LA DETECCIÓN AUTOMÁTICA Y PRIVADA DE PORNOGRAFÍA INFANTIL EN INTERNET: *HASHES* Y EL APARENTE CONFLICTO CON LAS NUEVAS LEYES EUROPEAS DE PRIVACIDAD

Carolina Christofoletti[*]
Paula Andrea Ramírez Barbosa[**]
Víctor Gabriel Rodríguez[***]

* Licenciada en Derecho por la Facultad de Derecho de Ribeirão Preto de la USP, especialista en temas relacionados con la pornografía infantil y la ciberdelincuencia. Facultad de Derecho de Ribeirão Preto, Universidad de São Paulo. Correo-e: carolina.christofoletti@alumni.usp.br

** Doctora en Derecho por la Universidad de Salamanca (España), máster y especialista en Derecho Penal. Profesora de la Universidad Externado de Colombia y Universidad Católica de Colombia. Profesora honorífica de la Universidad Autónoma de México. Correo-e: paula.ramirez@uexteernado.edu.co

*** Profesor de Derecho Penal de la Facultad de Derecho de Ribeirão Preto de la USP, miembro del PROLAM / USP y becario de la Fundación Carolina (España). (Facultad de Derecho de Ribeirão Preto, Universidad de São Paulo). Correo-e: victorgabrielr@hotmail.com
Fecha de recepción: 5 de enero de 2021. Fecha de aceptación: 12 de abril de 2021. Para citar el artículo: CAROLINA CHRISTOFOLETTI; PAULA ANDREA RAMÍREZ BARBOSA y VÍCTOR GABRIEL RODRÍGUEZ. "La detección automática y privada de pornografía infantil en internet: *hashes* y el aparente conflicto con las nuevas leyes europeas de privacidad". *Revista Derecho Penal y Criminología*, vol. 42, n.° 112, enero-junio de 2021, Bogotá, Universidad Externado de Colombia, pp. 57-80. DOI: https://doi.org/10.18601/ 01210483.v42n112.02

Resumen: En las disposiciones de confidencialidad y retención de la Directiva Europea de Privacidad Virtual (que entró en vigor en diciembre de 2020), denominada "Una amenaza para los métodos de detección automática de pornografía infantil", se destaca como la Comisión Europea propuso, en septiembre de 2020, una derogación provisional de estas disposiciones. El argumento es la existencia de una colisión necesaria entre las políticas de cumplimiento que practican actualmente plataformas como Facebook e Instagram y las nuevas pautas de privacidad europeas. En el centro de la discusión está la tecnología *hash*, un sistema de escaneo para la identificación de contenido criminal previamente conocido. El propósito de este artículo es demostrar que tal colisión no existe, siempre que se adopten ciertas precauciones fundadas en los principios de razonabilidad y utilidad.

Palabras clave: pornografía infantil, detección automática de contenido delictivo, privacidad, análisis de riesgos.

THE AUTOMATIC AND PRIVATE DETECTION OF CHILD PORNOGRAPHY ON THE INTERNET: HASHES AND THE APPEARING CONFLICT WITH THE NEW EUROPEAN PRIVACY LAWS

Abstract: In the confidentiality and retention provisions of the European Virtual Privacy Directive (which came into force in December 2020) a threat to automatic child pornography detection methods, the European Commission proposed, in September 2020, a repeal provisional of these provisions. The argument is the existence of a necessary collision between the compliance policies currently practiced by platforms such as Facebook and Instagram and the new European privacy guidelines. At the center of the discussion is hashing technology, a scanning system for the identification of previously known criminal content. The purpose of this article is to demonstrate that such a collision does not exist, provided certain precautions based on the principles of reasonableness and utility are taken.

Keywords: child pornography, automatic detection of criminal content, privacy, risk analysis.

INTRODUCCIÓN

El compromiso de los proveedores de servicios de internet de combatir la difusión de materiales de pornografía infantil, asumiendo el peso de convertirse en

"limpiadores" de la red[1], obligó a la creación de verdaderos órganos de investigación privada, básicamente compuestos por un aparato bifurcado: comisiones de evaluadores contratados por las empresas que dependen, a su vez, de grandes laboratorios de inteligencia artificial. Este mecanismo bilateral, en observancia a la legalidad existente, tiene que colaborar con otro polo de inhibición de la práctica punitiva, esto es, las fuerzas policiales públicas como entes con legitimidad formal en la persecución del crimen. Sin embargo, la falta de comprensión de los propios funcionarios públicos y los abogados, sobre el funcionamiento de estos mecanismos privados, su alcance y utilidad, hace que el Estado, en general, aproveche poco su potencial para combatir la delincuencia. Tal deficiencia, en sí misma, justificaría la redacción de un texto, como este; sin embargo, es preciso analizar la forma en que funcionan estos mecanismos de vigilancia privada y sus dificultades de operacionalización ante la ley. Además, existe un problema adicional: las nuevas leyes de privacidad en internet, especialmente la Directiva del Parlamento Europeo sobre el tema, están a punto de prohibir totalmente la búsqueda de nuevos contenidos digitales por parte de los usuarios, lo que dificultaría la efectividad de todos estos mecanismos privados. Esta prohibición absoluta es otra consecuencia de la falta de comprensión de cómo puede funcionar estas formas de control. Demostrar que existen formas de vigilancia del contenido privado que no atentan directamente con la privacidad de los usuarios es, por tanto, un objetivo específico de este texto. Pese a ello, antes de entrar en este tema de la Directiva Europea de Privacidad Virtual, parece relevante destacar que en ningún momento se menciona la imposibilidad de poner en funcionamiento instrumentos para la detección automática de contenidos de pornografía infantil en la red. La controversia solo puede —y, por lo tanto, surge efectivamente— mediante un ejercicio interpretativo en torno a (a) la confidencialidad de las comunicaciones electrónicas y (b) la protección legal contra la retención de datos por parte de los usuarios de internet[2].

---

1 Nomenclatura tomada del documental *The Cleaners* para retratar con precisión el papel de "garantes de la ética de la plataforma" que desempeñan los empleados contratados por los propios proveedores de servicios.

2 Nótese que es precisamente a partir de ahí que surge la necesidad de estabilizar, a través de la vía legislativa, la pregunta: "No debe haber lugar a dudas o ambigüedad en un asunto de tan fundamental importancia para la protección de la niñez. Y sin embargo lo hay". John Carr en Hymas, Charles (2020). ¿La privacidad de los pedófilos es más importante para la Comisión Europea? Expertos legales del Reino Unido, [disponible en https://www.legalexperts-uk.com/blog/posts/paedophiles-privacy-more-important-to-european-commission] (consulta: 12 de noviembre de 2020).

1. LAS TÉCNICAS: *HASHES*, *FLAGGING*, *GROOMING* Y LA ENTRADA EN VIGOR DE LA PROHIBICIÓN DE CONTROL AUTOMÁTICO DE CONTENIDOS EN INTERNET

La inseguridad jurídica sobre los mecanismos de cumplimiento que utilizan las plataformas virtuales[3] es la principal razón por la que se lanzaron grandes coaliciones internacionales dedicadas a la lucha contra la pornografía infantil, como la Internet Watch Foundation (IWF) o Inhope (Asociación Internacional de Líneas Directas de Internet). En el preámbulo de una propuesta de septiembre de 2020 enviada a la Comisión Europea para solicitar la derogación provisional de dos dispositivos (referidos a la retención de datos y la confidencialidad de las comunicaciones) de dicha Directiva de Privacidad Virtual. La elección legal hecha aquí es cuestionable[4]. Al observar los actuales mecanismos instrumentales para la detección de pornografía infantil en la red, no hay razón, al menos según lo que se conoce hoy sobre esta tecnología, para que puedan violar la legislación europea de privacidad. Con respecto a los *hash*, que se explica a continuación, todos los materiales identificados mediante estos, son parte de contenidos previamente identificados como pornografía infantil, por lo que circulan de manera efectiva. En este sentido, la mejor técnica jurídica quizás no sería una derogación provisional, sino una enmienda capaz de regular la forma en que se haría a partir de la identificación de los contenidos de pornografía infantil[5].

