización y 79 de las 123 aplicaciones probadas manualmente compartían datos de los usuarios con terceros, como socios publicitarios[83]. La seguridad de los datos es preocupante. Microsoft, por ejemplo, informó de 5,7 millones de incidentes de programas maliciosos que afectaron a los usuarios de su *software* educativo entre el 24 de agosto y el 24 de septiembre de 2020[84].

109. Los propios centros escolares poseen una cantidad importante de información de los niños y cada vez hacen más seguimiento de estos controlando las actividades en línea de los estudiantes y con cámaras de vigilancia[85]. Al igual que las aplicaciones tecnológicas educativas, el uso de esa tecnología requiere responsabilidad, consentimiento fundado, limitación del propósito, reducción al mínimo de los datos, transparencia y garantías de seguridad[86].

110. Los procesos educativos no tienen que socavar el disfrute de la intimidad y de otros derechos, con independencia del lugar o la forma en que se imparta la educación[87], ni intensificar las desigualdades existentes; y no deben hacerlo[88].

Adecuación a la edad y capacidad evolutiva

111. El término “adecuado a la edad” se acepta generalmente como un ajuste entre la edad cronológica y los comportamientos, y un ajuste de la edad cronológica a los servicios disponibles para los niños, como los contenidos en línea. La adecuación a la edad, en el sentido normativo, es un criterio que deben seguir los proveedores en línea al prestar servicios acordes con la edad de los niños. Un ejemplo reciente es el Código de Diseño Adecuado a la Edad del Reino Unido de Gran Bretaña e Irlanda del Norte[89]. En los Estados Unidos de

[77] *Ibid.*, párr. 48.
[78] Documento de South Australia Commissioner for Children and Young People.
[79] Véase https://rm.coe.int/educational-settings/16809f3ba3.
[80] Documento de Global Privacy Assembly, pág. 4.
[81] Documentos de DefendDigitalMe; Consejo de Europa.
[82] Documento de Office of the Victorian Information Commissioner, Australia.
[83] Alfred Ng, “Education apps are sending your location data and personal info to advertisers”, CNET, 1 de septiembre de 2020.
[84] Documento de Human Rights Watch, párr. 49.
[85] Documento de South Australia Commissioner for Children and Young People.
[86] Documentos de InternetLab y Alana Institute; Grupo de Investigación sobre Tecnología, Información y Sociedad, Universidad de Fortaleza (Brasil); Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires; Consejo de Europa.
[87] Comité de los Derechos del Niño, observación general núm. 1 (2001); resolución 75/166 de la Asamblea General; documentos de DefendDigitalMe; Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires; Grupo de Investigación sobre Tecnología, Información y Sociedad, Universidad de Fortaleza (Brasil); Organismo Nacional de Protección de Datos y Libertad de la Información de Hungría, caso número NAIH/2020/7127/.
[88] Resolución 75/166 de la Asamblea General; documentos de Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires; CEPAL; Consejo de Europa.
[89] Véase https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/01/ico-publishes-code-of-practice-to-protect-children-s-privacy-online/.

América, la Ley de Protección de la Privacidad en Línea de los Niños, de 1998, impone requisitos a los operadores de sitios web y servicios en línea dirigidos a niños menores de 13 años, así como a los operadores de otros sitios web o servicios en línea que saben que están recogiendo información personal en línea de niños menores de 13 años.

112. No obstante, el criterio de adecuación a la edad no es una panacea, ya que:

a) El material puede ser adecuado a la edad y aun así ser perjudicial para los niños y sus derechos. El sistema puede proteger y empoderar a un niño cuando se individualiza, pero puede no satisfacer las necesidades de un conjunto de niños, habida cuenta de la considerable variación en el desarrollo intelectual y emocional que existe entre niños de la misma edad[90];

b) Como umbral genérico, la adecuación a la edad plantea desigualdades para niños de diferente capacidad y es una medida burda de sus capacidades evolutivas, ya que puede limitar el desarrollo de su personalidad y el ejercicio autónomo de sus derechos, y es posible que sea discriminatoria;

c) Cuando la edad es el criterio para acceder a los servicios, se requieren documentos de identidad verificables, lo que suscita preocupaciones en torno a la seguridad, los enfoques prescriptivos y la falta de criterios, herramientas y sistemas de certificación del sector para verificar la edad[91]. Otros indican que los procesos de verificación de la edad pueden llevarse a cabo de manera compatible con la privacidad[92].

