Comité: Unión Internacional de Telecomunicaciones
Tema: Definir las normas internacionales y orientaciones hacia el futuro sobre el derecho a la privacidad en línea
Directores: Charles Hermann Gomez, Antonio Badilla Olivas, Marit Pauwelyn

Definir las normas internacionales y orientaciones hacia el futuro sobre el derecho a la privacidad en línea

Las TIC por los ODS

La Unión Internacional de Telecomunicaciones es una organización de las Naciones Unidas cuya misión es estandarizar, armonizar y regular el desarrollo de las tecnologías de la información y la comunicación (TIC) en el mundo. Uno de sus objetivos es promover la inclusión y el acceso universal a estas tecnologías. La UIT también está colaborando con otras organizaciones de las Naciones Unidas para aprovechar eficazmente el potencial de las TIC para alcanzar los Objetivos de Desarrollo Sostenible (ODS).

Introducción

Vivimos en un mundo donde todo está en línea. Incluso podríamos decir que vivimos en línea. Todas nuestras conversaciones, investigaciones, ideas, experiencias, opiniones, amigos, fotos, canciones que escuchamos en el autobús, toda la información que nos preocupa es absorbida por este espacio increíblemente complejo que es el Internet. Como este espacio ahora es accesible casi en todo el mundo, el derecho de una persona a la privacidad está en juego en todo momento. Esto afecta la capacidad de ejercer casi todos los demás derechos, en particular la libertad de expresión y la libertad de reunión y asociación. Pero, la privacidad en línea no solo nos concierne individualmente, se trata de cómo nuestro gobierno, otras organizaciones y asociaciones, utilizan nuestra información para su beneficio. De hecho, los gobiernos han fortalecido su capacidad de monitorear los movimientos de los ciudadanos, censurar los discursos, bloquear o filtrar el acceso a la información y rastrear las comunicaciones para controlar nuestra información y opiniones sociales, económicas, sociales y políticas sobre el mundo. Entonces, ¿hasta dónde llegará? ¿Hasta dónde viviremos en un mundo donde pronto no tendremos derecho a ser un simple individuo? ¿Cómo podemos, como Unión Internacional de Telecomunicaciones, evitar que esto vaya demasiado lejos?

Conceptos clave

El derecho a la privacidad, ¿cómo definirlo universalmente?

Sin duda, es importante comenzar desde la base del derecho fundamental a la privacidad que se ha declarado en el Artículo 12 de la Declaración Universal de Derechos Humanos:

"Nadie será sometido a interferencia arbitraria con su privacidad, familia, hogar o correspondencia, ni a ataques contra su honor y reputación".

De todos los derechos humanos, la privacidad es quizás la más difícil de definir y circunscribir. Las definiciones de privacidad varían considerablemente según el contexto y el entorno. En muchos países, el concepto se ha fusionado con la protección de datos, que interpreta la privacidad en términos de gestión de información personal. Más allá de este contexto bastante estricto, la privacidad a menudo se ve como un medio para determinar cuánto puede interferir la sociedad en los asuntos de una persona. A menudo se divide en cuatro categorías:

- Confidencialidad de la información, que implica el establecimiento de normas que rigen la recopilación y el procesamiento de datos personales, como información crediticia y registros médicos;
- La protección de la privacidad, que se refiere a la protección de la persona física contra procedimientos invasivos, como pruebas de drogas y excavaciones cavernosas;
- Confidencialidad de las comunicaciones, que cubre la seguridad y confidencialidad del correo, teléfonos, correos electrónicos y otras formas de comunicación; y
- Privacidad territorial, que se refiere a establecer límites a la intrusión en entornos domésticos y de otro tipo, como lugares de trabajo o espacios públicos.

Casi todos los países del mundo reconocen explícitamente el derecho a la privacidad en sus constituciones. Como mínimo, estas disposiciones incluyen los derechos de inviolabilidad del hogar y la confidencialidad de las comunicaciones. Las constituciones más recientes, como las de Sudáfrica y Hungría, incluyen derechos específicos de acceso y control de la información personal.