En lo que respecta a las plataformas virtuales, con especial énfasis en las redes sociales, es un hecho que el problema que se plantea ante las comisiones reguladoras de internet es mucho más delicado: ¿qué podemos hacer para mejorar los mecanismos de identificación, no de imágenes repetidas, sino de nuevos contenidos

---

3 "The Commission wants its proposal to be finalized by December 21, but some lawmakers dismissed the deadline as artificial, since scanning would not stop overnight without the derogation"; Europe's thermonuclear debate on privacy and child sexual abuse. Politico, disponible en https://www. politico.eu/article/europes-thermonuclear-debate-on-privacy-and-child-sexual-abuse-2 (consulta: 22 de noviembre de 2020).

4 Esta también parece ser la opinión del supervisor europeo de Protección de Datos, para quien "Para satisfacer el requisito de proporcionalidad, la legislación debe establecer reglas claras y precisas que regulen el alcance y la aplicación de las medidas en cuestión e impongan garantías mínimas, para que las personas cuyos datos personales se vean afectados tengan garantías suficientes de que los datos estarán protegidos eficazmente contra el riesgo de abuso"; Dictamen 7/2020 sobre la propuesta de excepciones temporales de la Directiva 2002/58 / CE con el fin de luchar contra el abuso sexual infantil en línea. Supervisor Europeo de Protección de Datos. 10 de noviembre de 2020.

5 El reglamento especial incluso fue propuesto el 24 de julio por la Comisión Europea. Sin embargo, el texto de la propuesta de excepción provisional no menciona esta iniciativa, ni siquiera en lo que respecta a la redacción de esta iniciativa dentro del periodo solicitado de cinco años; Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones Estrategia de la UE para una lucha más eficaz contra el abuso sexual infantil. Comisión Europea. Bruselas, 24.7.2020 COM (2020) 607 final.

de pornografía infantil en las plataformas? Después de todo, estos son los contenidos que importan para una actuación policial eficaz. Estos son precisamente los archivos que escapan a las tecnologías de inteligencia artificial que utilizan la mayoría de plataformas. Estos son los contenidos en los que es más probable que se activen formas de explotación sexual.

Es cierto que en lo que respecta a la pornografía infantil existe una falta de tecnología similar a la que existe con los *groomings*, que se explicará a continuación. Es fundamental, como se argumentará en este artículo, que se desarrolle una tecnología basada en estándares circunstanciales para identificar el contenido "nuevo" de pornografía infantil tan pronto como aparezca. Y es precisamente en relación con el "nuevo" contenido de la pornografía infantil que merece hacerse una advertencia con respecto a las leyes de privacidad, aunque aquí no se prevé la colisión. Después de todo, es posible realizar un mapeo de plataforma activo sin necesidad de una mayor intromisión en la privacidad del usuario. Para eso, basta con que los mecanismos de abanderamiento sean adecuados y eficientes.

Se hace énfasis, aún a modo de introducción, la circunstancia de que existe un problema anterior a los *hashes*, bastante sutil, y que precisamente por eso merece atención: para ser *hash* hay que buscar primero los contenidos ilícitos. La necesidad de que las plataformas virtuales participen activamente en la identificación de nuevos *hashes* es algo que pretende llamar la atención por sus repercusiones y efectos que precisan de atención.

Si bien la técnica legal elegida para la propuesta que estaba pendiente para finales de diciembre de 2020 en la Comisión Europea, quizás no sea la más adecuada[6], al dejar abierta una brecha interpretativa en relación con la detección automática de contenidos de pornografía infantil, el cual es un escenario con igual potencial caótico[7]. A continuación, procedemos a analizar las repercusiones jurídicas según lo propuesto.

---

6 Si se propusiera la detección automática de actividades de pornografía infantil como una adición a la Directiva de Privacidad Virtual, entonces se evitaría el compromiso entre los defensores de la privacidad y los defensores de los niños. Después de todo, "El propósito de las regulaciones es detener el abuso y el uso indebido de datos y la privacidad de las personas, pero las consecuencias que potencialmente perjudican lo que se está haciendo para abordar el abuso sexual infantil en línea". Hymas, Charles. ¿Es la privacidad de los pedófilos más importante para la Comisión Europea? Legal Experts UK, disponible en [https://www.legalexperts-uk.com/b og/posts/pedophiles-privacidad-más-importante-para-la-comisión-europea] (acceso: 12 de noviembre de 2020).

7 "This Directive (E-Privacy Directive) does not contain an explicit legal basis to continue the current voluntary practices"; The EU will continue to protect children from child sexual abuse online. European Commission, 10 de septiembre de 2020, disponible en https://ec.europa.eu/home-affairs/news/20200910_eu-continue-protect-children-from-child-sexual-abuse-_en. (consulta: 22 de noviembre de 2020).

2. LA IMPRESCINDIBILIDAD DE LOS SISTEMAS DE VIGILANCIA DE INTERNET

Con la sobrecarga de contenidos en internet, los proveedores se ven obligados a buscar formas para mantener la legalidad en los contenidos de cuya publicación, en última instancia, son responsables. Luego, desarrollan formas de escaneo digital automatizado. Si bien son mecanismos eficientes, su funcionamiento, si se interpreta desde el punto de vista de las leyes de protección de la privacidad, puede representar un gran riesgo de falla regulatoria. Después de todo, su trabajo no es otro que identificar o, en el caso analizado aquí, recibir instrucciones para identificar contenido potencial de pornografía infantil y combinar datos para encontrar direcciones IP de posibles infractores, mientras se bloquea su contenido. Por mucho que avance la tecnología, no hay otra forma de perseguir el material prohibido: en busca de unas pocas imágenes, la inteligencia artificial y los censores humanos tienen que controlar todo el contenido de la red.

Ante el carácter inestable del marco de las organizaciones criminales que operan en una red, cambiando constantemente tanto sus direcciones IP como su denominación y su método de comunicación, se filtran formas alternativas de control, como la simple definición de un "entorno de riesgo", que son ineficaces, al menos por el momento[8]. Hasta que se cree un medio para hacerlo, es necesario preservar la legalidad del sistema de inteligencia privada más poderoso desarrollado: el sistema *hash*.

Los *hashes* surgen de una tecnología que, similar a una imagen de ADN, permite la detección de la aparición de una imagen (ya precatalogada en una base de datos) en una ubicación virtual cuya administración ha instituido este sistema de alarma. De cada imagen, criminal o no, es posible derivar un *hash*, marcado criptográfico que marca y ubica, en toda la red, solo esa imagen a través de una función matemática.

Dado que se trata de filtrar, entre todos los ADN, los que corresponden a los preinscritos en esa base de datos, es fundamental un filtro general (aunque discriminado) de todo el flujo de contenido. Después de todo, si las autoridades supieran dónde

8 La "evaluación de riesgos" se ha vendido como una gran solución contemporánea, en el sistema GRC (gobernanza, riesgo y cumplimiento). Véase, por ejemplo, que las recomendaciones del GAFI / GAFI, en la lucha contra el blanqueo de capitales, actualizadas en 2020, están encabezadas por la recomendación de "evaluar los riesgos y aplicar un enfoque basado en el riesgo". En sus palabras, "y con base en esa evaluación, los países deben aplicar un enfoque basado en el riesgo (RBA) para garantizar que las medidas para prevenir o mitigar el lavado de dinero y el financiamiento del terrorismo sean acordes con los riesgos identificados". GAFI (2012-2020), Normas internacionales sobre la lucha contra el blanqueo de capitales y la financiación del terrorismo y la proliferación, GAFI, París, Francia, disponible en [www.fatf-gafi.org/recommendations.html] (Consultado: 19 de noviembre de 2020) p. 10.

está el contenido delictivo, los *hash* serían innecesarios. Y es así como la confidencialidad de la información, junto con la prohibición de retención de datos (en el caso de colisiones de *hash*), afecta la búsqueda de pornografía infantil: no hay, por el momento, forma de conciliar una imposición de confidencialidad del flujo de información con vigilancia preventiva sobre la aparición de nuevas imágenes, aún no catalogadas en bases de datos para su cruce[9]. Después de todo, hasta que la Política de Privacidad no resuelva qué hacer con los "nuevos *hashes"*, se producirán y difundirán nuevas imágenes pedófilas casi libremente[10].

