SATELITES Y PROTECCION DE DATOS

El Documentalista Enredado
“Los crímenes de los siete pecados capitales y una biblioteca”

- *“Somerset confirma a Mills que el FBI dispone de un registro de libros prohibidos que prestados aleatoriamente no suelen aportar mayores problemas, pero que si se empiezan a solicitar libros muy próximos entre sí, en forma de patrón, los agentes federales acabarán investigando a esa persona. Mills se muestra completamente escéptico, sin embargo Somerset, mediante un contacto en la organización, compra una lista de usuarios de bibliotecas que han tomado prestados alguno de los libros que el detective señala mediante un listado. Por supuesto que esta vez sí, analizando la lista de usuarios, encuentran al asesino y llegan hasta la puerta de su casa”.*

SEVEN

TIEMPOS DIFICILES PARA LA PROTECCION DE DATOS
LAS REDES SOCIALES Y EL CABALLO DE TROYA

- ***WIRED:***

- "Empresas como Google, X y Meta recopilan enormes cantidades de datos de los usuarios, en parte para comprender mejor y optimizar sus plataformas, pero sobre todo para vender publicidad dirigida. Aunque la recopilación de información sensible sobre el origen étnico, la sexualidad u otros identificadores de los usuarios supone un riesgo para las personas. Por ejemplo, a principios de este año, Meta y el Departamento de Justicia de EE UU llegaron a un acuerdo después de que se descubriera que el algoritmo de la compañía permitía a los anunciantes excluir a determinados grupos raciales de ver anuncios sobre temas como vivienda, empleo y servicios financieros. En 2018, se impuso a la empresa una multa de 5,000 millones de dólares, una de las mayores de la historia, después de que una investigación de la Comisión Federal de Comercio de EE UU (FTC, por sus siglas en inglés) hallara múltiples casos en los que la organización no protegía la información de los usuarios, a raíz de una investigación sobre los datos compartidos con la consultora británica Cambridge Analytica. Desde entonces, Meta ha modificado algunas de estas opciones de segmentación publicitaria".

TIEMPOS DIFICILES PARA LA PROTECCION DE DATOS
LAS REDES SOCIALES Y EL CABALLO DE TROYA

- ***WIRED:***

- “Incluso para los usuarios que quieren excluirse voluntariamente de la voraz recopilación de datos , las políticas de privacidad siguen siendo complicadas y vagas, y muchos de ellos no tienen tiempo ni conocimientos jurídicos para analizarlas”.

TIEMPOS DIFICILES PARA LA PROTECCION DE DATOS
LAS REDES SOCIALES Y EL CABALLO DE TROYA

- ***WIRED:***

- Pese a que algunas plataformas aportan un mayor respeto a la privcacidad de sus usuarios (no recopilan información personal sensible ni datos de geolocalización), muchas personas siguen prefiriendo usar las más conocidas como X

LA IMPORTANCIA DE LOS SATÉLITES

- ***Marcin Frackiewicz:***
- ***"La relación entre los satélites y las leyes de privacidad basadas en el espacio"***

"La proliferación de satélites de bajo costo ha hecho que el monitoreo desde el espacio sea más accesible que nunca. Como resultado, los satélites de vigilancia se utilizan cada vez más para una variedad de propósitos"

"Con el avance de la tecnología satelital, los datos se pueden recopilar y monitorear con mayor precisión y velocidad que nunca y en grandes cantidades".

"A medida que la tecnología satelital continúa evolucionando y los datos se vuelven cada vez más valiosos, la necesidad de proteger estos datos contra el acceso no autorizado y el uso indebido es primordial".

PROS Y CONTRAS DE LOS SATÉLITES COMO CAPTADORES DE DATOS

Marcin Frackiewicz: “El impacto de los satélites en los derechos de privacidad personal”

- **VENTAJAS**

- Facilitan el control de movimientos de personas y la labor de los servicios de emergencia en ***operaciones de rescate***
- Suministro de ***imágenes detalladas de la tierra*** (se pueden usar para tomar decisiones informadas. Estos datos se pueden utilizar para ayudar con la navegación y la planificación de rutas, optimizar las prácticas agrícolas y mejorar la planificación urbana)
- Al monitorear las comunicaciones digitales, crear redes de comunicación seguras, rastrear las ubicaciones de los dispositivos y facilitar el almacenamiento de datos, los satélites pueden ***ayudar a garantizar que nuestros datos permanezcan seguros, protegidos y privados.*** Al escanear constantemente las comunicaciones digitales, los satélites pueden detectar cualquier intento de interceptar, manipular o explotar datos. Esto puede ayudar a identificar ataques cibernéticos y acceso no autorizado a datos en tiempo real, lo que permite una respuesta rápida y la prevención de posibles filtraciones de datos.

