# Delitos en la era digital.

## Cibercrimen & crimen organizado en un mundo interconectado

Leonel Benitez[1]

*"Si tienes conocimiento, deja que otros se iluminen con él."*
*- Margaret Fuller.*

**SUMARIO:** I.- Introducción; II.- Desarrollo; III.- Hipótesis; IV.- Conclusión; V.- Bibliografía

**RESUMEN:** En el siguiente trabajo se realiza un análisis respecto de la ciberdelincuencia, en donde se aborda el concepto de los delitos individuales para llegar a los delitos trasnacionales. En el desarrollo de este, se hace mención a diversos delitos llevados a cabo por estas organizaciones delictivas, se analiza la conformación de su estructura, así como su manejo en los diferentes niveles del ciberespacio, pero particularmente en la conocida *dark web* o red obscura. Para finalizar, se hace mención respecto de la lucha llevada adelante por parte de organismos internacionales en conjunto con países, la legislación que fueron aportando y el caso de Argentina. Como conclusión, se hace un breve desarrollo respecto de la problemática de estos delitos y la posible connivencia de los funcionarios públicos.

**PALABRAS CLAVE:** Ciberdelincuencia – Organizaciones delictivas – Ciberespacio – *Dark web* – Connivencia

[1] Bachiller Universitario en Derecho de la Universidad de Buenos Aires (UBA). Estudiante de Derecho en la Universidad de Buenos Aires (UBA), Email: benitez800@est.derecho.uba.ar.

## I.- Introducción

A lo largo de la historia la comisión de delitos individuales -motivados por factores socioeconómicos, psicológicos, culturales e incluso políticos-, fue provocando un flagelo en la comunidad. Ello, sumado a la falta de políticas públicas e integrales que ataquen el eje de la cuestión, fue el puntapié para que el crimen organizado pueda formarse.

*"(…) la pequeña delincuencia es directamente promovida por las organizaciones criminales, que explotan las condiciones de miseria, necesidad y marginación social de la mano de obra que trabaja para ellas."*[2]

En primer lugar, se puede decir que el desarrollo del crimen organizado se produjo debido a la necesidad y la falta de oportunidades de los individuos, quienes fueron captados por diversos grupos organizados, que, aprovechando su estado de vulnerabilidad crearon una estructura compleja y poderosa.

En segundo lugar -pero no menos importante-, hay que considerar el efecto del surgimiento de la globalización. Se puede advertir que, si bien ha generado avances significativos, también trajo consigo problemáticas que agudizan y ponen en peligro la seguridad a nivel mundial. Tal es así que, con el fin de expandir sus negocios y aumentar las ganancias generadas de manera ilícita, las redes criminales han sabido utilizar la globalización para su beneficio.

*"Si tuviera que aportar una definición jurídica de la globalización, la definiría como un vacío de derecho público a la altura de los nuevos poderes y de los nuevos problemas (..)"*[3]

Estas, lograron -y logran- operar a nivel mundial, sobrepasando las fronteras de los diferentes países, e incluso continentes. En muchos casos, la falta de legislación, de control o ante la connivencia de los diversos gobiernos, ha permitido la expansión y diversificación de las organizaciones criminales.

---

[2] Luigi Ferrajoli. "Criminalidad y Globalización". Boletín Mexicano de Derecho Comparado, año XXXIX, núm. 115, 2006, pág. 305.

[3] Luigi Ferrajoli. "Criminalidad y Globalización". Boletín Mexicano de Derecho Comparado, año XXXIX, núm. 115, 2006, pág. 302.

En búsqueda de dar solución a esta problemática, organismos internacionales comenzaron a crear legislación para tratar de contrarrestar el avance de estos grupos criminales. En el mismo sentido, algunos países coinciden en luchar de manera conjunta, mediante coordinación y cooperación a fin de combatir el crimen organizado.

## II.- Desarrollo[4]

Como se advirtió previamente, el crimen organizado produce graves daños y una afectación al normal funcionamiento de los diversos países y sistemas democráticos. Más allá de esta cuestión, el daño generado hacia la sociedad y particularmente contra las personas, es mucho más grave, daño que en muchos casos es irreversible.

Dentro del conjunto de delitos cometidos por estas organizaciones se podría destacar a uno en particular, el **ciberdelito**[5].

El avance tecnológico produjo un exponencial desarrollo a nivel sociocultural, pero particularmente en los individuos. Si bien, son innumerables los aportes que trajo consigo la tecnología, también lo son las amenazas por el uso indebido de esta. Frente a ello, una de las mayores preocupaciones que surgió a nivel mundial y tiene en vilo a Organizaciones, Estados, Empresas e Individuos, es el ciberdelito.