En muchos países donde la privacidad no está explícitamente reconocida en la Constitución, como los Estados Unidos, Irlanda e India, los tribunales han encontrado este derecho garantizado por otras disposiciones. En muchos países, se han adoptado acuerdos internacionales que reconocen el derecho a la privacidad, como el Pacto Internacional de Derechos Civiles y Políticos o el Convenio Europeo de Derechos Humanos.

Más específicamente, ¿cuál es el derecho a la privacidad en línea?

La privacidad en Internet, también conocida como privacidad en línea, es un subconjunto de la privacidad de datos y un derecho humano básico. De hecho, se refiere a la privacidad a la que tiene derecho un individuo cuando muestra, almacena o proporciona información sobre sí mismo en Internet. Esto puede incluir tanto la información de identificación personal (PII) como la información de identificación no personal (PII), como su comportamiento en un sitio web. ¡Sin la confidencialidad en Internet, todas las actividades pueden ser reunidas y analizadas por cualquier parte interesada!

¿Qué son los datos personales?

Esta es toda la información relacionada con una persona física identificada o identificable, directamente o no, a través de un identificador o uno o más elementos específicos de su identidad.

Puede ser, por ejemplo, un nombre, un nombre, una dirección de correo electrónico, una ubicación, un número de tarjeta de identificación, una dirección IP, una foto, Un perfil social o cultural.

Finalmente, ¿qué es un estándar internacional?

Durante los debates, será necesario definir estándares internacionales sobre el tema, es decir, resoluciones que ayuden a cada delegación y cuyas soluciones sean accesibles y factibles para todos. Por eso serán internacionales.

Resumen general

Situación actual y problemas

¿Dónde se almacenan los datos personales?

Herramientas en línea

Las herramientas en línea tienen la capacidad de rastrear y almacenar la ubicación, el consumo de información, los patrones de compra, las interacciones sociales e incluso, a través de PDA, el comportamiento y las discusiones domésticas de sus usuarios. Aquí hay algunas herramientas importantes que nos rodean a diario:

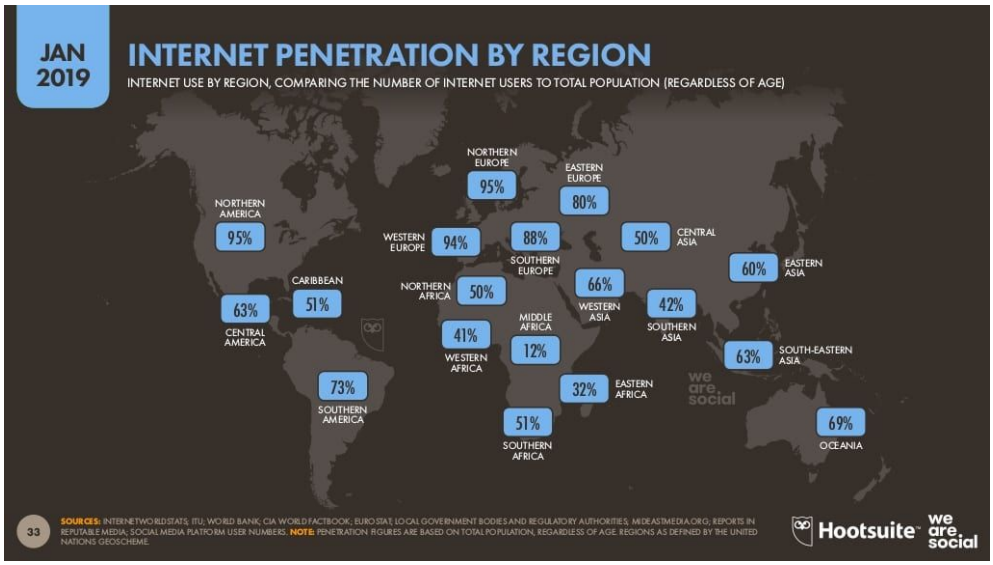
1. Redes sociales (IIP)

El uso ingenuo de las redes sociales puede tener consecuencias emocionales, financieras y legales y, en algunos casos, la divulgación o propagación de datos personales. Los niños y adolescentes ya están en riesgo en las redes sociales, pero los adultos, los gobiernos, los bancos e incluso las grandes empresas web no son inmunes al riesgo.