PROS Y CONTRAS DE LOS SATÉLITES COMO CAPTADORES DE DATOS

Marcin Frackiewicz: “El impacto de los satélites en los derechos de privacidad personal”

- **DESVENTAJAS**

- Gran potencial ***para violar las libertades civiles e invadir la privacidad*** de los individuos, el cual es un derecho fundamental base de otros derechos humanos, ya que forman parte de nuestra vida diaria
- se utilizan a menudo para ***rastrear los movimientos de las personas***, lo que otorga a las agencias gubernamentales y otras entidades privadas como las empresas la capacidad de monitorear el paradero de las personas sin su conocimiento o consentimiento o crear perfiles del comportamiento de las personas pudiendo incluso predecir actividades futuras. Esta tecnología se puede utilizar para espiar a las personas
- se pueden utilizar para ***interceptar comunicaciones***, como llamadas telefónicas, mensajes de texto y correos electrónicos. Esto significa que las conversaciones privadas de un individuo ya no están a salvo de miradas indiscretas.
- pueden recopilar ***datos sobre el hogar de una persona,*** como el diseño de la casa y la ubicación de ventanas y puertas. Este tipo de información se puede utilizar para apuntar a individuos o grupos de diversas maneras, como robos u otras actividades delictivas.

PROGRAMA ITFLOWS

- Sistema de satélites para pronosticar el flujo migratorio para prever la respuesta que deben dar las Administraciones públicas y las ONGs (previsión de ruta de llegada y asistencia en tierra)
- La red de satélites permite geolocalizar personas para interceptar con técnicas invasivas radiofracuencias, comunicaciones, móviles, barcos, etc
- Se trata de redes privadas que venden información a las agencias estatales (caso de la empresa USA Hawkeye360 y la Agencia UE Fontex
- Debate sobre si es un sistema que sirve para salvar vidas o reprimir la inmigración ilegal (Informe del Consejo de Europa)

SOLUCIÓN TÉCNICA AL PROBLEMA

- Diseño de satélites considerando las necesidades de privacidad como ocurre con los drones.
- Así, es necesario implementar una tecnología de mejora de la privacidad, como dispositivos de interferencia basados en satélites. Esto interrumpiría la capacidad de los satélites para recopilar datos y limitaría su capacidad para rastrear a las personas.
- Algunos han sugerido la creación de un organismo de control de vigilancia satelital global, que monitorearía y regularía el uso de satélites para vigilancia.

SOLUCIÓN LEGISLATIVA

- A medida que aumenta el uso de satélites de vigilancia, está claro que deben abordarse las implicaciones legales de dicha tecnología. Es fundamental que los gobiernos de todo el mundo desarrollen ***regulaciones integrales*** para garantizar que el uso de dicha tecnología se regule adecuadamente y que se proteja la privacidad y la seguridad de los ciudadanos. Hasta que tales regulaciones estén en vigor, las implicaciones legales del uso de satélites de vigilancia seguirán siendo en gran parte desconocidas. La industria espacial se encuentra en la cúspide de una revolución satelital, gracias a los avances tecnológicos y la creciente demanda de datos. Pero con cada revolución surge la ***necesidad de regulación***, y el sector espacial no es una excepción.
- El impacto de estas leyes en el desarrollo de satélites es significativo. Con regulaciones de privacidad más estrictas, los fabricantes de satélites ahora deben diseñar sus productos para cumplir con la ley. Este puede ser un ***proceso costoso y lento***, que puede ralentizar el desarrollo y, en última instancia, aumentar el costo de los servicios satelitales. Además, estas leyes también pueden crear un **obstáculo para las nuevas empresas y los empresarios que buscan ingresar al mercado satelital.** El costo de cumplir con los requisitos legales puede ser prohibitivo, lo que dificulta que las pequeñas empresas compitan con jugadores más grandes y establecidos.
- A pesar de estos desafíos, la necesidad de protección de la privacidad es clara. A medida que la tecnología satelital continúa evolucionando y ***los datos se vuelven cada vez más valiosos***, la necesidad de proteger estos datos contra el acceso no autorizado y el uso indebido es primordial.