113. La edad por sí sola se ha considerado un criterio de medición imperfecto para evaluar las capacidades de los niños[93]. Algunos países no reconocen la capacidad tomando como base la edad cronológica[94]. A principios de 2020, las autoridades de Ontario (Canadá) aprobaron legislación que permite a los jóvenes acceder a su información personal y solicitar que se corrija tomando como base explícitamente la capacidad, y no la edad. En caso de conflicto, los derechos del niño podrían prevalecer sobre las decisiones de los padres o tutores[95].

114. La mejor manera de determinar la preparación de los niños para la toma de decisiones y la autorresponsabilidad no es la edad cronológica por sí sola, sino el contexto, incluidos los riesgos existentes y el apoyo disponible, la experiencia individual, los derechos afectados y la capacidad para comprender las consecuencias de las acciones (o inacciones). La determinación de cuándo son capaces los niños, por ejemplo, de consentir en el tratamiento de sus datos personales, ha de tener en cuenta su comprensión real de dicho tratamiento, el interés superior del niño, los derechos de este y sus opiniones[96].

115. En esencia, la noción de adecuación a la edad no concuerda bien con el principio de capacidad evolutiva. El ajuste de los servicios a las capacidades en evolución de los niños requiere mayor análisis.

Opciones para las soluciones

116. Es fundamental que se atienda al máximo a la privacidad de los niños para actuar teniendo en cuenta su interés superior[97]. Un enfoque basado en el interés superior del niño requiere que los adultos soliciten las opiniones de los niños y las traten con seriedad. Esto no siempre queda claro en las actuaciones de los Estados, las empresas, los padres y otros[98]. No obstante, el derecho internacional reconoce a los niños como seres humanos, y no como

[90] Comité de los Derechos del Niño, observación general núm. 7 (2005).
[91] Documentos de CNIL, pág. 10; Facebook.
[92] Documento de Yoti.
[93] Véase https://www.dataprotection.ie/sites/default/files/uploads/2019-09/Whose%20Rights%20Are%20They%20Anyway_Trends%20and%20Hightlights%20from%20Stream%201.pdf.
[94] Documento de Global Privacy Assembly, pág. 20.
[95] *Ibid.*, pág. 25.
[96] Documento del Consejo de Europa.
[97] Documento de UNODC.
[98] Documento de Promsex.

meras futuras personas y, por tanto, los niños son titulares de derechos humanos con arreglo al derecho internacional[99].

117. Todas las partes (Gobiernos, empresas, comunidades, personas físicas y padres) han de reconocer a los niños como titulares de derechos. Así, para combatir de forma efectiva y exhaustiva el abuso infantil facilitado por las TIC, es necesario un enfoque multisectorial basado en los derechos humanos, que incluya de manera activa a los niños, las familias, las comunidades, los Gobiernos, la sociedad civil y el sector privado[100].

118. Aunque la dependencia de los niños, y por lo tanto su vulnerabilidad, puede conllevar riesgos, estos no equivalen a daños y es necesario sortear algunos riesgos para que los niños desarrollen resiliencia y habilidades para afrontar los problemas[101]. Definir a los niños únicamente por su vulnerabilidad, sin tener en cuenta su capacidad o su potencial, puede dar lugar a planteamientos excesivamente proteccionistas, que pueden ser perjudiciales para la personalidad del niño.

Protección de los datos sobre los niños

119. Aunque la privacidad es un concepto más amplio y complejo, la protección de los datos está estrechamente relacionada con él. Cuando se protege a las personas contra la recopilación, el almacenamiento, el uso y el intercambio ilimitados de datos personales, se fomenta el libre desarrollo de la personalidad.

120. Para muchos, el consentimiento es el fundamento. No obstante, el consentimiento no es necesariamente una expresión de la autonomía del niño ni la protege, especialmente cuando existen desequilibrios de poder. Además, el consentimiento de los padres no siempre responde al interés superior del niño ni se ajusta a la opinión de este[102].