Además, dado que los detectives digitales comienzan a actuar aquí como ejecutores del interés público, la operatividad de sus funciones debe estar expresamente garantizada por la ley. En otras palabras, la posibilidad de retención de datos no puede verse amenazada con sanciones en nombre de la protección absoluta de las reglas de privacidad. En resumen, es una divergencia de engranajes, una parte natural de los roles de todos: mientras que la policía digital simplemente quiere limpiar internet, la aplicación estatal debe llegar a los delincuentes, que son individuos. En este sentido, la policía digital debe transformar datos, en nuestro caso, de pornografía infantil, en información que permita la identificación de los individuos que suben tal contenido ilícito, y para eso no hay más alternativas que tocar —solo tocar— la privacidad de todos los internautas. Como posibilidad técnica, la combinación de estos datos almacenados en los *hashes* es la única forma de lograr resultados relevantes en esta transición obligatoria del enfoque investigativo.

3. ¿LOS *HASHES* COMO TÉCNICA DE ESPÍAS?

La existencia de *software* para la detección de contenidos prohibidos no es nueva, pero para nuestros fines indicamos que, desde mediados de 2009, un experto en imágenes del equipo de investigación de Microsoft presenta el embrión de lo que sería el paradigma, en términos de pornografía infantil virtual, para el próximo siglo: el ADN de las imágenes[11].

---

9 La propuesta que existe de un "cifrado de extremo a extremo" de los contenidos privados de internet sería fatal en relación con la posibilidad de controlar el material pedófilo.

10 Hace tiempo que se advierte la necesidad de preservar estos medios. Esto es lo que se advirtió, hace décadas, cuando se descubrió el gran club de pedófilos llamado Wonderland. En 1998, una de las autoridades participantes en las investigaciones llegó a afirmar precisamente la relevancia de lo que se está discutiendo casi dos décadas después: la importancia de resguardar los mecanismos de detección. "Tenemos una relación muy cooperativa con los proveedores de servicios de Internet, pero es tecnológicamente imposible para ellos detener esto"; MARTIN BRIGHT y TRACY MCVEIGH (2001). El guardián. Este club tenía su propio presidente y tesorero. Su negocio era el abuso infantil, disponible en [https://www.theguardian.com/uk/2001/feb/11/tracymcveigh.martinbright] (Consulta: 2 de noviembre de 2020).

11 CHRISTINE ARENA. (2010). Child porn too big for law enforcement? Microsoft steps in. The Christian Science Monitor. 13 de junio de 2010, disponible en [https://www.csmonitor.com/

La "huella digital de las imágenes" (*hashes*) permitiría identificar, sin necesidad de constantes contrapruebas, contenidos previamente considerados ilegales en un contexto en el que el volumen de tráfico ya se ha vuelto, en relación con las redes sociales, desorbitado. Desde entonces, se ha debatido si la implementación de este sistema representaría un espionaje indebido a la red. Con el desarrollo de la técnica a lo largo de los años y el aumento de su capacidad de escaneo virtual, esta problematización se agudizó.

Sin embargo, incluso si el sistema *hash* opera mediante una comparación constante de datos, no puede calificarse exactamente como un mecanismo de vigilancia, al contrario: dado que el proceso está automatizado, la sustracción del elemento humano de los primeros pasos del procedimiento sí lo hace, con lo cual la verificación se realiza únicamente sobre algunos contenidos, conocidos como *red flags*, como "banderas rojas"[12]. A excepción de las denuncias que se originan en los canales de denuncias[13], el contenido que se verifica para su eliminación es, en la mayoría de los casos, el indicado previamente por mecanismos de detección inhumanos (bases *hash*).

En el caso de la vigilancia activa en busca de contenido de pornografía infantil por plataformas (materiales aún no cubiertos), la efectividad de mecanismos análogos de inteligencia artificial (marcación) depende de la búsqueda de contenido en el lugar correcto. De ahí la importancia de que estos estén lo más calibrados posible con la situación real de la red para evitar enfocar los esfuerzos en lugares de bajo riesgo. En otras palabras, basado en una buena acción humana para identificar riesgos, el escaneo digital está justificado porque indica protección contra

---

Business/Case-in-Point/2010/0613/Child-porn-too-big-for-law-enforcement-Microsoft-steps-in.] (Consulta: 10 de octubre de 2020).

12 Después de todo, los algoritmos *hash* no "comprenden", además de la colisión, el contenido escaneado. Además, se ha utilizado algo muy similar a los *hashes* para identificar la infracción de propiedad intelectual (Político, 2020) y para la propia formulación de los denominados antivirus, que también operan identificando contenidos previamente considerados maliciosos. El debate termonuclear europeo sobre la privacidad y el abuso sexual infantil. Político. 22 de noviembre de 2020, disponible en [https://www.politico.eu/article/europes-thermonuclear-debate-on-privacy-and-child-sexual-a buse-2] (Consulta: 22 de noviembre de 2020). Hany Farid. (2020). Reunión de expertos de intergrupos sobre la legislación de la UE sobre la lucha contra el abuso sexual infantil en línea. Missing Children Europe (canal de Youtube). 15 de octubre de 2020, disponible en [https://www.youtube.com/watch?v=adY_uWfs90E&t=24m28s] (Consulta: 2 de noviembre de 2020).

13 En particular, hay un punto a estudiar en cuanto a la efectividad de los mecanismos de cumplimiento de que disponen las empresas privadas. "Los desafíos para el inicio y la coordinación efectivos de las operaciones de ciberdelito han sido la incapacidad de EC3 para recibir pruebas e inteligencia esenciales directamente de la industria privada. La subnotificación de los delitos cibernéticos a las fuerzas del orden, por temor a dañar la marca, ha provocado que la policía no tenga una imagen completa del alcance y las tendencias"; Centro Europeo de Ciberdelincuencia (2014), "First Year Report", La Haya: Europol, p. 15.

un riesgo de infracción grave. El análisis de riesgos, entonces, no es algo nuevo, pero no funciona por sí solo: es el punto de partida para los escaneos digitales.

Así como la denuncia de que se está alojando contenido ilícito, por ejemplo, en una página de Facebook, dará lugar a una verificación y posterior eliminación sin una violación real de la privacidad, la sustitución del denunciante por *software* de inteligencia artificial no debe alterar este paradigma. Además, dado que algunas plataformas digitales condicionan el uso de sus servicios al respeto de una política de cumplimiento penal, una mínima intervención para el control de contenidos es una consecuencia lógica. Después de todo, solo es posible afirmar que existe algo como Facebook o Instagram porque hay un centro de control de publicaciones, a diferencia de lo que ocurre en las plataformas huérfanas en la *deep web*, por ejemplo[14]. En otras palabras, la centralidad del control es más esencial para un servicio de redes sociales que su plataforma de difusión.

Un sistema de control mínimo, que el usuario de los proveedores de internet debe posibilitar para aceptar el servicio, es la llamada "transparencia de extremos" que, lejos de ser vigilante, es la premisa de todos y cada uno de los sistemas de comunicación. Es por eso que las plataformas pueden acceder, por ejemplo, a un texto extraído del mensaje encriptado que Alice envía a Bob, de A a B[15]. Para los administradores de la plataforma, el mensaje estaría a la vista. Incluso la inserción de un sistema de cifrado de extremo a extremo no altera el hecho de que para los administradores de la plataforma los contenidos son visibles, incluso si no pueden ser interceptados durante su transmisión. Dado que no se trata de interceptar comunicaciones, se mantiene la confidencialidad de la comunicación. Es en el momento en que se descarga en la plataforma contenido de pornografía infantil previamente identificado, ya sea en forma de mensaje o publicación, cuando entran en juego los *hashes*[16].

---

14 "For those working in online child protection, some believe the reality is that those companies in control of the infrastructure and platforms of the internet are the only ones who can be effective against CSAM". Inhope. Fighting Crime in the 21st Century–Part 1. Inhope. 12 de novembro de 2020, disponible en [https://www.inhope.org/EN/articles/fighting-crime-in-the-21st-century] (Consulta: 18 de noviembre de 2020).

15 Nombres ficticios habitualmente utilizados en el campo de la teoría criptográfica (A y B).

16 "We don't want this illegal content shared on our products and services. And we want to put the PhotoDNA tool in as many hands as possible to help stop the re-victimization of children that occurs every time a video appears again online." JENNIFER LANGSTON. How PhotoDNA for Video is being used to fight online child exploitation. Microsoft. 12 de septiembre de 2018. Disponible en [https://news.microsoft.com/on-the-issues/2018/09/12/how-photodna-for-video-is-being-used-to-fight-online-child-exploitation/] (Consulta: 18 de noviembre de 2020).