SOLUCIÓN LEGISLATIVA

- ***El marco legal que rodea el uso de satélites de vigilancia se caracteriza por los siguientes rasgos:***
- - aún se encuentra en sus ***primeras etapas***. La mayoría de los países aún tienen que desarrollar regulaciones integrales sobre el uso de dicha tecnología,
- - las leyes existentes ***varían ampliamente según la jurisdicción***. Unos países permiten el uso sin restricciones de los satélites de vigilancia, mientras que otros han prohibido su uso por completo.
- - La falta de regulación en torno al uso de satélites de vigilancia ha provocado un debate mundial sobre las ***implicaciones éticas*** de dicha tecnología. Los críticos argumentan que el uso de dicha tecnología puede conducir a un estado de vigilancia, donde los ciudadanos son monitoreados constantemente por el gobierno. Otros argumentan que la tecnología se puede utilizar para mejorar la seguridad pública y la seguridad nacional. ***Debate sobre la videovigilancia.***

DERECHO DE LA UNION EUROPEA

- **CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA**

- Artículo 8 Protección de datos de carácter personal 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedarÆ sujeto al control de una autoridad independiente.

DERECHO DE LA UNION EUROPEA

- La Unión Europea ha tomado una postura firme en la protección de la privacidad de los ciudadanos.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos –RGPD-)
- El RGDP exige que las empresas procesen los datos de manera segura y legal.
- Esto incluye cualquier dato recopilado de los satélites, que debe hacerse de acuerdo con los requisitos de RGDP.

DICTAMEN 13/2011
Servicios de geolocalización en los dispositivos móviles inteligentes

- El objetivo del dictamen es aclarar el marco jurídico aplicable a los servicios de geolocalización disponibles en dispositivos móviles inteligentes (o que son generados por éstos) que se pueden conectar a Internet y están equipados con sensores de localización tales como el GPS.

DICTAMEN 13/2011
Servicios de geolocalización en los dispositivos móviles inteligentes

- Los dispositivos móviles inteligentes disponen de una serie de microprocesadores con receptores de GPS que determinan su ubicación.
- La tecnología GPS (sistema de posicionamiento global por satélite, GPS en sus siglas inglesas) utiliza 31 satélites que giran en 6 órbitas diferentes alrededor de la Tierra; cada satélite transmite una señal radioeléctrica muy precisa.
- El dispositivo móvil puede determinar su ubicación cuando la antena del GPS recibe las señales. La tecnología GPS ofrece un posicionamiento exacto, de entre 4 y 15 metros,
- Con la ayuda de tecnologías de geolocalización como las estaciones de bases de datos, el GPS y el cartografiado de puntos de acceso WiFi, los dispositivos móviles inteligentes pueden ser seguidos por todos los tipos de responsables del tratamiento de datos, para fines que van desde la publicidad orientada por los comportamientos al control de los hijos.

DICTAMEN 13/2011
Servicios de geolocalización en los dispositivos móviles inteligentes

- **Datos que pueden obtener a partir de nuestro móvil (gráfica social):**

- mensajes electrónicos
- fotografías privadas,
- historial de navegación por Internet
- una lista de contactos (redes sociales).
- Localización (a partir de un período de inactividad nocturna puede deducirse el lugar donde duerme la persona y a partir de una pauta de desplazamientos regulares por la mañana, la localización de su empresa) Riesgo de robo en domicilio, acoso, etc
- pautas de movimientos de amigos
- Visitas a determinados lugares que permiten conocer mis pensamientos, opiniones, hábitos, etc

- Esto permite a los proveedores de servicios de geolocalización disponer de una panorámica detallada de los hábitos y pautas de comportamiento del propietario de estos dispositivos y establecer unos perfiles exhaustivos. Puesto que los teléfonos inteligentes y las tabletas digitales están inextricablemente vinculados a su propietario, las pautas de desplazamiento de los dispositivos ofrecen una visión muy precisa de la vida privada de los propietarios. Uno de los grandes riesgos es que los propietarios no se percaten de que están transmitiendo su localización y a quién.