121. Si bien el Reglamento General de Protección de Datos europeo podría proteger mejor los datos personales de los niños, incluye una protección especial de los menores al exigir información adaptada a ellos sobre el tratamiento de sus datos (art. 12)[103]; una especial vigilancia sobre la elaboración de perfiles de los niños (considerando 71); y un refuerzo del "derecho al olvido" (considerando 65). Asimismo, en el artículo 8 se reconoce la capacidad de los niños de entre 13 y 16 años para consentir en el tratamiento de los datos[104]. Además, los elementos generales de protección de los datos mediante el diseño, la privacidad por defecto, el derecho a no ser sometido a decisiones individuales automatizadas (art. 22) y las evaluaciones del impacto de dicha protección, merecen una aplicación más amplia con miras a la protección de los datos personales de los niños[105].

122. El Convenio 108+[106] también protege contra las decisiones basadas únicamente en el tratamiento automatizado de los datos (art. 1 a)), y las directrices recientemente adoptadas por el Consejo de Europa sobre la protección de datos de los niños en un entorno educativo amplían la definición de tratamiento de los datos personales para incluir las predicciones sobre grupos o personas con características compartidas, así como la definición de tratamiento de datos biométricos al objeto de incluir esos tipos de tratamiento[107].

[99] John Tobin, "Understanding children's rights: a vision beyond vulnerability", *Nordic Journal of International Law*, vol. 84, nº 2 (junio de 2015).

[100] Documentos de UNODC; Facebook.

[101] Documento de South Australia Commissioner for Children and Young People.

[102] Documento de la Defensoría de la Infancia de Croacia, pág. 4.

[103] Simone van der Hof and Eva Lievens, "The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR", *Communications Law*, vol. 23, No. 1 (2018).

[104] Por debajo de esa edad, el tratamiento de los datos requiere el consentimiento de los padres o del tutor en nombre del niño.

[105] Van der Hof y Lievens, "The importance of privacy".

[106] Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, modernizado por el Protocolo que lo modifica, Serie de Tratados del Consejo de Europa 223. Puede consultarse en https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (en inglés).

[107] Documento del Consejo de Europa.

Ingeniería de la privacidad y alfabetización digital

123. El diseño tecnológico puede ayudar a contrarrestar el "diseño persuasivo" y las "prácticas oscuras"[108], y promover los propósitos de las leyes y disposiciones normativas[109].

124. Junto con la ingeniería de la privacidad de las tecnologías digitales, los niños y los adolescentes necesitan destrezas operativas y habilidades cognitivas y sociales para utilizar las tecnologías de forma reflexiva, ética y segura. La alfabetización digital puede prevenir los comportamientos nocivos en línea en su origen[110]. Existe un amplio consenso, también entre los niños, en que la alfabetización digital puede reforzar su seguridad y autonomía en línea[111], especialmente teniendo en cuenta las edades cada vez más tempranas a las que los niños se conectan y las dificultades de los padres para proporcionar un apoyo efectivo[112].

125. No obstante, las soluciones técnicas y la alfabetización digital por sí solas son insuficientes sin una actuación rigurosa y continuada por parte de los Estados para afrontar las desigualdades estructurales y garantizar la privacidad, la protección de datos y la seguridad de los niños[113]. Hay un margen considerable para que los Estados inviertan en mejores asociaciones con la sociedad civil, la industria, el mundo académico y los niños para buscar con ellos soluciones que sirvan de prototipo.

III. Conclusiones

126. **La promoción de la privacidad de los niños y el fomento de su autonomía requiere:**

a) Aprobar políticas, legislación y normativas que:

i) Consideren a los niños como titulares de derechos humanos, con un derecho inalienable a la intimidad, la autonomía y la igualdad[114];

ii) Incorporen el alcance general de la privacidad, y no sólo en relación con la protección de datos, para permitir el pleno desarrollo del potencial de los niños[115];

iii) Incorporen en las políticas públicas las opiniones de los niños, las estrategias de estos respecto de la privacidad, las conclusiones de investigaciones centradas en los niños y/o las evaluaciones del impacto en la privacidad de los niños[116];

iv) Proporcionen medios independientes para conciliar, arbitrar y reparar en el caso de vulneraciones individuales o sistémicas de los derechos humanos de los niños[117]; y aseguren la adopción de medidas coercitivas en caso de infracción[118];