---

[4] Esta investigación adopta una definición restringida de ciberseguridad, lo que implica ciertos presupuestos que pueden ser considerados como un error conceptual desde otras perspectivas. Si bien este enfoque nos permite analizar ciertos tipos de ciberdelitos de manera más focalizada, es importante tener en cuenta que no podemos pasar por alto la complejidad de fenómenos como el cibercrimen organizado, donde las amenazas están intrínsecamente ligadas a factores sociales, políticos y económicos. No obstante, es importante señalar que existe un debate académico sobre la definición de ciberseguridad, y algunos autores abogan por un enfoque más amplio que incluya estos aspectos. Para una visión más completa, se recomienda consultar otras fuentes que aborden la ciberseguridad desde una perspectiva más amplia. Véase, por ejemplo, Europol (2024), "Internet Organised Crime Threat Assessment" (IOCTA) 2024, Publications Office of the European Union, Luxembourg. Ricardo Antonio Parada; José Daniel Errecaborde "Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet / compilado. - 1a ed. - Ciudad Autónoma de Buenos Aires: Erreius, 2018".

[5] https://www.unodc.org/ropan/es/ciberdelito.html

Jürgen Stock - Secretario General de INTERPOL. "Guía sobre la Estrategia Nacional contra la Ciberdelincuencia". Japan-ASEAN Cooperatión. Abril 2021, pág. 9.

Esta, es una conducta ilegal que se lleva adelante en el denominado *ciberespacio*[6] mediante el uso de dispositivos electrónicos y redes informáticas, sean públicas o privadas. Ahora bien, dentro de este espectro se podría resaltar a dos grandes grupos, por un lado, se encuentran los que atentan contra la intimidad y la privacidad y por el otro, los que apuntan contra los de naturaleza económica.

Esta modalidad delictiva es llevada adelante con la ayuda de programas maliciosos y tiene por fin suprimir, dañar, deteriorar, alterar u obtener datos informáticos y/o personales sin autorización, para poder sacar un rédito económico o simplemente causar algún daño.

*"El vínculo malicioso con los hackeos se documentó por primera vez en los años 70, cuando los primeros teléfonos informatizados se convirtieron en un objetivo. Los expertos en tecnología conocidos como "phreakers" encontraron una forma de evitar el pago de las llamadas de larga distancia mediante una serie de códigos. Fueron los primeros hackers (…)"*[7]

El crecimiento exponencial de la tecnología acompañado de la dependencia que se fue generando en los individuos, empresas, etc., permitió que diversos grupos se adapten y comiencen a llevar adelante esta modalidad delictiva.

[6] Cyberspace Policy Review Assuring a Trusted and Resilient Information and Communications Infrastructure https://irp.fas.org/eprint/cyber-review.pdf

[7] https://www.pandasecurity.com/es/mediacenter/tipos-de-cibercrimen/

 [8]

Una particularidad de relevancia es que, en los delitos cometidos de manera individual los actores no gozan -salvo excepciones- de grandes ingresos, con lo cual los recursos que tienen son escasos. En el caso de las organizaciones delictivas[9], ocurre completamente lo contrario debido a que la abundancia de sus ingresos les permite una mayor adaptación y la posibilidad de crear estructuras mucho más sofisticadas para la comisión de este tipo de delitos.

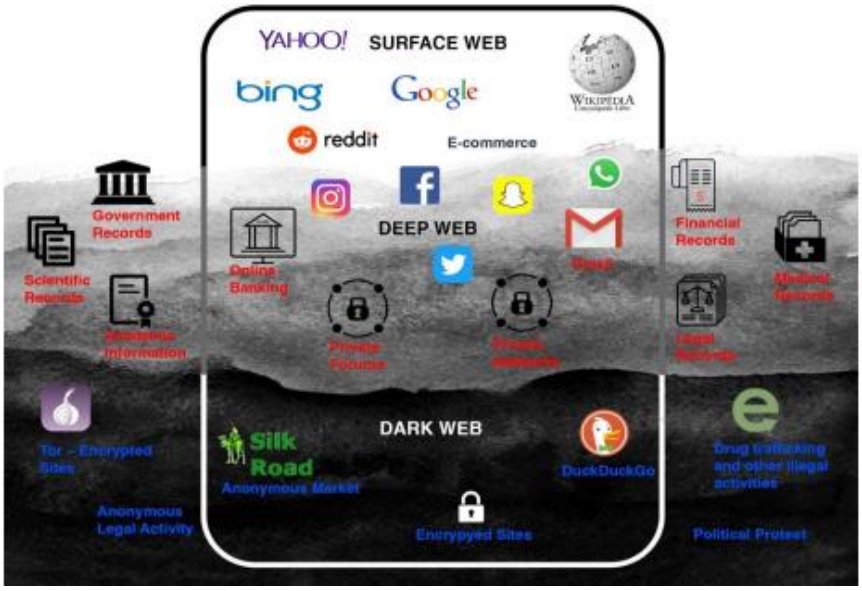
El ciberespacio, se ha convertido en un protagonista de suma trascendencia en un mundo cada vez más virtualizado, que no reconoce fronteras y que, sin dudas fue abriendo paso a una gama de opciones que, de cierta manera, inciden en la vida de las personas.