Lo que suele suceder es que el mensaje de Alice a menudo se encapsula para que Bob pueda leerlo, sin ningún tipo de vigilancia[17], en una ubicación externa, no rastreada por los proveedores de contenido[18]. Solo piense en los casos en los que comparte no una imagen de pornografía infantil, sino la dirección de un sitio web (externo a la plataforma) en la que se aloja el contenido, una dirección con acceso restringido. Y este es, finalmente, el paradigma policial del siglo que involucra, por ejemplo, buena parte de la discusión sobre el programa TOR[19], *software* mediante el cual la comunicación entre dos usuarios se puede realizar sin ninguna plataforma de control central. El problema de la criptografía surge, en definitiva, cuando el contenido delictivo pasa a "plena vista".

En todo este complejo, el sistema de creación de huellas digitales, *hashes*, por parte de las propias empresas, se ha vuelto cada vez más imprescindible. Después de todo, si no se puede identificar a los distribuidores de contenido criminal, surge la posibilidad de que al menos sean eliminados si las plataformas incorporan ampliamente la política de *hash*.

4. CONFLICTOS CON LA PRIVACIDAD: LA PERVERSIÓN DE *HASHES*

Si bien se ha desarrollado el mecanismo de *hashes* o filtros de cualquier tipo con el fin de alertar a las propias plataformas sobre los fenómenos delictivos que ocurren en su interior, existe la posibilidad de perversión del mecanismo. Y especialmente en los casos de pornografía infantil, en los que no solo compartir, sino también recibir y acceder a sabiendas a material pedófilo representan comportamientos típicos, la privacidad es de especial interés para los usuarios de internet que efectivamente corren el riesgo de recibir contenido malicioso e inadvertidamente este tipo de contenido en su *feed*.

Quizás esta sea la razón por la que la Ley de Privacidad Europea no excluyó de forma el contenido de protección criminal. Después de todo, si en cualquier

17 Como mención, en relación con la criptografía (principalmente en relación con la cuestión de la protección de claves), hay otro debate sobre el derecho a no presentar pruebas contra uno mismo y las pruebas cifradas. Los *hash* pueden volverse relevantes en casos, por ejemplo, cuando la comunicación está abierta solo en uno de los puntos, es decir, cuando se notifica la colisión de *hash*, aunque (y debido a la criptografía) la materialidad criminal no es accesible.

18 Por ejemplo, mediante el uso de un servicio oculto en Tor que, debidamente gestionado por delincuentes, no muestra interés por filtros de ningún tipo.

19 TOR es un programa de enrutamiento IP que permite, a través de un sistema de laberinto, que no se pueda llegar al equipo que origina el contenido. Al crear este laberinto, TOR permitió la formación de la llamada *deep web*, es decir, aquella cuyo contenido no es alcanzado por los buscadores habituales de internet. Más sobre el tema, véase CHRISTOFOLETTI Y RODRÍGUEZ. *La ciberpornografía infantil y su combate: la ineficacia de los filtros de internet y el informe premiado como alternativa a la persecución penal*. Tirant lo Blanch Colombia, 2021.

momento prevaleciera el objetivo principal de luchar contra la delincuencia, no habría ningún conflicto real con la protección de datos como objetivo. Además, dado que la identificación de estos contenidos y la posterior denuncia a las autoridades se realiza a través de las propias plataformas, es innegable la posibilidad de perseguir objetivos equivocados. Así, preservar la privacidad es algo positivo, porque la existencia de contenidos ilícitos no significa necesariamente que su titular sea un delincuente.

Por otro lado, proteger la privacidad del contenido puede conducir legalmente a la impunidad de los delincuentes reales. Después de todo, si la detección de contenido de pornografía infantil se lleva a cabo en violación de las leyes de protección de la privacidad (por ejemplo, escaneo previo de pantallas)[20], entonces cualquier enjuiciamiento penal basado en dicha evidencia tendrá una ilegalidad en su origen, lo que contaminaría cualquier investigación adicional. No es un dilema fácil de resolver.

5. *COMPLIANCE* DIGITAL Y DEBER DE INFORMAR

Si bien la falta de consentimiento de los delincuentes para que las plataformas observen sus comunicaciones ha sido un punto controvertido, se topa con el hecho de que pueden negar, a través de contratos de prestación de servicios que solo pueden suscribirse con esta cláusula, la prestación de sus servicios a quienes se niegan a cumplir con sus políticas[21]. Sin embargo, desde el momento en que la política de retención y confidencialidad de datos se enfrenta a la ley de privacidad, la cláusula contractual resulta nula[22]. El riesgo legal derivado de la mera inserción

---

20 Un ejemplo, en un análisis anterior sobre la detección de intentos de acceso a sitios web bloqueados. En este caso, la probada ilegalidad del sitio web parece indicar la legalidad de su escaneo. Una posible discusión en este caso sería si la detección de intentos de acceso debe quedar bajo el control de las autoridades públicas o si esto podría ser realizado directamente por agentes privados, discusión que surge precisamente ante la imposibilidad (a menudo común) de la doble conferencia, teniendo en cuenta en vista del gran volumen de material rodante. Jamie Grierson. El guardián. Watchdog revela 8,8 millones de intentos de acceder al abuso infantil en línea en abril. 20 de mayo de 2020, disponible en https://www.theguardian.com/society/2020/may/20/watchdog-starts-88 m-tries- to-access-online abuso infantil en abril (Consulta: 2 de noviembre de 2020).

21 "The European Commission should be seeking to legislate in a way that enables all Members States and tech companies, who it should be remembered operate globally, to monitor their networks to detect abuse, safeguard users from stumbling across illegal content and bring to justice those who do abuse technical networks to abuse children." Michael Tunks. IWF joins coalition of charities raising concerns over the European Commission's E-Privacy Directive. Internet Watch Foundation. 2018, disponible en [https://www.iwf.org.uk/news/iwf-joins-coalition-of-charities-raising-concerns-over-european-c ommissions-e-privacy] (Consulta: 15 de outubre de 2020).

22 Aquí se hace énfasis en la falta de tratamiento legal de los temas de esta categoría, es decir, cuando las demandas (en el caso de la persecución penal) hechas por agentes estatales a agentes privados entran en conflicto con una ley protegida internacionalmente (a nivel europeo, la ley

de una cláusula en esta categoría haría que los proveedores de servicios opten por hacer opcional la adhesión a dicha cláusula[23], lo que implicaría la nulidad de sus efectos: los delincuentes utilizarían las plataformas sin renunciar a la vigilancia[24].

En tiempos de criminalización del acceso intencional a contenidos de pornografía infantil, el problema se profundiza aún más cuando, ante el acceso a materiales pedófilos, las plataformas digitales enfrentan la necesaria calificación de la intención del agente para decidir si el acceso al contenido es criminal o no. Esta es la razón por la que no es una mera derogación provisional, sino una aclaración real sobre los modelos de decisión, en estos casos parece ser la mejor alternativa aquí. Pero el problema va más allá del consentimiento de la vigilancia privada: el problema relacionado con la privacidad está, como hemos dicho, en la obligación de denunciar un posible delito. Después de todo, si la ley penal decide crear un deber de colaboración público-privada en relación con la cibergobernanza, también debe brindar la posibilidad legal para su implementación y, en esto, las leyes de privacidad, tal como están, son un gran obstáculo. Se trata, en general, de otro gran conflicto entre las nuevas obligaciones de control y cumplimiento y las normas que defienden a los ciudadanos de los mecanismos de vigilancia extrema, especialmente los privados[25].

---

a la privacidad de las comunicaciones). En referencia con la relación del sector privado con el derecho internacional de los derechos humanos, la ONU lanzó recientemente el Marco de Presentación de Informes de Principios Rectores centrado en cómo las empresas respetan los derechos humanos en la práctica empresarial. Sin embargo, como señala Korff, el marco aborda cómo los Estados pueden actuar contra las violaciones de las empresas, pero no se ocupa de situaciones en las que los Estados exigen a las empresas que las llevarían a cometer violaciones del derecho internacional de los derechos humanos; D. Korff. Rule of Law on the Internet and in the Wider Digital World, documento temático del Comisionado de Derechos Humanos del Consejo de Europa, 2014, 12, citado en Dirección General de Políticas Internas Política Departamento C: Derechos de los ciudadanos y asuntos constitucionales (2015). Los desafíos de la aplicación de la ley del delito cibernético: ¿realmente estamos poniéndonos al día? Parlamento Europeo, p. 45.