DICTAMEN 13/2011
Servicios de geolocalización en los dispositivos móviles inteligentes

- **EL CONSENTIMIENTO**

- Un riesgo vinculado es que el consentimiento para determinadas aplicaciones que utilicen sus datos de localización no sea válido, ya que la información sobre los elementos clave del procesamiento es incomprensible, anticuada o insuficiente por cualquier otro motivo.
- Debido a que los datos de localización de los dispositivos móviles inteligentes revelan detalles íntimos sobre la vida privada de su propietario, el principal interés legítimo aplicable es el consentimiento fundamentado previo.
- El consentimiento no puede obtenerse a través de condiciones generales.
- El consentimiento debe ser específico para los diferentes fines para los que se procesen los datos, por ejemplo para elaborar perfiles y orientaciones de comportamiento. Si la finalidad del tratamiento de los datos cambia de forma sustancial, el responsable del tratamiento deberá obtener la renovación del consentimiento específico.
- Por defecto, los servicios de localización deben estar desconectados. Un posible mecanismo de exclusión voluntaria no constituye un mecanismo adecuado para obtener el consentimiento del usuario informado.
- • El Grupo de trabajo recomienda limitar el período de validez de la autorización y recordar su existencia a los usuarios al menos una vez al año. Recomienda igualmente una claridad suficiente en el consentimiento con respecto a la precisión de los datos de localización.
- • Los interesados deberán poder retirar su consentimiento de forma muy fácil, sin consecuencias negativas para el uso de su producto.

DICTAMEN 13/2011
Servicios de geolocalización en los dispositivos móviles inteligentes

- Un ámbito conflictivo se presenta cuando otorgar ***el consentimiento es una condición para el empleo. En teoría, el trabajador puede denegar su consentimiento,*** pero la consecuencia podría ser la pérdida de una oportunidad de empleo. En tales circunstancias el consentimiento no se otorga libremente y por tanto no es válido. En vez de solicitar el consentimiento, los empresarios deben investigar si es una necesidad demostrable controlar la localización exacta de los empleados con un fin legítimo y sopesar dicha necesidad con los derechos y libertades fundamentales de los trabajadores. En los casos en que la necesidad pueda justificarse adecuadamente, la base jurídica podría ser el interés legítimo del responsable del tratamiento (artículo 7.f) de la Directiva sobre protección de datos). ***El empresario debe siempre buscar los medios menos intrusivos, evitar un seguimiento continuo y, por ejemplo, elegir un sistema que envíe una alerta cuando un empleado cruce una frontera virtual preestablecida. El empleado deberá poder desactivar cualquier dispositivo de vigilancia fuera de las horas de trabajo y deberá instruírsele sobre cómo hacerlo***. Los dispositivos de seguimiento de vehículos no son dispositivos para la localización de empleados ya que su función es hacer un seguimiento o vigilar la ubicación de los vehículos en que estén instalados. Los empresarios no deben considerarlos como dispositivos para seguir o supervisar el comportamiento o el paradero de los conductores o de otro tipo de personal, por ejemplo, mediante el envío de alertas relacionadas con la velocidad del vehículo.

DICTAMEN 13/2011
Servicios de geolocalización en los dispositivos móviles inteligentes

- En algunos casos, el ***consentimiento del niño*** debe ser dado por sus padres orepresentantes legales. Esto significa, por ejemplo, que el proveedor de una aplicación de geolocalización debe informar a los padres sobre la obtención y el uso de datos de geolocalización y obtener su consentimiento, antes de recabar y procesar información sobre sus hijos. Algunas aplicaciones de geolocalización están específicamente diseñadas para el control parental, por ejemplo informando continuamente sobre la localización del dispositivo en un sitio Internet o mediante la emisión de una alerta si el dispositivo sale de un territorio predefinido. El uso de este tipo de aplicaciones es problemático. En su Dictamen 2/200913 sobre la protección de los datos personales el Grupo de Trabajo del Artículo 29 afirmó: *«Hay que evitar en todo caso que, por motivos de seguridad, los niños sean sometidos a una vigilancia excesiva que limite su autonomía. En este contexto, hay que alcanzar un equilibrio entre la protección de la intimidad y la vida privada de los niños y su seguridad».*
- El marco jurídico establece que los padres son responsables de que se garantice el derecho de los niños a la intimidad. Como mínimo, si los padres consideran que la utilización de dicha aplicación está justificada en circunstancias específicas, los niños deberán ser informados y, tan pronto como sea razonablemente posible, deberá permitírseles participar en la decisión de utilizarla.