Esta diversificación que se da en el ciberespacio puede ser entendida en tres niveles, *Surface Web, Deep Web y Dark Web.*

---

[8] Imagen ilustrativa de una organización criminal operando. Aunque es comúnmente asociada a los hackers, estos representan solo una pequeña parte del espectro de la ciberdelincuencia. El crimen organizado cibernético involucra a una amplia variedad de actores y técnicas, desde hackers hasta grupos organizados que utilizan una gran diversidad tecnológica para la comisión de delitos.

[9] Depetris, J. A. (2021). Organizaciones criminales digitales: conocerlas para enfrentar su desafío. Revista Del CLAD Reforma Y Democracia, 79, 117-154. https://clad.org/wp-content/uploads/2022/03/079-04-D-1.pdf



[10]

En el primer nivel se encuentra la *Surface Web*[11], también conocida como red superficial. Esta, es la parte por la que se navega a diario y que representa la gran mayoría de internet, mediante la cual se accede a través de motores de búsqueda. Como, por ejemplo: portales de noticias, redes sociales, plataformas de comercio electrónico, etc.

En esta red, las direcciones de IP son de fácil rastreo, con lo cual los usuarios pueden ser detectados. Sin embargo, el fácil y rápido acceso permite que se produzca la mayor parte de interacciones, y como consecuencia surge una realidad no tan agradable, la formación de un terreno fértil para una gran cantidad de ciberdelitos, como estafas, acosos, difamaciones, hasta apropiación intelectual, entre otros.

En el segundo nivel, se encuentra la *Deep Web*[12] o red profunda. En esta parte, figura el conjunto de páginas que no están indexadas por los motores de búsqueda tradicionales, como pueden ser Google, Bing o Yahoo! y, por lo tanto, cuando se realiza una búsqueda en estas plataformas, no figura el resultado debido a que su contenido no está incluido en el índice de los buscadores.

---

[10] Imagen ilustrativa de los diferentes niveles de la Web.

[11] INTERPOL/ENACT. "Online African organized crime from surface to dark web" Analytical Report. Julio 2020, pág. 17.

[12] INTERPOL/ENACT. "Online African organized crime from surface to dark web" Analytical Report. Julio 2020, pág. 17.

La clave principal se centra en el uso de los servidores *proxy*[13] o *VPN*[14], los cuales actúan como intermediarios que colocan barreras, permitiendo enmascarar la identidad de los usuarios y así evitar la detección mediante rastreo, otorgando de esa manera, una especie de anonimato.

En el último nivel, se encuentra la *Dark Web*[15] o red obscura. Esta, forma una pequeña parte de la red profunda, pero requiere software personalizado para acceder a su contenido. En esta parte de la *web*, los usuarios tienen la posibilidad de mantener oculta su identidad, así como también su ubicación, lo que les permite escudarse con una navegación anónima de cara a otras personas y en especial, a los agentes de la ley.

*"(…) se utilizan direcciones IP enmascaradas y es solo accesible con un navegador web especial. Estas páginas que normalmente utilizan los dominios. onion o .i2p solo son accesibles con un software especial (por ejemplo, TOR, i2p y freenet) que dan acceso a las Darknets en las que se alojan."*[16]

Es un método utilizado por particulares, pero principalmente por grandes grupos para la comisión de delitos. A través del anonimato, las organizaciones delictivas logran su objetivo y se pueden manejar de una manera en donde no quedan expuestas y, por ende, no pueden ser desmanteladas.

---

[13] INCIBE (s/f). "Glosario de términos de ciberseguridad" https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf, pág. 64.

[14] INCIBE (s/f). "Glosario de términos de ciberseguridad" https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf, pág. 77.

[15] INTERPOL/ENACT. "Online African organized crime from surface to dark web" Analytical Report. Julio 2020, pág. 40.