Las redes sociales son más populares que nunca. De los 3,43 billones de usuarios de Internet del mundo, 2,28 billones de personas (aproximadamente un tercio de la población mundial) visitan regularmente las redes sociales (una tendencia al alza). La Plataforma que tiene el mayor número de clics mensuales, Facebook lidera el paquete y celebra una doble victoria entre los usuarios móviles con su subsidiaria WhatsApp.

El usuario no solo es un consumidor, también es un actor, crea contenido (textos, videos, fotos, ...) a diferencia de Internet tradicional. De hecho, detrás de cada red social, hay personas que tienen acceso a todos sus datos, incluso aquellos llamados "privados". En internet, no puedes controlar nada.

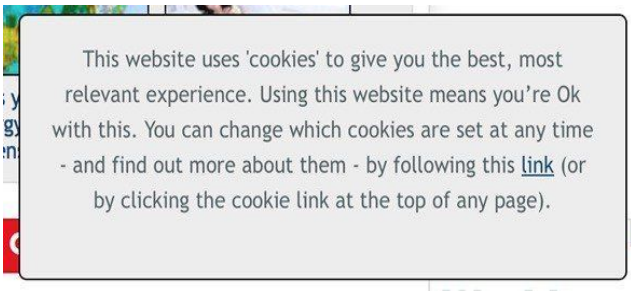
Las redes sociales están llenas de hackers, cibercriminales y vendedores de datos. Cuando miramos este mapa, podemos ver que Internet está presente en todo el mundo, en algunos países más que en otros. También significa que las redes sociales juegan un papel importante en todo el mundo, poniendo a más de la mitad de la población mundial en riesgo de invadir la privacidad.



(https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/)

2. El uso de cookies (IINP)

Las cookies, también conocidas como cookies, han estado en Internet por más de 20 años. Permiten retener los datos del usuario durante una conexión, para facilitar la navegación a los usuarios de Internet. Tienen diferentes funciones, en particular en el caso de una actividad de comercio electrónico para almacenar el contenido de un carrito de compras, registrar la configuración de idioma de un sitio web, o en un propósito más comercial, para hacer el Publicidad dirigida. Sin embargo, las cookies siempre han sido más o menos controvertidas porque estos archivos de texto contienen información personal que puede ser explotada por terceros, lo que puede generar un riesgo en términos de seguridad.



Existe una regulación para asegurar la privacidad del usuario, que insiste en el consentimiento del individuo antes del depósito de cookies, la comunicación sobre el propósito de estas cookies y una forma de oponerse a ellas. Además, este consentimiento es válido por un máximo de 13 meses.

(Https://www.termsfeed.com/blog/4-ways-notify-users-cookies/)

Sin embargo, existen muchos peligros y riesgos al aceptar estas cookies. De hecho, facilitan el trabajo de los piratas informáticos, el objetivo es que exploten el contenido y utilicen estos datos personales con fines maliciosos que pueden llegar hasta el establecimiento de ataques cibernéticos. Por ejemplo, la NSA (Agencia de Seguridad Nacional) utiliza estas cookies para monitorear la vida de los usuarios de Internet, como lo revelan los documentos publicados en diciembre de 2013 por Edward Snowden. Según el Washington Post, la técnica utilizada por la NSA y el GCHQ, la agencia de inteligencia británica, es obtener cookies PREF, específicas de Google, para identificar objetivos y controlar su navegación. En nombre de la protección nacional y bajo el pretexto de la "Ley Patriota", este conjunto de leyes que obliga a las empresas

estadounidenses a proporcionar la información deseada, la NSA ha otorgado el derecho de acceso a esta información.