[108] Documentos de Campaign for Commercial-Free Childhood y Center for Digital Democracy; CNIL.
[109] Documento de ACT/The App Association.
[110] Jane Bailey y Valerie Steeves, *eGirls, eCitizens: Putting Technology, Theory and Policy into Dialogue with Girls' and Young Women's Voices* (University of Ottawa Press, 2015); Jane Bailey y Jacquelyn Burkell, "Legal remedies for online attacks: young people's perspectives", *The Annual Review of Interdisciplinary Justice Research*, vol. 9 (2020).
[111] Documentos de la Federación Internacional de Asociaciones de Bibliotecarios y Bibliotecas, pág. 2. Office of the Victorian Information Commissioner,(Australia); Future of Privacy Forum; Consejo de Europa; Comisión de Derechos Humanos de Australia; y Crock y otros, pág. 5.
[112] Documento del Comisionado de Información y Protección de Datos de Albania. InternetLab y Alana.
[113] Resolución 75/166 de la Asamblea General.
[114] Bailey y Steeves, *eGirls, eCitizens*.
[115] Documentos de South Australia Commissioner for Children and Young People. International Child Rights Center y MINBYUN;Organismo Nacional de Protección de Datos y Libertad de la Información de Hungría, pág. 58.
[116] Documentos de South Australia Commissioner for Children and Young People; Bailey y Steeves; *eGirls, eCitizens*.
[117] Documento de Canadian Human Rights Commission.
[118] Documento de 5Rights Foundation.

b) Abordar las dinámicas estructurales que hacen que los niños sean vulnerables y no tengan capacidad de decisión;

c) Fomentar las innovaciones tecnológicas para mejorar los servicios de comunicación de la información, protegiendo al mismo tiempo la privacidad de los niños[119]**.**

IV. Recomendaciones

127. **El Relator Especial recomienda a los Estados:**

a) Velar por que los derechos y valores de la Convención sobre los Derechos del Niño relativos a la privacidad, la personalidad y la autonomía sirvan de base a la legislación, las políticas, las decisiones, los sistemas de registro de datos y los servicios del Gobierno;

b) Respaldar el análisis exhaustivo de la capacidad de los niños para tomar decisiones autónomas a la hora de acceder a los servicios en línea y de otro tipo, a fin de contar con legislación, políticas y normativas en materia de privacidad de base empírica específicas para los niños;

c) Aprobar disposiciones adecuadas a la edad únicamente con fines reguladores, y con la mayor precaución, cuando no existan medios mejores;

d) Promover y requerir la aplicación de principios rectores de seguridad incorporada en el diseño, privacidad incorporada en el diseño y privacidad por defecto en el caso de productos y servicios destinados a los niños, y velar por que los niños dispongan de recursos efectivos contra las vulneraciones de la privacidad;

e) Fomentar las asociaciones con la sociedad civil y la industria para crear conjuntamente ofertas tecnológicas que tengan en cuenta el interés superior de los niños y los jóvenes;

f) Adoptar las recomendaciones del Relator Especial para la protección contra las vulneraciones de la intimidad en razón del género (A/HRC/43/52, párrafos 33 y 34);

g) Desarrollar planes de acción integrales sobre la enseñanza en línea tomando como base el artículo 29, párrafo 1, de la Convención sobre los Derechos del Niño y las directrices del Consejo de Europa sobre la protección de datos de los niños en un entorno educativo[120]**;**

h) Velar por que se establezcan y mantengan marcos legales apropiados para la educación en línea;

i) Crear infraestructuras públicas para espacios educativos y sociales no comerciales;

j) Subsanar todas las lagunas legislativas y las excepciones procedimentales a fin de que se repete la privacidad de todos los niños en contacto con los sistemas de justicia durante todas las actuaciones, y prohibir de manera vitalicia la publicación de antecedentes penales de niños;

k) Revisar los marcos legales a fin de que las empresas puedan adoptar voluntariamente medidas para detectar, de manera legal y proporcionada, contenidos relacionados con el abuso sexual infantil en línea;

l) Velar por que los datos personales de los niños asociados a grupos terroristas o extremistas violentos sean confidenciales y se revelen sólo cuando sea estrictamente necesario para coordinar la rehabilitación y la reintegración individual;

[119] Documento de ACT/The App Association.