[16] https://www.a2secure.com/blog/diferencias-entre-surface-web-deep-web-y-dark-web/

[17]

*"El tipo de contenido que tiene más popularidad en la web oscura es la pornografía ilegal, más específicamente, la pornografía infantil. Alrededor del 80% de su tráfico web está relacionado con el acceso a la pornografía infantil a pesar de ser difícil de encontrar incluso en la web oscura. Un sitio web llamado Lolita City, que desde entonces ha sido desmantelado, contenía más de 100 GB de medios pornográficos infantiles y tenía unos 15.000 miembros."*[18]

## III.- Hipótesis

### a) Estructura de la organización

La diferencia principal en comparación con las organizaciones criminales convencionales es que estas se manejan en el ámbito del ciberespacio lo que les permite moverse en un ámbito mucho más seguro y *encriptado*[19], en donde predomina el anonimato.

La particularidad de estos canales seguros es que, toda aquella información sensible va a ser compartida por aquellos a quienes se pretenda compartir y no a terceros que puedan poner en riesgo a la organización debido a las filtraciones.

Como fue mencionado anteriormente, la modalidad delictiva y el rápido ingreso de dinero, permite que la organización pueda ir perfeccionándose y de esa

---

[17] https://es.slideshare.net/slideshow/deep-web-o-internet-profunda/235077692

[18] https://es.wikipedia.org/wiki/Dark_web#:~:text=El%20tipo%20de%20contenido%20que,y%20ten%C3%ADa%20unos%2015.000%20miembros.

[19] https://cloud.google.com/learn/what-is-encryption?hl=es

manera crear estructuras mucho más complejas con el fin de evitar a las fuerzas de seguridad.

*"Con ganancias estimadas en miles de millones, sus negocios criminales se parecen mucho a los negocios legítimos internacionales. Cuentan con modelos operativos, estrategias a largo plazo, jerarquías, e incluso alianzas estratégicas, todo con el propósito de generar un máximo de beneficios con un mínimo de riesgo."*[20]

Respecto de la estructura jerárquica, cabe destacar que quienes integran estos grupos criminales -y que, generalmente están a la cabeza de la organización- son personas con bastos conocimientos técnicos en áreas como programación, ingeniería o seguridad informática.

Los reclutadores, son quienes se encargan del crecimiento de la organización y su tarea es ir captando individuos para sumarlos a la red criminal mediante la utilización de métodos como, por ejemplo, anuncios en línea, publicaciones en foros, etc.

Para la mano de obra final -o consumación del delito-, se van a necesitar operadores que actúen conforme a las órdenes dictadas por los técnicos, quienes determinarán el objetivo del ciberataque[21].

**b) Modalidad de ciberdelincuencia utilizada**

Estas organizaciones utilizan diversos métodos para llevar adelante la comisión de delitos. Si bien, hay múltiples delitos, se destacarán los siguientes:

*"Por regla general, las redes delictivas organizadas están implicadas en muchos tipos diferentes de actividades delictivas extendidas por varios países. Estas actividades pueden incluir trata de personas, tráfico de drogas, mercancías ilícitas y armas, robo a mano armada, falsificaciones y blanqueo de capitales."*[22]

---

[20] https://www.interpol.int/es/Delitos/Delincuencia-organizada#:~:text=Por%20regla%20general%2C%20las%20redes,falsificaciones%20y%20blanqueo%20de%20capitales.

[21] https://www.microsoft.com/es-ar/security/business/security-101/what-is-a-cyberattack

[22] https://www.interpol.int/es/Delitos/Delincuencia-organizada#:~:text=Por%20regla%20general%2C%20las%20redes,falsificaciones%20y%20blanqueo%20de%20capitales.

– *Phishing*[23]: Es una modalidad de engaño que se realiza mediante el envío de correo electrónico, mensaje de texto falso o a través de la realización de llamados telefónicos, cuyo objetivo es obtener información personal o financiera de la víctima.

*"Los ciberdelincuentes se hacen pasar por empresas de servicios, oficinas de gobierno o amigos de algún familiar y te piden los datos que les faltan para suplantar tu identidad y así operar tus cuentas en bancos, perfiles en las plataformas y redes sociales, servicios y aplicaciones web."*[24]

– *Malware*[25]: Es una modalidad en donde se crean software malicioso para obtener datos sensibles de una persona y de esa manera exigir un monto de dinero para devolverlo. Ejemplo: virus, troyanos, *ransomware* y *spyware*.

– Sextorsión[26]: Es un método en donde se extorsiona a la víctima, y se la amenaza con la difusión de imágenes sexuales a cambio de dinero.

– Ciberterrorismo[27]: En algunos casos, se intenta atacar a la seguridad nacional mediante el ataque a redes eléctricas, sistemas de transporte, sistemas de comunicación o infraestructura crítica con el fin de crear terror entre la población.

