Leyes de control de privacidad de información en internet

Danny Sebastián Díaz Padilla
Facultad de ingeniería en sistemas
Escuela Politécnica Nacional
Andalucía y av. Ladrón de Guevara, 170525, Quito, Ecuador
danny.diaz@epn.edu.ec

***Abstracto*- Este documento presenta la definición de cuatro leyes a las que se puede acudir con el fin de proteger nuestra privacidad en internet junto a estrategias para reducir las causas de la problemática que enmarca a las leyes. Se termina con una conclusión personal de cuál ley se considera más importante en la actualidad y por qué.**

***Palabras Clave*:** SOPA, ECPA, CISPA, CFAA

I. INTRODUCCIÓN

Debido a los delitos informáticos de hoy en día se han creado leyes y reglamentos para mermarlos.

Las leyes a ser analizadas y agrupadas en una misma problemática se describen a continuación:

Stop Online Piracy Act (SOPA) que se encarga de hacer a las compañías responsables de bloquear el acceso a sitios que ofrezcan material con derechos de autor. [1]

En trabajos anteriores encontrados en Association for Computing Machinery (ACM) se analiza si la ley Stop Online Piracy Act (SOPA)' puede realmente ser detenida [2] y en otros se busca optimizar su política [3] por medio de la selección dinámica de almacenamiento caché por medio del 'framework' establecido por el mismo autor. Es de hecho una recomendación para cuando SOPA esté aplicada a nivel mundial de forma rígida.

Electronic Communications Privacy Act (ECPA) esta ley fue promulgada por los Estados Unidos para ofrecer restricciones gubernamentales a las escuchas telefónicas de las llamadas. [4] En otras palabras, es una ley diseñada para evitar el acceso no autorizado del gobierno a las comunicaciones electrónicas privadas.

Cyber Intelligence Sharing and Protection Act (CISPA) se encarga de las amenazas cibernéticas y a pesar de cualquier otra disposición de la ley, una entidad autoprotegida puede con fines de seguridad cibernética: utilizar sistemas de ciberseguridad para identificar y obtener información sobre amenazas cibernéticas para proteger los derechos y la propiedad de dicha entidad autoprotegida y compartir dicha información sobre amenazas cibernéticas con cualquier otra entidad, incluido el gobierno federal. [5]

El objetivo de esta ley es permitir un mayor intercambio de información entre el gobierno y las empresas privadas. CISPA permite a las empresas compartir datos privados de o sobre sus clientes con el gobierno, incluidas las agencias de inteligencia. Solo para amenazas cibernéticas.

Y por último Computer Fraud and Abuse Act (CFAA) prohíbe acceder intencionalmente a una computadora sin autorización o en exceso de autorización. Con severos esquemas de penalización y disposiciones maleables, se convirtió en una herramienta madura para el abuso y el uso contra casi todos los aspectos de la actividad informática. [6]

Las personas vulnerables (analfabetos informáticos) son las que más riesgo tienen de caer en la problemática que buscan proteger estas leyes.

II. DESCRIPCIÓN DE LA PROBLEMÁTICA

Aunque las leyes mencionadas anteriormente son 4, abordan un mismo problema desde diferentes perspectivas: compartición de datos en internet sin protección.

La ley SOPA busca reducir la piratería, de modo que los datos compartidos en internet tengan autorización de distribución, debido a que la piratería daña muchos modelos de negocio y facilita el lucro de terceros que no han realizado el material o que se toman los derechos de autor sin consentimiento.

Esta compartición de datos suele ser masiva en grandes servidores y cuando alguno no está disponible suele ser fácil habilitar otro. Cuando un dato se filtra en la red suele quedarse ahí para siempre debido a las múltiples copias

que los usuarios pueden hacer. La tendencia apunta que una gran mayoría de la gente prefiere piratear que pagar por un servicio [7]
La replicación de información es tan fácil como presionar 2 clics.

Algunos sistemas como 'YouTube' [8], utilizan una red neuronal artificial que busca similitudes entre contenidos para buscar posibles infracciones de copyright, aunque esto no suele ser muy efectivo [8]

En Estados Unidos se suele recolectar información sin el consentimiento de las personas [4], como por ejemplo de llamadas telefónicas. Debido a esto ECPA empieza a regular esta recopilación de información por parte del gobierno. La información se utilizaba mayormente para predecir comportamientos delictivos, sin embargo, esto era hecho sin ningún consentimiento de las personas y, de hecho, desconocían de esta recolección.

El gobierno suele tomarse muchos permisos debido al poder que tienen poniendo como excusa la seguridad nacional. Este propósito es factible de realizarlo siempre y cuando exista un contrato consentido entre ambas partes sobre la información, y además los datos deberían ser anónimos para que no se pueda identificar a ninguna persona.

Se establece una compartición de datos permitidos por medio de CISPA, si y solo si existe una amenaza cibernética y el análisis de la información permitirá proteger a una entidad autoprotegida. Aunque aquí no exista un consenso entre ambas partes puede ser necesario en algunas ocasiones, de otro modo las personas aprovecharían la protección para cometer delitos y evitar ser identificados.