23 "It is ridiculous to imagine that child sex offenders would be willing to give their consent to being monitored. Adopting this regulation would be a huge gaffe for children's rights. I'm sure the drafters did not intend to outlaw, reduce or limit the scope for companies to deploy these tools to identify child sex abuse material. We need to put this right." JOHN CARR. New EU online privacy law likely to endanger the safety of children. ECPAT. 2 de diciembre de 2018, disponible en https://www.ecpat.o rg/news/eu-online-privacy/. (Consulta: 21 de noviembre de 2020).

24 "Essentially this means that unless a paedophile agreed to the tech platform that they were using to exchange images on to scan their communications —which they would be extremely unlikely to agree to, if they are exchanging illegal images—, technology companies would no longer be able to do what the Home Secretary called on them to do in his recent speech about keeping children safe online." MICHAEL TUNKS. IWF joins coalition of charities raising concerns over the European Commission's E-Privacy Directive. Internet Watch Foundation. 5 de octubre de 2018, disponible en [https://www.iwf.org.uk/news/iwf-joins-coalition-of-charities-raising-concerns-over-european-commissions-e-privacy] (Contacto: 21 de noviembre de 2020).

25 Este es precisamente el punto central de la controversia. No se trata solo de identificar el contenido para eliminarlo, sino de denunciarlo a las autoridades policiales. "Las organizaciones benéficas dicen que las nuevas regulaciones de la UE evitarían que las empresas de tecnología

Si la transparencia de los datos de comunicación, por ejemplo, entre dos sujetos, tuviera que ser solicitada por la policía ante las empresas prestadoras del servicio en cuestión con justa causa, esta se puede extraer directamente del seguimiento privado, en las obligaciones de cumplimiento normativo y denuncias derivadas[26]. La lógica de la autorregulación forzada. Entonces, en lugar de dejar que la Policía Nacional mapee las redes para saber dónde está el contenido delictivo, deberían ser las mismas plataformas que los encuentran "a plena vista" e informan a las autoridades, cumpliendo con sus obligaciones éticas y de gobernabilidad.

Si bien el término *confidencialidad* debe ser interpretado dentro de los límites de la garantía de verdadera "administración" por parte de las plataformas, surgirían nuevas discusiones sobre qué circunstancias permiten a los guardianes de esta, ante un flujo de datos casi infinito, seleccionar una cuenta particular para un examen más preciso. Y solo un mapeo hipervigilante de las circunstancias de la aparición del contenido en red es capaz de establecer riesgos de manera precisa sin violar las leyes de privacidad[27]. Como lo afirma la Fundación Internet Watch, el requisito de cumplimiento efectivo que deben realizar las plataformas digitales depende de la legalidad de sus instrumentos esenciales[28]. Pese a lo anterior, un

---

busquen imágenes de abuso infantil en sus plataformas y las denuncien a la policía porque sería una posible violación de la privacidad de los pedófilos"; Charles Hamas.¿La privacidad de los pedófilos es más importante para la Comisión Europea? Expertos legales del Reino Unido. 2020, disponible en [https://www.legalexperts-uk.com/blog/posts/paedophiles-privacy-more-important-to-european-commission] (Consulta: 12 de noviembre de 2020).

26 Suele suceder que la Policía Nacional no tiene suficientes recursos humanos para hacerse cargo del enorme flujo de contenido virtual que se intercambia en las plataformas en línea. Departamento de Justicia de los Estados Unidos, abril de 2016. La estrategia nacional para la prevención e interdicción de la explotación infantil: un informe al congreso. Disponible en [https://www.justice.gov/psc/nacional-estrategia-niña-explotación-prevención- e-interdicción] (Consulta: 10 de noviembre de 2020).

27 Si bien la discusión puede enmarcarse en relación con cualquier tipo de ciberdelito (a través de referencias cruzadas de datos, que en última instancia apuntan a situaciones de riesgo), la mayor parte de la discusión se basa en la vigilancia policial preventiva del terrorismo, específicamente en relación con el seguimiento de la radicalización. La gran pregunta es saber cuál es el grado de riesgo y según qué indicaciones, lo que permite un seguimiento más cercano (incluso con violación autorizada de la privacidad) de un determinado individuo a efectos de seguimiento del terrorismo.

28 La manifestación se realiza en relación con la necesaria legalidad del tratamiento de datos relacionados con la aparición de contenido de pornografía infantil "El tratamiento es necesario para el cumplimiento de una obligación legal de la que es sujeto el responsable del tratamiento; El procesamiento es necesario para proteger los intereses vitales del interesado o de otra persona física; El tratamiento es necesario para el desempeño de una tarea llevada a cabo en interés público o en el ejercicio de una autoridad oficial o conferida al responsable del tratamiento". Michael Tunks. La iwf se une a la coalición de organizaciones benéficas que plantean preocupaciones sobre la Directiva sobre privacidad electrónica de la Comisión Europea. Fundación Internet Watch. 5 de octubre de 2018, disponible en [https: //www.iwf.org.uk/news/iwf-jo inscoalition-of-charities-lifting-concern-over-european -comisiones-e-privacidad] (Consulta: 21 de noviembre de 2020).

mapeo anterior de las circunstancias en las que se pueden utilizar los instrumentos parece constituir, de cara a una ley de privacidad, precisamente el equilibrio que aquí se busca.

6. LA COLISIÓN DE *HASHES* COMO RIESGO Y SU FUTURA PRODUCCIÓN PROBATORIA

Dado que los filtros de pornografía infantil son difíciles de operar principalmente por razones éticas[29], los *hashes* siguen siendo hoy en día el principal mecanismo para detectar contenido de pornografía infantil alojado en la red. La identificación de nuevos materiales, es decir, contenidos que aún no se han descubiertos, sigue siendo el gran desafío de la policía preventiva del siglo.

Después de todo, los hashes aparecen como una solución muy práctica en vista del gran volumen de pornografía infantil que circula en una red, que supera las capacidades materiales y humanas de cualquier Policía Nacional[30]. Además, al poner la tecnología *hash* en manos de plataformas que brindan servicios de internet con alcance transnacional, los mecanismos tradicionales de cooperación criminal internacional encuentran una alternativa más ágil y eficiente: los términos de servicio. Si se da el caso de que se identifique una copia de contenido delictivo (*hash* antiguo) circulando dentro de una plataforma determinada, se eliminará de inmediato. Solo en el tercer trimestre de 2018, Facebook identificó 8,7 millones de imágenes repetidas utilizando esta tecnología[31].

Dado que se trata de imágenes repetidas, la tecnología *hash* también alivia a la Policía Nacional en términos de identificación de víctimas. No obstante, les

---

29 "One of the biggest challenges for using AI to detect CSAM is training it to recognise new and previously unseen CSAM. The machine needs to be exposed to huge quantities of images and videos so that it can identify patterns and characteristics of the material. However, storing and sharing CSAM, even if only to help remove more in the long run, gives rise to all sorts of legal and ethical problems." Inhope. Artificial Intelligence in the fight against Child Sexual Abuse Material–Part 2. Inhope. 19 de noviembre de 2020, disponible en [https://www.inhope.org/EN/articles/artificial-intelligence-in-the-fight-against-child-sexual-abuse-material] (Consulta: 18 de noviembre de 2020).

30 Los *hashes* en última instancia simplifican el análisis de la Policía Nacional que inicialmente debería hacerse en relación a miles de contenidos. Al operacionalizar (a través de inteligencia artificial) el hallazgo de imágenes duplicadas, los recursos policiales pueden dirigirse a actividades de mayor urgencia (como la identificación de víctimas). Este hallazgo es particularmente relevante cuando "el 17% de [la policía] dice que la identificación de las víctimas no está asignada en su organización" y "el 63% dice que tiene demasiado material que revisar para tener tiempo para trabajar en la identificación de las víctimas". Netclean, Once increíbles verdades: The NetClean Report 2015, pp. 39-40.

31 New EU online privacy law likely to endanger the safety of children. ECPAT. 2 de deciembre de 2018. Disponible en [https://www.ecpat.org/news/eu-online-privacy/.] (Consulta: 21 de noviembre de 2020).

advierte de otros dos fenómenos: (a) la posibilidad de formación de un club de pornografía infantil, desde que circularon las imágenes, y (b) la necesaria persecución penal (en los casos en que no se realice la persecución penal de acuerdo con el marco de una negociación) de infracciones reveladas por actores privados. Si, por un lado, las plataformas privadas pretenden, a través de la comunicación con las autoridades locales, evitar (incluso por obligación legal) ser explotados por organizaciones delictivas, por otro lado, estas denuncias terminan congestionando los propios órganos de la Fiscalía. Finalmente, corresponderá a la Policía Local decidir qué casos serán objeto de seguimiento o no.