– Pornografía infantil[28]: Es una modalidad de corrupción de menores y explotación sexual que tiene por fin, producir y comercializar imágenes/videos con actividad sexual explícita. Esto, fomenta y normaliza la pedofilia, lo que representa un grave peligro para el conjunto de la sociedad.

---

[23] https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/spoofing-and-phishing

[24] https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-el-ciberdelito

[25] Richard Kissel, Editor. **"**NIST, Glosario de términos clave de seguridad de la información" [mayo de 2013] Pág. 118. https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

[26] https://staysafeonline.org/es/online-safety-privacy-basics/sextortion-what-to-do/ https://www.incibe.es/ciudadania/avisos/campana-de-sextorsion-no-publicaran-tus-videos-intimos-si-les-pagas-en-bitcoines

[27] https://www.ciberseguridad.eus/ciberglosario/ciberterrorismo

[28] https://www.oas.org/ios/glossarydetails.aspx?lang=es&type=0&id=7

– Lavado de activos[29]: Es una práctica en la que se utiliza al sistema financiero para realizar transferencias de dinero a cuentas bancarias falsas, para comprar bienes de alto valor o para invertir en negocios legítimos con el fin de ocultar la ilicitud de esas ganancias.

– Tráfico de drogas y armas[30]: Implica la producción, adquisición, transporte, almacenamiento, distribución y venta ilícitas de armas de fuego, municiones y sustancias estupefacientes en la red con el fin de obtener ganancias económicas y ejercer control territorial.

– Trata de personas[31]: En la trata en línea -a diferencia del modelo tradicional de trata- la explotación se adapta a las demandas que existan en el momento. En esta modalidad, se pueden reclutar y explotar a personas de diferentes géneros y edades según la demanda, lo que hace que sea más flexible y difícil de detectar. El sometimiento a las víctimas puede ir desde, explotación sexual, laboralmente o para la extracción de órganos.

*"Pueden usar estas herramientas en cada etapa del proceso, desde la identificación y el reclutamiento de víctimas potenciales, a través del proceso de coerción y control, hasta la publicidad y venta de bienes y servicios producidos a partir de su explotación y, finalmente, hasta el blanqueo del producto del delito"*[32]

– Cryptojacking[33]: Consiste en el uso no autorizado de la potencia de cálculo de dispositivos (computadoras, smartphones, servidores) con el fin de generar criptomonedas. Este proceso, denominado minería, se realiza a través de

---

[29] Pleé, R. (2008). El lavado de dinero. Un fenómeno transnacional de política criminal contemporánea. Buenos Aires, Argentina: Thomson Reuters.
https://www.oas.org/es/sms/ddot/gelavex/54/docs/21-Presentaci%C3%B3n%20Perry%20Center-C.Realuyo-ESP.pdf

[30] Depetris, J. A. (2021). Organizaciones criminales digitales: conocerlas para enfrentar su desafío. Revista Del CLAD Reforma Y Democracia, 79, 117-154. https://clad.org/wp-content/uploads/2022/03/079-04-D-1.pdf, pág. 128.

[31] https://www.unodc.org/toc/es/crimes/human-trafficking.html#_ednref1
https://www.missingkids.org/es/theissues/trafficking

[32] https://www.unitedexplanations.org/2024/01/25/trata-de-personas-en-la-dark-web-una-nueva-forma-de-esclavitud/

[33] https://www.interpol.int/es/Delitos/Ciberdelincuencia/Cryptojacking

software malicioso que se instala en el dispositivo de la víctima, ralentizándolo y consumiendo recursos energéticos.

– Botnest[34]: Se trata de un conjunto de redes de dispositivos infectados por un software malicioso. Tras la infección, se convierten en un *bot* conectado a un servidor central. Estos pueden ser controlados de forma remota para realizar ataques cibernéticos a gran escala.

### c) ¿Escasa legislación o connivencia?

En el marco de esta investigación, se ha evidenciado cómo las organizaciones criminales han sabido capitalizar el exponencial avance de la tecnología y la globalización para expandir su estructura y dar un mayor alcance a sus actividades ilícitas. Uno de los factores principales que ha permitido y facilitado su crecimiento, es la inexistencia de fronteras en el ciberespacio. La falta de delimitaciones por parte de los Estados en el ámbito digital dio lugar a que estas organizaciones puedan actuar de manera trasnacional y de esa manera llegar a eludir el control de las autoridades de las diversas naciones.

*"En algunos países, incluso puede haber una falta de legislación y, en consecuencia, de criminalización de la ciberdelincuencia, lo que crea una situación en la que el país se convierte en un refugio seguro para los ciberdelincuentes."*[35]

En muchos casos no es solo falta de legislación, recursos o incapacidad, sino que la problemática surge por la connivencia e incluso la colaboración directa de quienes conforman los diferentes gobiernos. La complicidad de los funcionarios que los componen lleva a que estas organizaciones puedan desarrollarse y actuar sin límite alguno, aun siendo explicita su ilicitud.