[120] Véase www.coe.int/en/web/data-protection/-/protect-children-s-personal-data-in-education-setting (en inglés).

m) Llevar a cabo evaluaciones del impacto en los derechos humanos en lo que se refiere a las implicaciones para los niños y su privacidad, y organizar consultas para evaluar la necesidad, proporcionalidad y legalidad de la vigilancia biométrica, antes de vincular bases de datos de identidad civiles y penales;

n) Establecer prácticas y normativas legales para que la información que se facilite a los medios de comunicación no vulnere el derecho a la privacidad de los niños y que, en la información que transmitan dichos medios y otras entidades, se proteja la intimidad de los niños cuyos padres estén en conflicto con la ley;

o) Velar por el respeto de la privacidad de los niños en todos los contactos con padres encarcelados, incluidas las comunicaciones escritas, electrónicas y telefónicas y las visitas a prisión;

p) Velar por que no se recopilen datos biométricos de los niños, salvo como medida excepcional, y únicamente cuando sea legal, necesario, proporcionado, y respetando plenamente los derechos del niño;

q) Velar por que los datos personales de los niños se traten de forma justa, precisa y segura, con una finalidad específica y de acuerdo con una base jurídica legítima, utilizando marcos de protección de datos que representen las mejores prácticas, como el Reglamento General de Protección de Datos y el Convenio 108+;

r) Velar por que quienes tratan los datos personales, incluidos los padres o cuidadores y los educadores, sean conscientes del derecho de los niños a la privacidad y a la protección de los datos;

s) Velar por que los niños tengan acceso a información sobre el ejercicio de sus derechos, por ejemplo, en los sitios web de las autoridades encargadas de la protección de datos, y que haya a su disposición asesoramiento, mecanismos de reclamación y medidas de reparación que sean específicos para los niños, también en caso de ciberacoso;

t) Velar por que el anonimato, el empleo de seudónimos o el uso de tecnologías de encriptación por parte de los niños no estén prohibidos en la legislación ni en la práctica;

u) Velar por que los niños y jóvenes de todos los orígenes tengan la oportunidad de participar en la toma de decisiones y en el diseño de los marcos, políticas y programas dirigidos a ellos;

v) Prohibir el tratamiento automatizado de los datos personales que elaboran perfiles de niños para la toma de decisiones que les conciernen o para analizar o predecir las preferencias personales, el comportamiento y las actitudes, salvo en circunstancias excepcionales en razón del interés superior del niño o de un interés público superior y con las garantías legales adecuadas;

w) Velar por que los derechos y valores de la Convención sobre los Derechos del Niño relativos a la privacidad, la personalidad y la autonomía sustenten las políticas, las decisiones administrativas y los servicios de las empresas;

x) Aplicar los Principios Rectores sobre las Empresas y los Derechos Humanos: "Marco de las Naciones Unidas para Proteger, Respetar y Remediar" y las directrices de género para esos Principios (A/HRC/41/43, anexo)[121];

y) Establecer mecanismos de reclamación y reparación, asegurándose de que con ellos no se impida el acceso a los mecanismos estatales;

z) Proporcionar información comprensible sobre la comunicación de cuestiones objeto de preocupación, incluida la presentación de denuncias, y sobre los mecanismos de reclamación y reparación;

[121] Véase también www.ohchr.org/Documents/Issues/Business/Gender_Booklet_Final.pdf. (en inglés).

aa) Adoptar medidas razonables, proporcionadas, oportunas y efectivas para que sus redes y servicios en línea no se utilicen indebidamente con fines delictivos u otros fines ilícitos que sean perjudiciales para los niños;

bb) Trabajar con las autoridades de orden público para apoyar la identificación legal y el enjuiciamiento de los autores de delitos contra niños.

Labor futura

128. **Entre las prioridades inmediatas para la labor futura sobre la privacidad y los niños cabe señalar:**

a) La puesta en marcha de iniciativas internacionales con objeto de desarrollar marcos para proporcionar orientación sobre el diseño con miras a proteger la privacidad de los niños en las actividades en línea;

b) La participación de los niños, durante las visitas a los países y en los informes temáticos, respecto de sus preocupaciones en materia de privacidad;

c) La realización de investigaciones sobre las normas de vigilancia parental y sus efectos en el desarrollo de los niños.

Annex I

Overview of activities

The key achievements of the mandate since 2015 include:

A. Detailed thematic reports and recommendations on:

Big data and open data, A/72/540 (2017) and A/73/438 (2018)

Health-related data, A/74/277 (2019)

Privacy and gender, A/HRC/40/63 (2019)

Artificial intelligence and privacy, and children's privacy, A/HRC/46/37 (2021)

B. Security and surveillance

The establishment of the International Intelligence Oversight Forum, which met in Bucharest (2016), Brussels (2017), Valletta (2018) and London (2019).