3. Asistentes personales digitales (IINP)

Principalmente presentes en los teléfonos inteligentes, estas herramientas, más conocidas bajo los nombres de Siri, Alexa, Google Assistants o Cortana, a menudo están ocultas en un gabinete y sirven como un asistente doméstico. Gracias a su inteligencia artificial, responden preguntas u órdenes de su propietario después de escuchar la llamada específica que espera la máquina.

(imagen: Her película, que trata sobre una historia de amor entre un hombre y un asistente personal: http://www.allocine.fr/film/fichefilm-206799/dvd-blu-ray/?cproduct=374684)

Cada vez surgen más dudas sobre la intención de estos "asistentes", se han formado muchas teorías que dicen que son muy peligrosas y que pueden hacer algo más que reaccionar a las expectativas de los humanos. En principio, estos dispositivos se activan cuando el usuario pronuncia la palabra clave esperada ("Alexa", "OK Google", etc.). Antes de esta palabra clave, "escuchan", pero en principio no envían ninguna información sobre la red. Después de la palabra clave, las conversaciones se envían a la nube para procesar el pedido. Amazon, Google o Apple aseguran que los datos estén encriptados y que no se escuche nada. Lo que digan las compañías, "detrás de los asistentes de voz, los humanos te escuchan", advierte La Quadrature du Net, que defiende las libertades en el mundo digital. De hecho, los seres humanos ayudan a las máquinas a volverse inteligentes escuchando y verificando las transcripciones de las palabras habladas. ¿Los asistentes personales no son solo ayudantes domésticos sino espías del gobierno? Ha habido muchos incidentes que parecen justificar estas ideas, pero los creadores todavía parecen encontrar una explicación. ¿Esta invención supera los límites de la vida privada del individuo? ¿Quién podría decidir estas regulaciones?

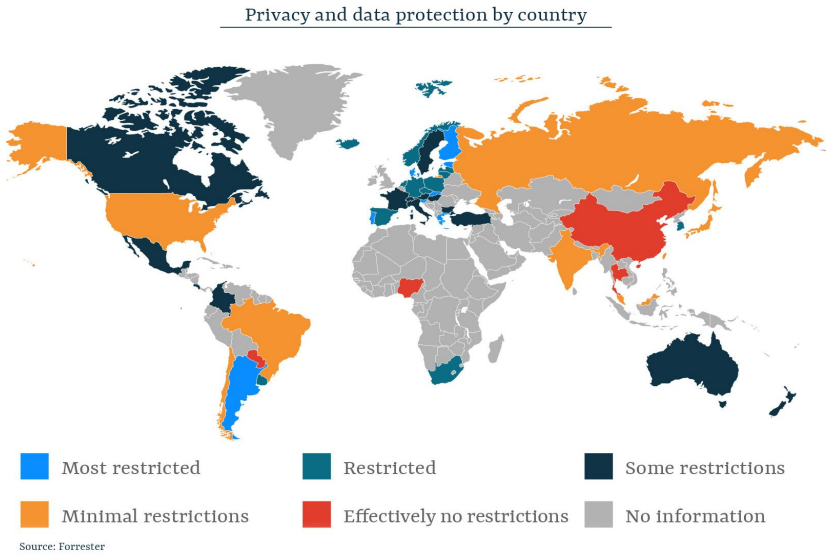
¿Qué leyes existen para limitar el uso de estos datos personales?

Como se indicó anteriormente en el informe, casi todos los países reconocen el derecho a la privacidad y la protegen a través de sus leyes. Pero, ¿qué marco legislativo se ha establecido a nivel internacional?

A nivel mundial, un movimiento general para la adopción de leyes que se basa principalmente en los modelos establecidos por la Organización para la Cooperación y el Desarrollo Económico (https://www.oecd.org/es/) y el Consejo de Europa (https://www.coe.int/en/) está en marcha.