DICTAMEN 13/2011
Servicios de geolocalización en los dispositivos móviles inteligentes

LA INFORMACIÓN

- La información deberá ser clara, completa, comprensible para un público amplio y no técnico, y accesible de forma permanente y fácil. La validez del consentimiento está vinculada indisolublemente a la calidad de la información sobre el servicio.
- Los terceros, como los navegadores y los sitios de redes sociales, deben desempeñar un papel clave en lo que se refiere a la visibilidad y la calidad de la información sobre el tratamiento de los datos de geolocalización.

DICTAMEN 13/2011
Servicios de geolocalización en los dispositivos móviles inteligentes

• LOS DERECHOS DE LOS INTERESADOS

- Los distintos responsables del tratamiento de información de geolocalización procedente de dispositivos móviles deben permitir a sus clientes acceder a sus datos de localización en un formato legible por personas y permitir la rectificación y el borrado sin recoger datos personales excesivos.
- Los interesados también tendrán derecho de acceso, rectificación y borrado de posibles perfiles basados en estos datos de localización.
- El Grupo de trabajo recomienda la creación de un acceso en línea (seguro).

DICTAMEN 13/2011
Servicios de geolocalización en los dispositivos móviles inteligentes

- **EL PERÍODOS DE RETENCIÓN**

- Los proveedores de aplicaciones o servicios de geolocalización deberán aplicar políticas de retención que garanticen que los datos de geolocalización o los perfiles obtenidos a partir de estos datos, sean suprimidos después de un período justificado.

ESTADOS UNIDOS

- En EE.UU el uso de satélites de vigilancia no está regulado en gran medida.
- La Corte Suprema de los EE. UU. ha dictaminado que las personas no tienen una expectativa razonable de privacidad de las imágenes satelitales, lo que significa que el gobierno puede usar dicha tecnología sin obtener una orden judicial.
- Se promulgó la Ley de Privacidad del Consumidor de California (CCPA) para proteger la privacidad de sus ciudadanos.
- Sentencia del Tribunal de Justicia de la UE M.Schrems y Data Protection Commissioner y Digital Rights Ireland Ltd, de 6 de octubre de 2015, As C-362/14

DERECHO ESPAÑOL

- Ley 14/2010, de 5 de julio, sobre las infraestructuras y los servicios de información geográfica en España.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.
- Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana. **Artículo 22. Uso de videocámaras.** La autoridad gubernativa y, en su caso, las Fuerzas y Cuerpos de Seguridad podrán proceder a la grabación de personas, lugares u objetos mediante cámaras de videovigilancia fijas o móviles legalmente autorizadas, de acuerdo con la legislación vigente en la materia.

DERECHO ESPAÑOL

- **Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.**
- **- Preámbulo:**
- “Por otro lado, la realidad demuestra que los desafíos para la Seguridad Nacional que afectan a la sociedad revisten en ocasiones una elevada complejidad, que desborda las fronteras de categorías tradicionales como la defensa, la seguridad pública, la acción exterior y la inteligencia, así como de otras más recientemente incorporadas a la preocupación por la seguridad, como el medio ambiente, la energía, los transportes, ***el ciberespacio*** y la estabilidad económica”
- **- Artículo 10. Ámbitos de especial interés de la Seguridad Nacional.**
- Se considerarán ámbitos de especial interés de la Seguridad Nacional aquellos que requieren una atención específica por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales. A los efectos de esta ley, serán, ***entre otros, la ciberseguridad,*** la seguridad económica y financiera, ***la seguridad marítima, la seguridad del espacio aéreo y ultraterrestre,*** la seguridad energética, la seguridad sanitaria y la preservación del medio ambiente.