The draft legal instrument on government-led surveillance, while not progressed, has increasingly been demonstrated as needed and a useful reference for future work.

Networks have been established through the use of working parties, consultations and involvement of regional human rights bodies/entities, particularly in Europe.

Discussions with and specific recommendations to intelligence agencies, police forces and/or Governments of Member States concerning reinforcement of safeguards and remedies, including legislation regarding surveillance, encryption and independent oversight authorities.

Intensive work on complaints of infringement of privacy by Julian Assange and President Lenin Moreno, including preparation of interim reports.

The Special Rapporteur presented a report to the Human Rights Council on governmental surveillance activities from a national and international perspective, A/HRC/34/60 (2017).

The Special Rapporteur presented a report to the General Assembly on the implications of the COVID-19 pandemic for the right to privacy, A/75/147 (2020).

Communications to Member States

Since 2015, 101 communications have been issued to Member States concerning practices that appeared inconsistent with the right to privacy. Thirty were issued in 2020 (see annex II).

Visits and events

The COVID-19 pandemic prevented any official country visits during 2020.

Country visits were undertaken in: the United States of America in 2017 (A/HRC/46/37/Add.4); France in 2018 (A/HRC/46/37/Add.2); the United Kingdom of Great Britain and Northern Ireland in 2018 (A/HRC/46/37/Add.1); Germany in 2018 (A/HRC/46/37/Add.3); Argentina in 2019 (A/HRC/46/37/Add.5) and the Republic of Korea in 2019 (A/HRC/46/37/Add.6).

During 2020, the Special Rapporteur continued to promote privacy via online events, including the forty-second International Conference of Data Protection and Privacy Commissioners and multiple civil society organization and non-governmental organization events.

Taskforces

Security and surveillance

The annual International Intelligence Oversight Forum 2020 was postponed due to the COVID-19 pandemic. However, collaborative networks were maintained. The Special Rapporteur continued to work with various countries and their intelligence agencies on the upgrading of laws regulating surveillance and encryption. More detailed laws are needed to protect encryption and thereby, the privacy of communications.

Taskforce on corporations' use of personal data

The Special Rapporteur held five taskforce meetings attended by civil society organizations and leading corporations. The dialogue was highly productive, addressing issues including identity verification, European Court judgments concerning cross border movement of data, artificial intelligence, and privacy and children.

The taskforce's recommendation on artificial intelligence is provided in the main text of the present report. The draft was provided for international consultation, to which 28 submissions were received.

Taskforce on privacy and personality: children

The Special Rapporteur worked independently yet collaboratively with the Committee on the Rights of the Child on new guidelines to protect children's privacy. He also provided feedback to the Committee on its draft general comment No. 25.

The Special Rapporteur released a call for contributions on how privacy affects the development of personality, particularly the evolving capacity of the child and the growth of autonomy. Contributions were sought from interested parties on research, consultations with children and good practice mechanisms. Nearly 60 submissions were received. The principles and recommendations are included in the main body of the present report.

Annex II

Communications on the right to privacy

Communications (joint and from the Special Rapporteur on the right to privacy alone) on the right to privacy sent, and replies received, between 1 June 2015 and 1 January 2021

TIME PERIOD: Sent and Responses Received	*TYPE of COMMUNICATION*						
	Joint Urgent Appeals	*Joint Allegation Letters*	*Joint Other Letters*	*SRP Urgent Appeals*	*SRP Allegation Letters*	*SRP Other Letters*	*Total*[a]
2015–2020 Sent	6	60	19	0	5	11	101
2015–2020 Responses	4[b]	51[c]	10[d]	0	7[d]	5	77[a]
2020 Sent	1	22	5	0	0	2	30
2020 Responses	0	16[e]	4[f]	0	0	2	22[a]

Source: OHCHR communication database, https://spcommreports.ohchr.org/TmSearch/Results.

Abbreviation: SRP, Special Rapporteur on privacy.

[a] The number of replies received is not equal to the number of matters raised, as some replies included more than one response.

[b] Two Joint Urgent Appeals received two responses each.

[c] 44 responses to Joint Allegation Letters included six matters which received two responses, and one matter received a total of three responses, making a total of 51 responses from Member States.

[d] Two replies consisted of two responses.

[e] One reply included three responses.

[f] One reply consisted of two responses.