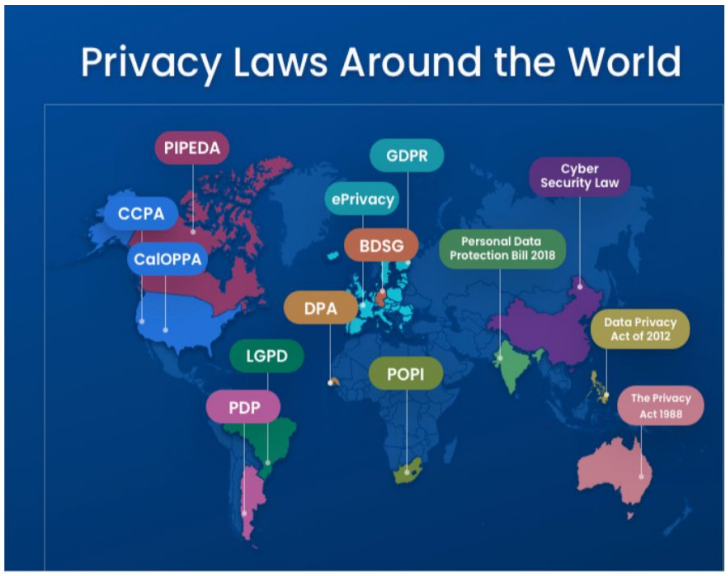
En 1995, consciente de las deficiencias de la ley y de las muchas diferencias en el nivel de protección en cada uno de sus estados, la Unión Europea adoptó una directiva europea que ofrece a los ciudadanos una protección más variada y detallada contra el mal uso de sus derechos. datos.

La Directiva exige a los Estados miembros que garanticen que los datos personales relacionados con los ciudadanos europeos están cubiertos por la ley cuando se exportan o procesan en países fuera de Europa. Este requisito ha llevado a una presión creciente sobre otros gobiernos, lo que lleva a más de cuarenta países a introducir leyes de protección de datos o privacidad de la información. Otros están en proceso de adopción.



¿Por qué adoptar leyes integrales?

- Para remediar las injusticias pasadas. Muchos países, incluidos Europa Central, América del Sur y Sudáfrica, están aprobando leyes para abordar los abusos de privacidad cometidos en regímenes autoritarios anteriores.
- Promover el comercio electrónico. Muchos países, como los de Asia, pero también en Canadá, han desarrollado o están desarrollando legislación para promover el comercio electrónico. Estos países reconocen que los consumidores se sienten incómodos al enviar su información personal a todo el mundo. Las leyes de privacidad son parte de un conjunto de leyes diseñadas para facilitar el comercio electrónico mediante el establecimiento de reglas uniformes.
- Asegúrese de que las leyes sean compatibles con las leyes paneuropeas. La mayoría de los países de Europa Central y Oriental están adoptando nuevas leyes basadas en el Convenio del Consejo de Europa y la Directiva de la UE sobre protección de datos. Algunos esperan unirse a la Unión Europea en el futuro cercano, otros, como Canadá, están adoptando nuevas leyes para garantizar que el comercio no se vea afectado por los requisitos de la directiva de la UE. (Http://gilc.org/privacy/survey/intro.html)



¿Cuáles son los problemas de estas leyes?

- El intenso desarrollo de la tecnología, que introduce más y más máquinas que pueden recopilar, analizar y difundir datos a una velocidad increíble, crea muchas confusiones y lagunas en las leyes de protección, y también crea proporcionalmente más potencial para invasión de la privacidad. Con este crecimiento, la situación urgente solo empeora.
- Los nuevos desarrollos en investigación y atención médica, telecomunicaciones, sistemas avanzados de transporte y transferencias financieras han aumentado significativamente el nivel de información generada por cada individuo.
- La globalización elimina las limitaciones geográficas del flujo de datos. El desarrollo de Internet es quizás el ejemplo más conocido de una tecnología globalizada.
- La convergencia, debido al desarrollo de la tecnología, lleva a la eliminación de las barreras tecnológicas entre los sistemas. Los sistemas de información modernos son cada vez más interoperables con otros sistemas y pueden intercambiar y procesar diferentes formas de datos.
- En algunos países, las agencias y asociaciones han tenido muchas exenciones con respecto a la aplicación de las leyes de confidencialidad.