La última ley no trata los datos de forma directa, sin embargo, cuando alguien accede a la computadora de una persona puede recopilar más que datos personales, puede recopilar información de organizaciones y conocidos relacionados a la persona inicial. De modo que CFAA protege a las personas que son 'hackeadas' (entiéndase por intrusión al sistema de una entidad sin el permiso de la entidad).

En CFAA el problema de la compartición de datos puede crecer hasta extorsiones y amenazas graves.

III. METODOLOGÍA

A. Objetivo general y específicos

Objetivo general

Definir acciones que permitan la protección de la compartición de datos en internet con respecto a las leyes ECPA y CFAA definidas en la introducción.

Objetivos específicos

- *Listar herramientas informáticas que ayuden a la protección de comunicaciones con relación a la ley ECPA.*
- *Establecer acciones para personas vulnerables, con el fin de aumentar su seguridad de sus datos en internet en apoyo a la problemática que trata CFAA.*

B. Herramientas de protección para apoyar la solución de los problemas al igual que ECPA

- **VPN**

La creación de una red privada que ni si quiera nuestro proveedor de internet pueda analizar es un excelente método para proteger los datos compartidos de internet. Sin embargo, pueden ser usados de manera equivocada para evitar ser enjuiciados por la ley CISPA; puede utilizarse para encriptar comunicaciones (llamadas) de forma que un gobierno que espíe los datos no pueda entender el contexto

También conocidos como VPN, estos programas enmascaran la dirección IP del computador y nos permite navegar de forma privada en internet, algunas opciones gratuitas recomendadas se listan a continuación:

1. Tunnelbear
2. ProtonVPN
3. Opera VPN
4. NordVPN

- **RadPhone**

Esta aplicación encripta la llamada de forma que, aunque sea interceptada, todos los datos leídos estarán ininteligibles por cualquiera que no conozca las claves secretas generadas se forma segura por la misma aplicación [9].

C. Propuesta de solución, recomendaciones para personas vulnerables para apoyar al problema tratado por CFAA

Las siguientes recomendaciones fueron creadas por la comisión federal del comercio [10].

Son recomendaciones realizadas por expertos que han trabajado sobre todo con sistemas bancarios.

- Indicaciones básicas

Sepa a quién le está dando su información personal o financiera. No dé su información personal por teléfono, por correo, ni en internet, a menos que usted haya iniciado el contacto o sepa con quién está tratando.

Si recibe un email de una compañía que aduce tener una cuenta con usted y le piden información personal, no haga clic sobre ningún enlace electrónico del email. En su lugar, escriba el nombre de la compañía en su navegador de internet, vaya a ese sitio y comuníquese con la compañía a través del servicio al cliente. O llame al número de teléfono del servicio al cliente que aparece listado en su resumen de cuenta. Pregunte si la compañía envió ese email solicitándole la información.
Elimine la información personal de manera segura.

Antes de deshacerse de su computadora, elimine toda la información almacenada en ella. Use un programa de barrido para sobrescribir y limpiar todo el disco duro.

Controle la seguridad de su navegador de internet. Para proteger sus transacciones en internet, use un programa de encriptación que cifre los datos enviados por internet. Cuando en la barra de estatus de su navegador de internet le aparece una pequeña imagen de un "candado" significa que su información estará protegida durante la transmisión. Antes de enviar información personal o financiera en internet, busque el candado.

- No comparta sus contraseñas con nadie

Use contraseñas sólidas para su computadora portátil y para acceder a sus cuentas de crédito, bancarias y demás cuentas. Use su imaginación: piense en alguna frase especial y use la primera letra de cada palabra para crear su contraseña. Substituya algunas palabras o letras por números. Por ejemplo, "Yo quiero ver el Océano Pacífico" podría convertirse en YQV3Re10P.
No comparta demasiada información en los sitios de redes sociales

- Aférrese firmemente a su número de Seguro Social y pregunte antes de dárselo a otra persona.

Pregunte si puede usar otro tipo de identificación. Si alguien le pide su número de Seguro Social o el de sus hijos, pregúntele lo siguiente:

- Por qué lo necesita.
- Cómo lo usará.
- Cómo lo protegerá.
- Qué sucede si no le da su número.

- Instale programas antivirus y anti-espía, y un firewall.

Configure las preferencias de los programas para que las protecciones se actualicen frecuentemente. Proteja su computadora contra intrusiones e infecciones que pueden poner en riesgo los archivos o sus contraseñas instalando los parches de seguridad ofrecidos por su sistema operativo y otros programas.

- Evite los emails phishing

No abra archivos, no haga clic sobre enlaces, ni descargue programas enviados por desconocidos. Al abrir un archivo enviado por un desconocido podría exponer el sistema de su computadora a un virus informático o programa espía que captura sus contraseñas y demás información que ingrese en su teclado.

