



MITIGACIÓN ROBO DATOS MEDIANTE COMPLIANCE Y POLÍTICAS CORPORATIVAS

ALAPSI

INDICE


- LA NUEVA SOCIEDAD DE LA VIGILANCIA:TUS DATOS
- REGRESO AL FUTURO
- LA NUEVA VIGILANCIA
- DERECHOS DIGITALES

LA NUEVA SOCIEDAD DE LA VIGILANCIA: TUS DATOS





¿CUÁL ES EL ALCANCE DE LA VIGILANCIA DE LA VIDA PRIVADA?



Enorme y mundial. Hoy una empresa puede venderte un «paquete completo de vigilancia» para que espíes lo que quieras de quien quieras. La industria del rastreo de teléfonos inteligentes es aterradora.

El artículo especial del New York Times One Nation, Tracked analizó la epidemia digital del rastreo telefónico en el marco del proyecto Privacy Project, una base de datos de más de 50.000 millones de rastreos de localización enviados a los teléfonos inteligentes de más de 12 millones de estadounidenses mientras se desplazaban por varias grandes ciudades. Cada orden de rastreo muestra la ubicación precisa del usuario, aunque se encuentre en el Pentágono.

Por cierto, rastrear, recopilar y vender esa información es legal.

Y no solo en Estados Unidos, sino también en la mayor parte del mundo. Rastrear a los seres humanos se ha convertido en un negocio lucrativo y es una actividad tanto legal como lícita

REGRESO AL FUTURO






EN NUESTRAS VIDAS DIGITALES SIEMPRE CONECTADAS,

¿CÓMO REGULAMOS, SUPERVISAMOS O LEGISLAMOS EL USO INFALIBLE DE NUESTROS DATOS PERSONALES EN TODO EL MUNDO?

¿EN QUÉ MOMENTO DECIDE UNA PERSONA QUE ESTÁ DE ACUERDO EN QUE UNOS DATOS PUEDAN CIRCULAR Y OTROS SEAN PRIVADOS?



En 1996, Google creó un proyecto llamado Backrub, un motor de búsqueda que se basaba en retroenlaces.

Backrub destacaba por dos funciones clave que allanaron el camino a la búsqueda tal como la conocemos ahora. La primera es que clasificaba las páginas a partir de citación-notación, es decir, cualquier mención a una página web desde otra otorgaba un punto a la página mencionada. En segundo lugar, la «autoridad» o fiabilidad de una página web dependía de cuántas personas hubieran enlazado con ella y en lo fiables que eran las páginas desde donde se enlazaba.

Fue una carrera por procesar y clasificar la información en un mundo de cookies de origen y de terceros que rastreaban cada uno de nuestros movimientos.

El gobierno chino clasifica a la ciudadanía en función de su nivel de confianza gracias a los datos que posee de todas y cada una de sus acciones. Las autoridades chinas puntúan a las personas por cómo cruzan la calle, qué comentarios políticos hacen en las redes sociales, cuál es su comportamiento de compra o desde dónde y a dónde envían sus currículos.

En China, una nueva ley de 2019 obliga ahora a quienes registren una nueva tarjeta SIM a que se sometan a una exploración de reconocimiento facial.


Los gobiernos emplean la Inteligencia Artificial para rastrear y controlar a la ciudadanía, incluso a quienes no tienen acceso a la nube,

Aunque cerca de la mitad de la población mundial no tiene acceso o tiene acceso limitado a Internet, igualmente es objetivo de la vigilancia de la Inteligencia Artificial.



EN NUESTRAS VIDAS DIGITALES SIEMPRE CONECTADAS

«QUIZÁ NO TENGAS ACCESO AL MUNDO CONECTADO,
PERO EL MUNDO CONECTADO TIENE ACCESO A TI».



En Estados Unidos, algunos estudiantes de la Universidad de California protestaron por el uso del reconocimiento facial en el sistema de vigilancia del campus de Los Ángeles.

Fight for the Future, el grupo de estudiantes que lucha por los derechos digitales, coordinó las acciones de protesta en los centros de enseñanza, demostró que el software de reconocimiento facial identificaba erróneamente a los profesores y deportistas de la UCLA, sobre todo cuando eran personas de color.

En agosto de 2019, la autoridad sueca de protección de datos multó al consejo escolar de Skellefteå, un municipio del norte de Suecia, con 200.000 coronas suecas (aproximadamente 20.000 Dólares) por utilizar tecnología de reconocimiento facial para controlar la asistencia de los alumnos al instituto, una infracción del RGPD.

LA NUEVA VIGILANCIA






¿TENEMOS DERECHO A PROTEGER NUESTRA INFORMACIÓN EN LÍNEA?

Y SI PERDEMOS NUESTRA PRIVACIDAD DIGITAL POR LA VIGILANCIA A LOS
CONSUMIDORES,

¿PERDEMOS NUESTRA LIBERTAD?



La vigilancia ha evolucionado en varias direcciones en las últimas tres décadas: de la vigilancia gubernamental y la privada hasta el punto en el que nos encontramos hoy: la vigilancia a los consumidores.

Un triángulo de vigilancia en el que nuestra privacidad es el centro.

En el nuevo orden mundial de nuestras vidas permanentemente digitales, los computadores, los teléfonos inteligentes, las tabletas, la ropa y los aparatos inteligentes establecen patrones de conducta con los que luego comercian.

DERECHOS DIGITALES



DERECHOS DIGITALES



1. Derechos y libertades en el entorno digital
2. Derecho a la identidad en el entorno digital
3. Derecho a la protección de datos
4. Derecho al pseudonimato
5. Derecho de la persona a no ser localizada y perfilada
6. Derecho a la ciberseguridad
7. Derecho a la herencia digital

DERECHOS DIGITALES



8. Derecho a la igualdad y a la no discriminación en el entorno digital
9. Derecho de acceso a Internet
10. Protección de las personas menores de edad en el entorno digital
11. Accesibilidad universal en el entorno digital
12. Brechas de acceso al entorno digital

DERECHOS DIGITALES

3. DERECHOS DE PARTICIPACIÓN Y DE CONFORMACIÓN DEL ESPACIO PÚBLICO



13. Derecho a la neutralidad de Internet
14. Libertad de expresión y libertad de información
15. Derecho a recibir libremente información veraz
16. Derecho a la participación ciudadana por medios digitales
17. Derecho a la educación digital
18. Derechos digitales de la ciudadanía en sus relaciones con las Administraciones Públicas

DERECHOS DIGITALES

4.

DERECHOS
DEL ENTORNO
LABORAL Y
EMPRESARIAL



19. Derechos en el ámbito laboral

20. La empresa en el entorno digital

DERECHOS DIGITALES

5. DERECHOS DIGITALES EN ENTORNOS ESPECÍFICOS



21. Derecho de acceso a datos con fines de archivo en interés público, fines de investigación científica o histórica, fines estadísticos, y fines de innovación y desarrollo
22. Derecho a un desarrollo tecnológico y un entorno digital sostenible
23. Derecho a la protección de la salud en el entorno digital
24. Libertad de creación y derecho de acceso a la cultura en el entorno digital
25. Derechos ante la inteligencia artificial
26. Derechos digitales en el empleo de las neurotecnologías

DERECHOS DIGITALES

6. GARANTÍAS Y EFICACIA



27. Garantía de los derechos en los entornos digitales

28. Eficacia



GRACIAS

ALAPSI