- Sin supervisión y aplicación, las leyes a veces simplemente se ignoran.

Más de 90 países controlan ilegalmente las conversaciones de opositores políticos, defensores de derechos humanos, periodistas y organizadores sindicales.

En Francia, una comisión gubernamental estimó en 1996 que había más de 100,000 grabaciones telefónicas realizadas por actores privados, a menudo en nombre de organismos públicos.

En Japón, la policía recientemente multó a 2.5 millones de yenes por escuchar ilegalmente a miembros del partido comunista.

Los servicios policiales, incluso en países con fuertes leyes de privacidad como Noruega o Suecia, aún mantienen muchos informaciones de ciudadanos no acusados o incluso sospechosos de delitos.

En los Estados Unidos, a pesar de la existencia de una ley de información de crédito al consumo, las empresas continúan utilizando esta información con fines de marketing.

El impacto de la invasión de la privacidad en la población.

Siempre ha sido difícil definir qué impacto resulta de una violación de la privacidad de un individuo. ¿Cuál es la diferencia entre alguien que ingresa a su hogar sin permiso o el estado que escucha una conversación telefónica personal? Es cada vez más difícil responder a esta pregunta ahora que las iniciativas de recopilación y procesamiento de datos se han desarrollado y ya no se centran solo en individuos específicos, sino en la sociedad en general. ¿Qué hace mal al recopilar datos sobre una población entera o al grabar con cámaras de vigilancia la vida cotidiana de los ciudadanos en la esquina de casi todas las calles? ¿Cómo se pueden tener en cuenta estos daños sin evidencia material o cantidades específicas?

Cuando un individuo está en línea, se vuelve enormemente vulnerable al exponerse a muchos riesgos e incertidumbres: ¿quién podría usar su información, para qué y por cuánto tiempo? Respetar la privacidad significa respetar los estándares de qué información se tiene en cuenta, cómo se usa y con quién se comparte.

En esta era tecnológica, el concepto de daño se vuelve cada vez más problemático. A menudo, un individuo simplemente no es consciente de que sus datos personales son utilizados por ciudadanos (redes sociales), empresas (el uso de cookies) o por el gobierno (vigilancia, por ejemplo, cámaras). Si un individuo va a la corte para defender sus derechos, ¿cómo podría acusar a alguien? ¿Qué daño específico ha hecho la Agencia de Seguridad Nacional (NSA) a un estadounidense o cualquier ciudadano?

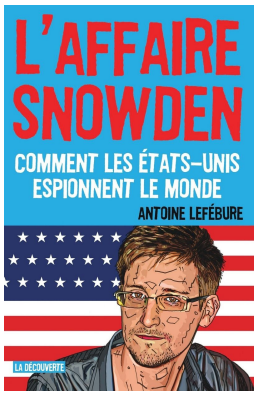
Los tribunales han luchado mucho contra este problema de daños, y se han realizado pocos progresos. Necesitamos desesperadamente una mejor comprensión y enfoque de estas violaciones.

Estos son algunos ejemplos de sus impactos en la población:

- La exposición de sus datos les causó angustia emocional.
- La exposición de sus datos los ha expuesto a un mayor riesgo de daños relacionados con el robo de identidad, fraude u otras lesiones.
- La exposición de sus datos los obligó a gastar tiempo y dinero para evitar futuros fraudes, como registrarse para el monitoreo de crédito, contactar agencias de informes de crédito, colocar fraude en sus cuentas, etc.
- La recopilación o uso de datos sin consentimiento o sin su conocimiento.

Los tribunales a menudo no aceptan estos argumentos porque no hay evidencia válida, o la explicación parece ser demasiado personal y abstracta. Por lo tanto, estos impactos se ignoran por completo en la mayoría de los países.