Por otra parte, uno de los principales contribuyentes para que las organizaciones criminales funcionen, se desarrollen y actúen con completa impunidad, son los denominados paraísos fiscales. Estos, permiten que grandes cantidades de dinero ingresen a las arcas de los individuos, organizaciones, etc. sin

[34] Eremin, Alexander (2 de abril de 2019). "Bots y botnets en 2018", Securelist. https://securelist.lat/bots-and-botnets-in-2018/88697/

[35] Jürgen Stock - Secretario General de INTERPOL. "Guía sobre la Estrategia Nacional contra la Ciberdelincuencia". Japan-ASEAN Cooperatión. Abril 2021, pág. 15.

necesidad de aclarar su procedencia, permitiendo así que, las organizaciones puedan manejarse de una manera más holgada.

### d) Coordinación entre los Estados

*"El CSIS informó de que en enero de 2023 se emitió una advertencia conjunta de tres autoridades estadounidenses de ciberseguridad -la CISA, la NSA (Agencia de Seguridad Nacional) y el MS-ISAC (Centro Multiestatal de Análisis e Intercambio de Información)- sobre el aumento del phishing y otros ataques contra ramas civiles del Gobierno estadounidense."*[36]

Frente a ello, diversos países tomaron medidas con el fin de contrarrestar estas amenazas cibernéticas. En principio, se fueron promulgando diversas leyes con el fin de dar una solución rápida y evitar la propagación de estos nuevos delitos, por otra parte, fueron desarrollando nuevos programas de ciberseguridad, con ingeniería sofisticada y personal especializado en la materia.

Aun así, hay países que tienen una mayor vulnerabilidad y son propensos a recibir ataques de tipo cibernético. Y esto se debe a la poca legislación que poseen, e incluso a la inexistencia de esta, con lo cual están en completa desprotección.

| País | Índice Nacional de Ciberseguridad (NCSI) | Índice Global de Seguridad (GSI) 2020 | Índice de Exposición a la Ciberseguridad (CEI) 2020* | Puntuación de Ciberseguridad (media de NCSI, GCI y |
|---|---|---|---|---|
| 1. Afganistán | 11.69 | 5.20 | 0.00 | 5.63 |
| 2. Birmania | 10.39 | 36.41 | 9.00 | 18.60 |
| 3. Namibia | 15.58 | 11.47 | 32.10 | 19.72 |
| 4. Libia | 10.39 | 28.78 | 20.70 | 19.96 |
| 5. Honduras | 22.08 | 2.20 | 39.70 | 21.33 |
| 6. Camboya | 15.58 | 19.12 | 29.70 | 21.47 |
| 7. Mongolia | 18.18 | 26.20 | 26.20 | 23.53 |
| 8. Etiopía | 32.47 | 27.74 | 13.40 | 24.54 |
| 9. Venezuela | 28.57 | 27.06 | 19.30 | 24.98 |
| 10. Nicaragua | 29.87 | 9.00 | 40.00 | 26.29 |

[37]

[36] https://seon.io/es/recursos/informe-global-sobre-ciberdelincuencia-que-paises-corren-mayor-riesgo/

[37] https://seon.io/es/recursos/informe-global-sobre-ciberdelincuencia-que-paises-corren-mayor-riesgo/

En respuesta a la lucha empleada, diferentes organismos fueron creando un marco normativo que, en cierto modo ayudó a que los países tengan herramientas para empezar a tomar acción frente a esta problemática.

El Convenio de Budapest[38] (firmado en 2001 – entrada en vigor 2004), el primer tratado internacional que inició la lucha contra el ciberdelito, establece las bases para que las naciones firmantes cooperen en temas relacionados con ciberseguridad, así como también es el primer instrumento internacional que tipifica y penaliza diversos delitos informáticos, incluyendo los que fueron cometidos por organizaciones criminales.

Interpol[39], a través de su Centro de Intercambio de Información sobre la Ciberdelincuencia elaboró una estrategia mundial para reducir el impacto de la ciberdelincuencia a nivel mundial, con el fin de brindar protección a la comunidad internacional. Allí se plantearon 4 objetivos, donde se establece el intercambio de información, la cooperación entre países miembro, el apoyo al desarrollo de las diversas estrategias y la participación en foros internacionales respecto de ciberdelincuencia.