Es cierto que desde el punto de vista de la "limpieza" de las plataformas, bastaría con la simple eliminación automática del contenido. El problema surge, sin embargo, cuando, en lugar de recurrir al fenómeno de cómo evitar que sus plataformas sean utilizadas para organizar clubes de pornografía infantil (actividades de inteligencia privada), las plataformas se centran en una actividad que es esencialmente policial: transmisión de datos.

Después de todo, si no hubiera material de pornografía infantil en circulación que tuviera que ser denunciado a las autoridades policiales, no se hablaría de retención de datos ni de confidencialidad, ya que la propia plataforma es la administradora del servicio que ofrece. Veremos así que el eje central de la controversia no está en los *hashes*, sino en lo que se hace de ellos.

En el caso de los antiguos *hashes*, se trata de identificar objetos delictivos, ahora alojados en ubicaciones virtuales. La colisión *hash*, utilizada para detectar contenido delictivo ya conocido por las autoridades[32], se basa en la misma suposición que el perro rastreador y el reactivo de la droga[33]. El perro rastreador también va al equipaje con drogas y los reactivos solo indican la presencia del contenido del reactor, sin ningún dato adicional cuando es negativo. El sistema parece ser mucho más confiable que el sistema tradicional de rayos X completo. Transportar esta misma lógica al entorno virtual y establecer un escudo para elementos no identificados como en riesgo no es una tarea difícil.

En aras de la complementariedad entre las excepciones reguladas de protección de datos y la ley penal, es necesario hacer énfasis en un problema que no existe con respecto a los *hashes*, sino con una posible derivación de la retención automática de datos cuando se perfecciona una colisión. El problema aquí se deriva

---

32 Illinois v. Caballes, 125 S. Ct. 834, 838 (2005) quoting United States v. Place, 462 U.S. 696, 707 (1983) citado en R. P. Salgado. Fourth Amendment Search and the Power of the Hash. *Harvard Law Review Forum*, vol. 119, n.° 48 (2005): 38-46, 44

33 United States v. Jacobsen, 466 U.S. 1og, 123 (1984) citado en R. P. Salgado. Fourth Amendment Search and the Power of the Hash. *Harvard Law Review Forum*, vol. 119, n.° 48 (2005): 38-46, 44.

de la ausencia de una legislación uniforme sobre la pornografía infantil. Dado que pueden existir varios conceptos de pornografía infantil vigentes en los lugares donde operan los proveedores de servicios, es necesario que la retención de datos solo se realice cuando el material que ha sido pirateado sea, aunque *a priori*, material ilegal.

Dado que las plataformas *hash* ahora tienen un carácter internacional, por lo tanto, derivado de una calificación realizada por múltiples actores con tecnologías *hash*, una organización de plataformas de acuerdo con la legislación local es muy recomendable en un escenario de menor conflicto. Por tanto, es posible categorizar qué tipos de hashes conducen a la retención de datos cuando se encuentran en una ubicación virtual determinada y cuáles, debido a que no violan la ley penal del país en el que se encuentran, simplemente deben eliminarse.

En este sentido, es necesaria una gran cantidad de síntesis legislativa, teniendo en cuenta el conocido conflicto de leyes que surge en relación con los delitos cometidos a través de internet. Sin embargo, si es el caso que solo para uno de los involucrados la retención es aplicable, entonces debe hacerse con respecto a esto. Habiendo hecho este juicio previo de calificación y aplicabilidad, se puede operar la detección automática.

Sin embargo, dado que es un juicio de calificación realizado por agentes privados, se debe reconocer que existe el riesgo de un error de apreciación. Debido a la dificultad para acceder a su autoría, es posible que muchas imágenes de las bases de datos nunca hayan sido objeto de una investigación en profundidad y mucho menos se hayan convertido en un proceso penal real. La calificación previa de acuerdo con los criterios legales adecuados, como se sugirió anteriormente, garantizaría a las plataformas que cualquier error de calificación podría descartar una supuesta violación de la privacidad. Al fin y al cabo, los medios utilizados para tal fin son proporcionales y adecuados, siendo las mismas plataformas las encargadas de gestionar el riesgo que generan. En estos casos, también se debe prever una exclusión típica para evitar el riesgo legal de un eventual error inevitable de calificación. Todo ello deja intacta la identificación de contenidos que, si bien no son delictivos, siguen violando las políticas comunitarias, que aún pueden ser objeto de simple remoción.

Parece fundamental, en este sentido, que la Policía Nacional e Internacional revise periódicamente las bases *hash* para identificar cuáles de las imágenes *hash* son en realidad materiales ilícitos entre el contingente localizado por agentes privados para el correcto uso del instrumento. Después de todo, la información es de amplio interés, para saber qué imágenes simplemente deben eliminarse y qué imágenes deben notificarse (incluso automáticamente) a las autoridades policiales, lo que implica retención de datos. Sin la retención, cualquier producción

probatoria que pueda ser necesaria en el futuro más allá del periodo de retención legal es imposible.

En los casos de *hashes* antiguos, debido a que el contenido es, *a priori*, criminal, no parece haber aquí ninguna contradicción entre la retención de datos (ahora de interés para la persecución penal) y las disposiciones contenidas en las Leyes de Privacidad, siempre que la calificación "criminal" Se realiza de acuerdo con la legislación penal vigente. En estos casos, argumentar la necesidad de una orden de registro e incautación para filtrar los hashes parece ser incoherente, ya que sería necesario identificar, *ex ante*, cuáles son (y por qué) las ubicaciones virtuales que deben inspeccionarse[34].

Y es precisamente de esta identificación previa de lo que se trata la discusión, orientada principalmente en torno a los mecanismos de detección automática que estuvieron hasta diciembre de 2020 (fecha de entrada en vigor de la Directiva E-Privacidad) en el Parlamento Europeo. Y el meollo del problema sigue siendo, como era de esperar, en los casos en que la causa justa de una investigación oficial provenga de una alarma de un sistema de inteligencia privado.

7. EL FUTURO: DEROGACIÓN Y NUEVOS SISTEMAS DE ESCANEADO SIN ALMACENAMIENTO DE DATOS

Según datos oficiales, casi toda la detección de grandes volúmenes de contenido de pornografía infantil se realiza a través de sistemas de vigilancia privados[35]. Si bien las nuevas políticas de detección de *hashes* son, por su carácter de "inteligencia",

---

34 Sin embargo, la tesis existe. Véase, por ejemplo, United States v. Reddick (2018), en el que se consideró "abusiva" la notificación de la plataforma Microsoft Skydrive sobre la colisión de hash identificada dentro de su plataforma al Centro Nacional para Menores Desaparecidos y Explotados (NCMEC). Por lo tanto, según se informa, la plataforma aquí "invadió una expectativa constitucional de privacidad, excedió el alcance de la búsqueda del valor hash de Microsoft Skydrive y no cayó en ninguna excepción al requisito de la orden judicial"; Estados Unidos v. Reddick 900 F.3d 636 (5th Cir.2018) Decidido: 17 de agosto de 2018.900 F.3d 636 (5th Cir.2018). Tribunal de Apelaciones de los Estados Unidos para el quinto circuito.

35 Según datos oficiales que se reportaron 39,5 millones de contenido de pornografía infantil en el primer periodo de 2020 y otros 35,7 millones en el segundo periodo, de estos 637,5 mil devueltos a la plataforma (informes incorrectos) solo en el caso de Facebook es un número muy aterrador. En el caso de Instagram, el aumento de 8,1 millones de contenidos reportados en el primer periodo de 2020 a 12,4 en el segundo periodo, otra cifra muy significativa, se justifica por la conducta proactiva de la plataforma en la búsqueda y eliminación de imágenes. A pesar de ello, saber si (a) la cantidad de material está aumentando o disminuyendo, (b) si los mecanismos son efectivos o las páginas de acogida son más discretas es una conclusión difícil, por lo que los datos aún parecen insuficientes. Informe de cumplimiento de normas comunitarias. Transparencia de Facebook. Abril de 2020 a junio de 2020, disponible en [https://transparency.facebook.com / community-standar ds -forcement # instagram-adult-nudity-and-sexual-activity] (Consulta: 10 de octubre de 2020).

poco transparentes para el público, se asume que son precisamente las principales amenazas que enfrentan los guardianes de internet con respecto a la vigencia de una Ley de Protección de Datos. Al fin y al cabo, en los propios Memorandos de Propuesta, la Comisión Europea refuerza su compromiso de regular el tema, hasta el segundo semestre de 2021[36].