Estudios de casos



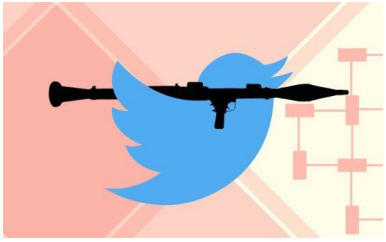
El caso de Snowden

Desde Wikileaks hasta Paradise Papers, la última década ha estado marcada por una proliferación de revelaciones de grandes filtraciones de documentos confidenciales. El asunto de Snowden, que estalló en 2013, se refería a Edward Snowden, analista de seguridad de un subcontratista de la NSA, pero especialmente al mayor pirata informático de su tiempo, que filtró decenas de miles de documentos de la NSA que describen el programa. vigilancia masiva de la agencia estadounidense. Aquí hay algunas revelaciones:

- varios programas de vigilancia masiva, llamadas telefónicas e intercambios en línea establecidos por la NSA.
- La agencia estadounidense se ha permitido espiar a muchos líderes extranjeros. (por ejemplo, los últimos 3 presidentes franceses)
- Se recopilan muchos datos sobre ciudadanos comunes en los Estados Unidos.
- La NSA obviamente está monitoreando con el propósito de combatir el terrorismo, pero también en el espionaje económico e industrial.

Después de estas revelaciones, hubo un shock no solo para los estadounidenses, sino para todo el mundo. Este evento fue en cierto modo un símbolo del comienzo de esta era tecnológica donde todos los datos son supervisados y registrados.

(Http://www.leparisien.fr/international/tout-comprendre-a-l-affaire-snowden-07-11-2017-7378926.php)



La famosa rama "ciber-yihadista"

El uso de Internet con fines terroristas es un fenómeno creciente. Internet se puede utilizar no solo para publicar videos retóricos y extremistas, sino también para establecer relaciones y solicitar apoyo de los más receptivos a la propaganda.

Las organizaciones terroristas utilizan cada vez más la propaganda en plataformas como sitios web protegidos con contraseña o grupos de noticias de acceso restringido para reclutar ilegalmente. El alcance de Internet ofrece a las organizaciones terroristas y sus partidarios un grupo mundial de posibles reclutas. Los ciberforos de acceso restringido brindan a los reclutas un lugar para aprender, apoyar y participar directamente en acciones relacionadas con el terrorismo.

El uso de cerraduras tecnológicas en la entrada a las plataformas de reclutamiento también dificulta que el personal de inteligencia y de aplicación de la ley controle la actividad terrorista. Como ejemplo: Twitter "fue una plataforma de elección para los yihadistas"

Este posicionamiento dio un giro masivo a fines de la década de 2000 con el advenimiento de las redes sociales Facebook, Youtube, Twitter. Hasta ahora, los yihadistas han ocupado principalmente sitios web y foros. En 2014, el grupo Estado Islámico está en su apogeo en las redes. Miles de cuentas transmiten contenido yihadista en masa en muchas plataformas. La toma de conciencia está teniendo lugar con el ataque de Charlie Hebdo en enero de 2015.

https://www.google.fr/amp/s/www.franceculture.fr/amp/numerique/twitter-etait-une-plateforme-de-choix-pour-les-djihadistes

Posibles soluciones

- **Aclarar y validar la adopción de leyes internacionales ya vigentes:** revisar sistemáticamente las políticas gubernamentales sobre comunicaciones digitales y la recopilación de datos personales, y encontrar políticas que violen la privacidad sin una justificación válida;
- **Garantizar que todas las leyes nacionales sobre privacidad en línea respeten los derechos humanos:** garantizar que las leyes y procedimientos nacionales de privacidad sean compatibles con las obligaciones de la Declaración Universal de Derechos Humanos ;
- **Examinar las responsabilidades del sector privado:** siguiendo el marco "Proteger, respetar y reparar" de los Principios Rectores de la ONU, en el contexto específico de las tecnologías digitales de información y comunicación;