La Convención de Palermo[40] (Convención contra la Delincuencia Organizada Transnacional), es un tratado impulsado por Naciones Unidas en el año 2000 en contra del crimen organizado. A diferencia del Convenio de Budapest, esta posee un enfoque mucho más amplio, sin embargo, define al ciberdelito como aquel que puede ser cometido mediante la utilización de un sistema o una red informática. También establece un marco regulatorio para la prevención, investigación y posterior sanción de las organizaciones criminales.

La Europol[41], es una agencia de seguridad que se encuentra bajo la órbita de la Unión Europea. Su objetivo principal es coordinar operaciones a gran escala contra redes criminales, facilitar el intercambio de información entre las fuerzas policiales de los Estados miembros con el fin de rastrear la actividad de los ciberdelincuentes y desarticular las organizaciones.

---

38 https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

39 https://www.interpol.int/es/Delitos/Ciberdelincuencia/Respuesta-a-las-ciberamenazas

40 https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf

41 https://www.europol.europa.eu/about-europol

*European Multidisciplinary Platform Against Criminal Threats* (EMPACT)[42], es una plataforma creada por la Unión Europea para combatir al crimen organizado, especialmente al cibercrimen. Mediante esta iniciativa de cooperación internacional, los Estados miembros comparten información, coordinan operaciones y desarrollan herramientas tecnológicas para desarticular redes criminales y garantizar la seguridad ciudadana en el entorno digital. Dicha plataforma representa un avance sumamente relevante para lograr una armonización en el marco jurídico penal internacional y en la lucha contra delitos que trascienden las fronteras.

Por el lado de la legislación interna, Argentina con el fin de acabar con este tipo de delitos, fue creando diversas normas que atacan la ciberdelincuencia como, por ejemplo, la Ley de Protección de Datos Personales (Ley 25326)[43], Ley de Propiedad Intelectual (Ley 11.723)[44], Ley de Delitos Informáticos (Ley 26.388)[45], Ley de Grooming (Ley 26.904)[46]. Sin embargo y pese a la lucha constante, delitos como el grooming siguen en ascenso.

## IV.- Conclusión

Según lo investigado, se puede definir a la ciberdelincuencia como crimen organizado. Esta denominación es correcta, ya que la conformación de estos grupos implica un riesgo significativo, no solamente a nivel individual, sino también mundial, debido a que es una amenaza que nos involucra a todos.

Por ello, resulta necesario que los Estados y organismos internacionales cooperen, y coordinen estrategias de detección de este tipo de delitos, con el fin de brindar una respuesta a esta problemática. Solo mediante el esfuerzo mundial se podrá construir un ciberespacio seguro. Por ello, dicha respuesta debe ser urgente, ya que es una amenaza latente que se encuentra en constante crecimiento.

Asimismo, es imprescindible que se ataque a las organizaciones y se detenga a quienes las componen, pero también, que se realicen tareas de prevención evitando la propagación de esta red criminal y un desarrollo mayor. De esta manera, se

[42] https://www.europol.europa.eu/crime-areas-and-statistics/empact
[43] https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm
[44] https://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/42755/texact.htm
[45] https://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm
[46] https://servicios.infoleg.gob.ar/infolegInternet/anexos/220000-224999/223586/norma.htm

limita el reclutamiento de individuos que se encuentren en una situación de desprotección.

¿Es posible educar y concientizar a la sociedad sobre estos riesgos? La respuesta es sí, claro. La falta de información brindada a la ciudadanía ayuda a que estos grupos avancen con mayor velocidad, con lo cual es de suma relevancia que se informe sobre los riesgos y como prevenir los ciberdelitos.

Por ello es necesario ir reforzando las diversas leyes que, si bien fueron relevantes, no están resolviendo el problema o bien la totalidad de estos.

¿Existe un interés real de la política para combatir la corrupción pública y connivencia con el crimen organizado?

## V.- Bibliografía


- Luigi Ferrajoli. "Criminalidad y Globalización". Boletín Mexicano de Derecho Comparado, año XXXIX, núm. 115, 2006, pág. 305.
- Luigi Ferrajoli. "Criminalidad y Globalización". Boletín Mexicano de Derecho Comparado, año XXXIX, núm. 115, 2006, pág. 302.
- Europol (2024), "Internet Organised Crime Threat Assessment" (IOCTA) 2024, Publications Office of the European Union, Luxembourg.
- Ricardo Antonio Parada; José Daniel Errecaborde "Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet / compilado. - 1a ed. - Ciudad Autónoma de Buenos Aires: Erreius, 2018"
- https://www.unodc.org/ropan/es/ciberdelito.html
- Jürgen Stock - Secretario General de INTERPOL. "Guía sobre la Estrategia Nacional contra la Ciberdelincuencia". Japan-ASEAN Cooperatión. Abril 2021, pág. 9.
- Cyberspace Policy Review Assuring a Trusted and Resilient Information and Communications Infrastructure https://irp.fas.org/eprint/cyber-review.pdf
- https://www.pandasecurity.com/es/mediacenter/tipos-de-cibercrimen/