La única solución, con una solvencia mínima, encontrada hasta ahora, como se dijo, fue derogar la aplicabilidad de las reglas de confidencialidad (art. 5, 1, Directiva Europea sobre Privacidad Electrónica)[37] y la retención de datos (art. 6, Directiva Privacidad Electrónica Europea)[38]. La propuesta del Consejo Europeo exige un

36 "The announced legislation will be intended to replace this Regulation, by putting in place mandatory measures to detect and report child sexual abuse, in order to bring more claarity and certainty to the work of both law enforcement and relevant actors in the private sector to tackle online abuse, while ensuring respect of the fundamental rights of the users, including in particular the right to freedom of expression and opinion, protection of personal data and privacy, and providing for mechanisms to ensure accountability and transparency." Proposal for a Regulation Of The European Parliament And Of The Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by numberindependent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online. Bruxelas, 10 de septiembre de 2020.

37 "Art. 5, (1), Confidentiality of the communications. 1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality"; Directive 2002/58/EC Of The European Parliament And Of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

38 Con especial énfasis en el párrafo (1), sobre el carácter anónimo de los datos, es que puede afectar futuras investigaciones en relación con los datos ya anonimizados, (3), sobre la necesidad de consentimiento para el procesamiento de datos, revocable en cualquier momento y (5), que no menciona las actividades de detección de pornografía en la lista: "(1) Los datos de tráfico relacionados con suscriptores y usuarios procesados y almacenados por el proveedor de una red pública de comunicaciones o servicio de comunicaciones electrónicas disponible al público deben borrarse o anonimizarse cuando ya no sea necesario para la transmisión de una comunicación sin perjuicio de los párrafos 2, 3 y 5 del presente artículo y del artículo 15, apartado 1. (3) Con el fin de comercializar servicios de comunicaciones electrónicas o para la prestación de servicios de valor agregado, el proveedor de un servicio de comunicaciones electrónicas disponible al público podrá procesar los datos mencionados en el párrafo 1 en la medida y durante el tiempo necesario para tales servicios o marketing, si el suscriptor o usuario a quien el informe de datos ha dado su consentimiento. Los usuarios o suscriptores tendrán la posibilidad de retirar su consentimiento para el procesamiento de datos de tráfico en cualquier momento. (5) El procesamiento de datos de tráfico, de conformidad con los párrafos 1, 2, 3 y 4, debe estar restringido a personas que actúen bajo la autoridad de proveedores de redes públicas de comunicaciones y servicios de comunicaciones electrónicas disponibles públicamente que manejen la facturación

periodo de gracia de cinco años tras la aprobación de la propuesta enviada por la Comisión Europea. A pesar del plazo de suspensión regulatorio solicitado, la propuesta del Consejo Europeo carece de una verdadera señalización de los horizontes, es decir, qué se hará durante estos cinco años para que, pasado este plazo, la Directiva de Privacidad Virtual pueda seguir en plena vigencia.

En cuanto a los *hashes*, la implementación de instrumentos para la correcta categorización de contenidos parece ser la principal recomendación. Sin embargo, parece fundamental que los proveedores de servicios, con el propósito de una verdadera vigilancia activa de las plataformas virtuales, den un paso atrás de los *hashe*s para mirar el momento anterior, es decir, la identificación de nuevos contenidos que aún no se han cubierto. Esto incluye, además de los instrumentos de inteligencia artificial, una mejora en el sistema de informes, por ejemplo.

Es fundamental, en este sentido, que las plataformas construyan su evaluación de riesgos y, de acuerdo con los resultados de esta, un sistema de cumplimiento racional apuntando especialmente (a) la ubicación de los sitios de aparición de contenido criminal "nuevos"–nuevos *hashes* y (b) a la identificación en vivo de sitios propicios para la formación de redes de distribución (clubes) de pornografía infantil. La buena noticia es que el estado actual de la técnica ya permite instrumentos para una vigilancia cada vez más segura de la privacidad.

Las técnicas de *clustering* permiten, por ejemplo, identificar patrones de comportamiento en relación con los datos, trasladando los patrones de criminalidad a patrones gráficos fácilmente visibles[39]. Las reglas de asociación identifican patrones dentro de una base de datos[40]. La minería de patrones secuenciales se ocupa de la recurrencia del resultado[41]. Las extracciones de identidad indican patrones no solo entre imágenes, sino también entre textos[42]. El abanico de posibilidades es amplio, especialmente ante un escenario en el que el propio sector tecnológico

---

o la gestión del tráfico, consultas de clientes, detección de fraude, comercialización de servicios de comunicaciones electrónicas o prestación de un servicio de valor agregado, y debe limitarse a lo que sea necesario para los fines de dichas actividades". Directiva 2002/58 / CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de datos personales y la protección de la privacidad en el sector de las comunicaciones electrónicas (Directiva sobre privacidad y comunicaciones electrónicas).

39 "In data mining terminology a cluster is a group of similar data points —a possible crime pattern. Thus appropriate clusters or a subset of the cluster will have a one—to-one correspondence to crime patterns." Shyam Nath Varan. Crime Pattern Detection Using Data Mining. IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology. (s. p.), 2006.

40 Chen *et al*. "Crime data mining: a general framework and some examples" *Computer*, vol. 37, n.° 4 (2004): 50-56, 51. DOI: 10.1109/MC.2004.1297301.

41 Ídem.

42 Chen *et al*. "Crime data mining: a general framework and some examples" *Computer*, vol. 37, n.° 4 (2004): 50-56, 51. DOI: 10.1109/MC.2004.1297301.

se ha mostrado dispuesto a revisar la técnica y adaptarla a una mayor protección de la privacidad.

La combinación de los resultados de un mapeo metodológicamente serio debería indicar, en el futuro, modelos de predicción de *hotspots* efectivos, capaces de orientar, de forma más racional y orientada a la privacidad, las políticas operativas de las plataformas digitales. Se trata de mecanismos que pueden garantizar la preservación de los datos individuales, construyendo mapas de riesgo. Su efecto sería indicar solo los lugares donde la vigilancia debería ser más precisa.

Sin embargo, la dinámica del mundo digital impone que se almacenen las pruebas relacionadas con publicaciones de pornografía infantil, vinculándolas a los autores y en su contra, produciendo pruebas. Sin esto, sería posible una internet con contenido menos pedófilo, pero sin el almacenamiento de material identificativo y probatorio. Y este es el que mejor logra concretar la colaboración de la vigilancia privada con la ejecución penal del Estado[43].

CONCLUSIONES

1. Aunque la minería de datos relacionada con las circunstancias de los delitos perpetrados a través de internet puede tener ahora un lugar reservado con la policía —una efectiva y coherente—, la pornografía infantil también depende de la medición del problema dentro del contexto específico de las propias plataformas. La derogación temporal de los dos artículos (art. 5, 1 y 6) de la Directiva 2002/58 / CE, aunque no corresponda a la mejor técnica legislativa (es decir, una modificación de la Directiva), es una opción plausible. Después de todo, el silencio de la Directiva de Privacidad sobre los mecanismos para la detección automática de pornografía infantil (incluido el *hash*) llevará a las plataformas virtuales a un entorno regulatorio legalmente riesgoso a partir de enero de 2021. Sin *hash*, las políticas de detección de contenido solo dependerían de los canales de información, dejando inoperante todo un instrumento ya constituido.

2. Si bien la Directiva europea de privacidad está en vigor sin ningún otro anexo con respecto a la detección automática de pornografía infantil, la confidencialidad del tráfico podría obstaculizar el sistema de notificación obligatoria, así como la vaguedad sobre las hipótesis de autorización de retención de datos (que conflicto sobre la definición de pornografía infantil) podría desalentar la notificación de un volumen considerable de contenido relevante.

---

43 Como se indica en Christofoletti, de Lima, Rodríguez y Peroli: Protección de datos personales y ciberdelitos: la propuesta de una base de datos de vigilancia preventiva para la difusión de contenidos ilícitos en Internet con el ejemplo de la pornografía infantil. *Revista Electrónica de la Asociación Nacional de Fiscales Públicos*, Brasil, 2020.