- Sea prudente con el uso de las conexiones Wi-Fi

Antes de enviar información personal desde su computadora portátil o teléfono inteligente a través de una red inalámbrica disponible al público en un café, biblioteca, aeropuerto, hotel o en algún otro lugar público, verifique si su información estará protegida.

Cuando use un sitio web encriptado, tenga en cuenta que la única información protegida es la que usted envíe y reciba hacia y desde ese sitio. Si usa una red inalámbrica segura, toda la información que envíe a través de esa red estará protegida.

- Cierre el acceso a los datos de su computadora portátil

Solamente guarde información financiera en su computadora cuando sea necesario. No use la opción de conexión automática que almacena su nombre de usuario y contraseña, y desconéctese siempre cuando termine de usarla. De esta manera, si le roban su computadora será más difícil que el ladrón pueda acceder a su información personal.
Lea las políticas de privacidad

Es verdad que pueden ser extensas y complejas, pero el texto de la política de privacidad de cada sitio le informará cómo se mantiene la exactitud, acceso, seguridad y control de la información personal que recolecta; cómo se usa la información, y si provee

información a terceros. Si no encuentra o no entiende la política de privacidad de un sitio web, considere hacer negocios en otra parte.

IV. RESULTADOS ESPERADOS

Los resultados esperados al divulgar esta información son:

Para apoyar **SOPA** se espera que se mejore la selección dinámica de almacenamiento caché según la política específica. Utilizando el 'framework' de [3]

Para apoyar a solucionar el problema de las comunicaciones espiadas por el gobierno al igual que la ley **ECPA**, se espera que con el programa Radphone, se reduzca los casos en donde un tercero intercepta y escucha la llamada que se realiza con otra persona.

Para **CISPA** no se propone en este artículo un método debido a la naturaleza de la ley que es una utilización de datos sin permiso, pero necesaria.

Para apoyar a solucionar el problema de intrusión en los sistemas personales al igual que la ley **CFAA**, se espera que las personas con desconocimiento de la informática usando las recomendaciones del punto III.C puedan evitar ser 'hackeadas' de forma que se reduzcan las intrusiones en sistemas informáticos.

V. CONCLUSIONES

La ley más importante de las mencionadas en la introducción es, a mi parecer, SOPA. Debido a que los creadores de contenido deben poder proteger sus obras y a causa de la facilidad que es 'copiar y pegar' esto se vuelve cada vez más y más difícil de controlar.

REFERENCIAS

A. References

[1]"Factbox: The 'Stop Online Piracy Act' explained", *SBS News*, 2015. [Online]. Available: https://www.sbs.com.au/news/factbox-the-stop-online-piracy-act-explained. [Accessed: 31- Jan- 2020].

[2]P. Samuelson, "Can online piracy be stopped by laws?", *Communications of the ACM*, vol. 55, no. 7, p. 25, 2012. Available: 10.1145/2209249.2209260 [Accessed 31 January 2020].

[3]Y. Wang, J. Shu, G. Zhang, W. Xue and W. Zheng, "SOPA", *ACM Transactions on Storage*, vol. 6, no. 2, pp. 1-18, 2010. Available: 10.1145/1807060.1807064 [Accessed 31 January 2020].

[4]"What is the Electronic Communications Privacy Act?", *Minclaw.com*. [Online]. Available: https://www.minclaw.com/legal-resource-center/what-is-the-electronic-communications-privacy-act/. [Accessed: 31- Jan- 2020].

[5]"The Cyber Intelligence Sharing and Protection Act: CISPA explained", *The Verge*, 2020. [Online]. Available: https://www.theverge.com/2012/4/27/2976718/cyber-intelligence-sharing-and-protection-act-cispa-hr-3523. [Accessed: 31- Jan- 2020].

[6]"NACDL - Computer Fraud and Abuse Act (CFAA)", *NACDL - National Association of Criminal Defense Lawyers*. [Online]. Available: https://www.nacdl.org/Landing/ComputerFraudandAbuseAct. [Accessed: 31- Jan- 2020].

[7]J. Tabares, "Según una encuesta, el 91% de los rusos prefieren piratear que pagar por el contenido en internet", *Social Geek*. [Online]. Available: https://socialgeek.co/tech/91-por-ciento-rusos-prefieren-piratear/. [Accessed: 31- Jan- 2020].

[8]S. Agrawal and A. Sureka, "Copyright Infringement Detection of Music Videos on YouTube by Mining Video and Uploader Meta-data", *Big Data Analytics*, pp. 48-67, 2013. Available: 10.1007/978-3-319-03689-2_4 [Accessed 31 January 2020].

[9]"Aplicaciones con las que encriptar llamadas y mensajes", *Todotech.com*. [Online]. Available: https://www.todotech.com/android/apps/aplicaciones-encripatr-llamadas-mensajes_t92.html. [Accessed: 31- Jan- 2020].

[10]"Cómo proteger su información personal", *Información para consumidores*. [Online]. Available: https://www.consumidor.ftc.gov/articulos/s0272-como-proteger-su-informacion-personal. [Accessed: 31- Jan- 2020].