- **Fomentar las normas internacionales que tratan la privacidad como un derecho:** ver la conexión entre la privacidad, la libertad de expresión y otros derechos humanos en el contexto digital;
- **Trabajando con expertos de la ONU:** en la protección de la libertad de expresión, libertad de reunión y asociación y defensores de los derechos humanos, para identificar amenazas específicas relacionadas con los derechos en el contexto de vigilancia masiva, para un enfoque más integral para la protección de la privacidad
- **Estimule las plataformas (p. Ej., Facebook, Twitter, Instagram) para que participen de manera más concreta:** en el seguimiento de los informes de sus usuarios, en el posible desarrollo de IA que evite a los piratas informáticos y la piratería antes de la acción, y en su cooperación con el políticas de cibercrimen. Más concretamente, tan pronto como un comentario sea realizado por un usuario, debe analizarse / responderse lo antes posible. Y se pueden establecer compromisos entre el país con sus leyes y la plataforma (ejemplo: una IA que detecta escenas de violencia, para una represión inmediata)

Países y organizaciones involucradas

Argelia: este país no tiene ley sobre datos privados, por lo que puede usarlos libremente, porque no está enmarcada

España: país donde se enmarcan los datos personales gracias al RGPD (Reglamento General sobre protección de datos) así protegido, y deplus no cuenta con herramientas de transferencias

CNIL (Comisión Nacional de Computación y Libertades): Este mapa muy detallado le permite ver los diferentes niveles de protección de datos de los países del mundo: https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

DIGIT (Dirección General de Informática de la Comisión Europea): Esta página detalla las responsabilidades de la comisión a nivel europeo https://ec.europa.eu/info/departments/informatics/mission-statement-informatics_fr

Preguntas orientadoras

- ¿Cómo podemos definir límites universales para la invasión de la privacidad en Internet?
- Qué estándares se pueden establecer que sean aplicables para cualquier gobierno (con uno que depende en gran medida del control en línea y el otro puede no serlo en absoluto)
- ¿Cómo podemos fortalecer las leyes existentes para que no sean ignoradas?
- Sabiendo que las soluciones deben estar "orientadas al futuro", ¿cómo podemos tener en cuenta el desarrollo constante y rápido de la tecnología en nuestros debates y resoluciones? ¿Qué deberíamos enfatizar o aclarar para que no haya brechas?

- ¿Cómo podemos explicar los riesgos de las redes sociales que son tanto personales como éticas y políticas? ¿Cómo podemos reducirlos?

Bibliografía

https://www.hrw.org/news/2015/03/26/un-major-step-internet-privacy
https://www.un.org/fr/universal-declaration-human-rights/
http://gilc.org/privacy/survey/intro.html
https://www.francetvinfo.fr/internet/amazon/faut-il-se-mefier-des-assistants-vocaux-trois-exemples-d-espionnage-qui-incitent-a-la-prudence_2771149.html
https://www.jipitec.eu/issues/jipitec-8-4-2017/4641/
https://teachprivacy.com/privacy-data-security-violations-whats-harm/
Service public pro
https://www.service-public.fr/professionnels-entreprises/vosdroits/F24270

Le petit juriste
https://www.lepetitjuriste.fr/la-protection-des-donnees-personnelles-sur-internet/

https://www.contrepoints.org/2019/07/22/349557-internet-il-faut-proteger-votre-vie-privee

https://www.google.fr/amp/s/sawisms.blog/2016/10/09/dangers-reseaux-sociaux-vie-privee/amp/

https://www.cnil.fr/fr/proteger-sa-vie-privee-en-6-etapes

https://www.fnac.com/5-conseils-pour-proteger-sa-vie-privee-sur-le-net/cp38684/w-4

Europea.Eu
https://www.google.fr/amp/s/europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/indexamp_fr.htm

Peut-on vraiment se protéger ?
https://www.legavox.fr/blog/alexandre-chombeau/atteinte-privee-internet-peut-vraiment-21846.htm

Utilisation de l'Internet UNODC :
https://www.unodc.org/documents/congress/background-information/Terrorism/Use_of_the_Internet_for_Terrorist_Purposes_French.pdf