DERECHO ESPAÑOL

- **Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional**

- Artículo 16. Tipos de operaciones. El cumplimiento de las misiones de las Fuerzas Armadas y el desarrollo de su contribución complementaria o subsidiaria de interés público requieren realizar diferentes tipos de operaciones, tanto en territorio nacional como en el exterior, que pueden conducir a acciones de prevención de conflictos o disuasión, de mantenimiento de la paz, actuaciones en situaciones de crisis y, en su caso, de respuesta a la agresión. En particular, las operaciones pueden consistir en: a) La vigilancia de los espacios marítimos, como contribución a la acción del Estado en la mar, la vigilancia del espacio aéreo y el control del espacio aéreo de soberanía nacional y aquellas otras actividades destinadas a garantizar la soberanía e independencia de España, así como a proteger la vida de su población y sus intereses

DERECHO ESPAÑOL

- **Díaz Díaz, Efrén "**Marco jurídico y administrativo de la geoinformación (Importancia jurídica de los datos espaciales y desarrollo de los metadatos)":

"Los esfuerzos técnicos y jurídicos en materia de geoinformación han de converger hacia un equilibrio solvente y coherente que tenga como directriz maestra la salvaguarda de los intereses legalmente tutelados, para su mejor protección y más eficaz ejercicio. Indudablemente, más que una legislación profusa y compleja, resultan necesarios principios jurídicos claros que iluminen un escenario con demasiadas sombras jurídicas y no pocas confusiones técnicas. Sugerimos que un principio esencial puede ser el "principio de confianza", aquel por el que los ciudadanos tengan tanta confianza en los medios on-line como en los sistemas off-line. Así será posible abandonar el estadio de "nativos digitales" (*digital native*), sin normas que articulen y armonicen su convivencia en la "isla digital", para pasar al de "ciudadanos digitales" (*digital citizens*), en el que la civilización creciente establezca la obtención del valor añadido de la geoinformación".

DERECHO INTERNACIONAL

Marcin Frackiewicz:

“La Unión Internacional de Telecomunicaciones (UIT) es una de las organizaciones que Trabaja para garantizar que la tecnología satelital se utilice de manera responsable. La UIT ha establecido un conjunto de normas y prácticas para garantizar que la tecnología satelital se utilice de manera que se respete la privacidad de las personas.

Estos estándares y prácticas incluyen garantizar que los operadores de satélites tengan una política de privacidad que describa sus prácticas, que las personas estén informadas de los datos recopilados de ellos y que los datos recopilados se utilicen únicamente con fines legítimos. Además, la UIT recomienda que los operadores de satélites utilicen el cifrado y otras medidas de seguridad para proteger los datos y garantizar su seguridad.

El uso de la tecnología satelital está creciendo exponencialmente y es importante que los gobiernos, las empresas y las personas comprendan sus derechos y responsabilidades en lo que respecta a la recopilación y el uso de estos datos. Al comprender y seguir las normas y prácticas internacionales, los operadores de satélites pueden asegurarse de que su uso de esta tecnología respete la privacidad de las personas en todo el mundo”.

LA LEGISLACIÓN DE PRIVACIDAD BASADA EN EL ESPACIO

- **Marcin Frackiewicz:**

- “Las leyes nacionales solo se aplican dentro de la jurisdicción de sus respectivos países. Para proteger verdaderamente nuestro derecho a la privacidad en la era digital, se necesita legislación a nivel internacional. Aquí es donde entra en juego la legislación sobre privacidad basada en el espacio.
- La legislación de privacidad basada en el espacio es un tipo de ley internacional que busca proteger la privacidad de las personas y organizaciones que operan en el espacio. Este tipo de legislación crearía un marco de normas y reglamentos para proteger los datos y la información personal de quienes operan en el espacio, independientemente de su nacionalidad o de dónde se encuentren. La legislación también podría brindar orientación sobre cómo manejar las violaciones de datos y otros incidentes relacionados con la privacidad en el espacio.
- Además de proteger la privacidad, la legislación sobre privacidad basada en el espacio también podría ayudar a promover el desarrollo de nuevas tecnologías y aplicaciones en el espacio. Al crear un entorno seguro para los datos y la información personal, se podría alentar y acelerar el desarrollo de tecnologías innovadoras.
- La legislación sobre privacidad basada en el espacio sería un gran paso adelante para proteger nuestro derecho a la privacidad en la era digital. Al crear un marco internacional de reglas y regulaciones, podemos garantizar que nuestros datos e información personal estén seguros y protegidos, sin importar en qué parte del mundo nos encontremos. En el mundo cada vez más conectado de hoy, este tipo de legislación es esencial para proteger nuestro derecho a la privacidad”.