3. En cuanto a la retención de datos (art. 6, Directiva Europea de Protección de Datos), la derogación es necesaria hasta que se organicen, de conformidad con la ley penal, cuáles son las hipótesis en las que se autoriza la retención de datos. Con el fin de garantizar la proporcionalidad y razonabilidad de la medida, respecto a las pautas de privacidad, una sedimentación legislativa del asunto, explicando las circunstancias que autorizarían la retención previa de datos y dejando claro que la política de *hashes* no choca con la privacidad parece esencial para el propósito de vigilar activamente el contenido de pornografía infantil. Después de todo, es en la retención de datos en la que aparece el conflicto potencial.

4. En cuanto a la confidencialidad de las comunicaciones (art. 5.1), una aclaración legislativa sobre el hecho de que los *hashes*, aunque sirvan para identificar contenido que simplemente viola los términos de servicio de las plataformas, no viola la privacidad del usuario y precisa de medidas normativas que debe efectuarse con urgencia. Después de todo, los proveedores de servicios tienen derecho a elegir, aunque por razones éticas, qué contenido (incluso si son delincuentes) no circulará entre sus plataformas.

5. A pesar de que los *hash* dominan el estado del arte con el propósito de detectar pornografía infantil, el verdadero compromiso ético con el cumplimiento de las plataformas debe ir más allá. Es urgente medir dónde están las circunstancias de riesgo para desarrollar un modelo de monitoreo de redes en tiempo real; es decir, descifrar cómo se explotan las plataformas virtuales con fines de organizaciones delictivas (en este caso, clubes de pornografía infantil.

6. En este sentido, una propuesta de modificación de la Directiva Europea de Privacidad parece ser una alternativa más coherente, regulando así en un régimen especial la aplicación separada, previamente justificada mediante un mapeo de riesgos, de las disposiciones sobre privacidad virtual para casos de pornografía infantil en red.

7. Se han desarrollado mecanismos de análisis en internet que permiten identificar áreas de riesgo para la pornografía infantil, pero evitar que los datos se almacenen impide que la colaboración entre la vigilancia privada y la aplicación del Estado cumpla sus objetivos, en materia de producción y preservación de posibles pruebas para el procesamiento penal. Si se quiere mantener dicha cooperación, una enmienda a la actual Directiva Europea de Privacidad parece esencial.

8. Aunque los mecanismos de detección de pornografía infantil se basan hoy predominantemente en la política de *hash*, un análisis de patrones, tal como existe para los casos de preparación, parece ser el objeto real de la futura gobernanza cibernética, que debería ser regulada. expresamente por legislación que también garantiza la privacidad de la red. La dimensión real de este mapeo preventivo es, sin embargo, un punto aún por estudiar.

BIBLIOGRAFÍA

ARENA, CHRISTINE. Child porn too big for law enforcement? Microsoft steps in. The Christian Science Monitor, 13 de junio de 2010, disponible en [https://www.csmonitor.com/Business/Case-in-Point/2010/0613/Child-porn-too-big-for-law-enforcement-Microsoft-steps-in] (consulta: 10 de octubre de 2020).

BRIGHT, MARTIN y TRACY MCVEIGH. The Guardian. This club had its own chairman and treasurer. Its business was child abuse, 2001. Disponible en [https://www.theguardian.com/uk/2001/feb/11/tracymcveigh.martinbright] (consulta: 2 de noviembre de 2020).

Carr, John. New EU online privacy law likely to endanger the safety of children. ECPAT, 2 de diciembre de 2018. Disponible en [https://www.ecpat.o rg/news/eu-online-privacy/] (consulta: 21 de noviembre de 2020).

CHEN *et al*. "Crime data mining: a general framework and some examples", *Computer*, vol. 37, n.° 4, 2004. DOI: 10.1109/MC.2004.1297301.

CHRISTOFOLETTI RODRÍGUEZ. *La ciberpornografia infantil y su combate: la ineficacia de los filtros de internet y la delación premiada como alternativa para la persecución penal*, Tirant lo Blanch, 2020.

Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions EU strategy for a more effective fight against child sexual abuse. European Commission. Brussels, 24.7.2020 COM(2020) 607 final.

Community Standards Enforcement Report. Facebook Transparency. Abril 2020-junio 2020, disponible en [https://transparency.f acebook.com/community-standards-enforcement #instagram-adult-nudity-and-sexual-activity] (consulta: 10 de octubre de 2020).

Directorate General For Internal Policies Policy Department C: Citizens' Rights And Constitutional Affairs. (2015). *The law enforcement challenges of cybercrime: are we really playing catch-up?* European Parliament.

European Cybercrime Centre. 'First Year Report', Europol, The Hague, 2014, p. 15.

Europe's thermonuclear debate on privacy and child sexual abuse. Politico. 22 de noviembre de 2020, disponible en [https://www. politico.eu/article/europes-thermonuclear-debate-on-privacy-and-child-sexual-abuse-2] (consulta: 22 de noviembre de 2020).

Farid, Hany. Intergroup expert meeting on EU legislation on the fight against child sex abuse online. Missing Children Europe (Youtube Channel). 15 de octubre de 2020, disponible en [https://www.youtube.com/watch ?v=adY_uWfs90E&t=24m28s] (consulta: 2 de noviembre de 2020).

FATF. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, París, 2012-2020, disponible en [www.fatf-gafi.org/recommendations.html] (consulta: 19 de noviembre de 2020).

Hymas, Charles. Paedophiles privacy more important to European Commission? Legal Experts UK, 2020, disponible en [https://www.legalexperts-uk.com/blog/posts/paedophiles-privacy-more-important-to-european-commission] (consulta: 12 de noviembre de 2020):

Inhope. Artificial Intelligence in the fight against Child Sexual Abuse Material–Part 2. Inhope, 19 de noviembre de 2020, disponible en [https://www.inhope.org/EN/articles/artificial-intelligence-in-the-fight-against-child-sexual-abuse-material] (consulta: 18 de noviembre de 2020).

Inhope. Fighting Crime in the 21st Century–Part 1. Inhope. 12 de noviembre de 2020, disponible en [https://www.inhope.org/EN/articles/fighting-crime-in-the-21st-century] (consulta: 18 de noviembre de 2020).

LANGSTON, JENNIFER. How PhotoDNA for Video is being used to fight online child exploitation. Microsoft. 12 de septimbre de 2018, disponible en [https://news.microsoft.com/on-the-issues/2018/09/12/how-photodna-for-vid eo-is-being-used-to-fight-online-child-exploitation/] (consulta: 18 de noviembre de 2020).

NATH VARAN, SHYAM. *Crime Pattern Detection Using Data Mining*. IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology, 2006, (s. p.).

NETCLEAN. *Eleven Unbelievable Truths*, The NetClean Report, 2015.

Opinion 7/2020 on the Proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online. European Data Protection Supervisor. 10 de noviembre de 2020.

Proposal for a Regulation Of The European Parliament And Of The Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by numberin dependent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online. Bruxelas, 10 de septiembre de 2020.

SALGADO, R. P. Fourth Amendment Search and the Power of the Hash. *Harvard Law Review Forum*, vol. 119, n.° 48, 2005.

The EU will continue to protect children from child sexual abuse online. European Commission. 10 de septiembre de 2020, disponible en [https://ec.europa.eu/home-affairs/news/20200910_eu-continue-protect-children-from-child-sexual-abuse-_en] (consulta: 22 de noviembre de 2020).

TUNKS, MICHAEL. IWF joins coalition of charities raising concerns over the European Commission's E-Privacy Directive. Internet Watch Foundation. 5 de octubre de 2018, disponible en [https://www.iwf.org.uk/ne ws/iwf-joins-coalition-of-charities-raising-concerns-over-european-commissions-e-privacy] (consulta: 21 de noviembre de 2020).

U. S. Department of Justice. The national strategy for child exploitation prevention and interdiction e a report to congress. Abril 2016, disponible en [https://www.justice.gov/psc/national-strategy-child-exploitation-prevention-and-interdiction] (consulta: 10 de noviembre de 2020).

United States v. Reddick 900 F.3d 636 (5th Cir. 2018) Decided: Aug 17, 2018. 900 F.3d 636 (5th Cir. 2018). United States Court of Appeals for the 5th Circuit.