- Depetris, J. A. (2021). Organizaciones criminales digitales: conocerlas para enfrentar su desafío. Revista Del CLAD Reforma Y Democracia, 79, 117-154. https://clad.org/wp-content/uploads/2022/03/079-04-D-1.pdf
- INTERPOL/ENACT. "Online African organized crime from surface to dark web" Analytical Report. Julio 2020, pág. 17.
- INCIBE (s/f). "Glosario de términos de ciberseguridad" https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf, pág. 64.
- INCIBE (s/f). "Glosario de términos de ciberseguridad" https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf, pág. 77.
- INTERPOL/ENACT. "Online African organized crime from surface to dark web" Analytical Report. Julio 2020, pág. 40.
- https://www.a2secure.com/blog/diferencias-entre-surface-web-deep-web-y-dark-web/
- https://es.slideshare.net/slideshow/deep-web-o-internet-profunda/235077692
- https://es.wikipedia.org/wiki/Dark_web#:~:text=El%20tipo%20de%20contenido%20que,y%20ten%C3%ADa%20unos%2015.000%20miembros.
- https://cloud.google.com/learn/what-is-encryption?hl=es
- https://www.interpol.int/es/Delitos/Delincuencia-organizada#:~:text=Por%20regla%20general%2C%20las%20redes,falsificaciones%20y%20blanqueo%20de%20capitales.
- https://www.microsoft.com/es-ar/security/business/security-101/what-is-a-cyberattack
- https://www.interpol.int/es/Delitos/Delincuencia-organizada#:~:text=Por%20regla%20general%2C%20las%20redes,falsificaciones%20y%20blanqueo%20de%20capitales.
- https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/spoofing-and-phishing
- https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-el-ciberdelito

- Richard Kissel, Editor. **"**NIST, Glosario de términos clave de seguridad de la información" [mayo de 2013] Pág. 118. https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
- https://staysafeonline.org/es/online-safety-privacy-basics/sextortion-what-to-do/
- https://www.incibe.es/ciudadania/avisos/campana-de-sextorsion-no-publicaran-tus-videos-intimos-si-les-pagas-en-bitcoines
- https://www.ciberseguridad.eus/ciberglosario/ciberterrorismo
- https://www.oas.org/ios/glossarydetails.aspx?lang=es&type=0&id=7
- Pleé, R. (2008). El lavado de dinero. Un fenómeno transnacional de política criminal contemporánea. Buenos Aires, Argentina: Thomson Reuters.
- https://www.oas.org/es/sms/ddot/gelavex/54/docs/21-Presentaci%C3%B3n%20Perry%20Center-C.Realuyo-ESP.pdf
- Depetris, J. A. (2021). Organizaciones criminales digitales: conocerlas para enfrentar su desafío. Revista Del CLAD Reforma Y Democracia, 79, 117-154. https://clad.org/wp-content/uploads/2022/03/079-04-D-1.pdf, pág. 128.
- https://www.unodc.org/toc/es/crimes/human-trafficking.html#_ednref1
- https://www.missingkids.org/es/theissues/trafficking
- https://www.unitedexplanations.org/2024/01/25/trata-de-personas-en-la-dark-web-una-nueva-forma-de-esclavitud/
- https://www.interpol.int/es/Delitos/Ciberdelincuencia/Cryptojacking
- Eremin, Alexander (2 de abril de 2019). "Bots y botnets en 2018", Securelist. https://securelist.lat/bots-and-botnets-in-2018/88697/
- Jürgen Stock - Secretario General de INTERPOL. "Guía sobre la Estrategia Nacional contra la Ciberdelincuencia". Japan-ASEAN Cooperatión. Abril 2021, pág. 15.
- https://seon.io/es/recursos/informe-global-sobre-ciberdelincuencia-que-paises-corren-mayor-riesgo/
- https://seon.io/es/recursos/informe-global-sobre-ciberdelincuencia-que-paises-corren-mayor-riesgo/
- https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
- https://www.interpol.int/es/Delitos/Ciberdelincuencia/Respuesta-a-las-ciberamenazas

- https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf
- https://www.europol.europa.eu/about-europol
- https://www.europol.europa.eu/crime-areas-and-statistics/empact
- https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm
- https://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/42755/texact.htm
- https://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm
- https://servicios.infoleg.gob.ar/infolegInternet/anexos/220000-224999/223586/norma.htm