14º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal

Kioto (Japón), 20 a 27 de abril de 2020

Distr. general
23 de enero de 2020
Español
Original: inglés

Tema 6 del programa provisional*
Cooperación internacional y asistencia técnica para prevenir y abordar todas las formas de delincuencia

Seminario 4. Tendencias delictivas actuales, fenómenos recientes y soluciones emergentes, en particular la utilización de las nuevas tecnologías como medio e instrumento contra el delito**

Documento de antecedentes preparado por la Secretaría

Resumen

En el presente documento de antecedentes se examina el impacto de la tecnología, que es un arma de doble filo: por un lado facilita la comisión de delitos, pero por otro contribuye a su prevención, detección y supresión. Así pues, en este documento se adopta un enfoque de doble vertiente para explicar el dualismo fundamental que se deriva de lo anterior: por un lado, el papel de la tecnología para hallar soluciones que faciliten la actuación policial, el ejercicio de la acción penal y la obtención de resultados en materia de justicia penal; por otro, el papel más oscuro de la tecnología, que mejora los *modus operandi* de los delincuentes y los grupos delictivos organizados. Este análisis tiene en cuenta la evolución de la situación en ámbitos concretos y abarca dos aspectos de carácter transversal: la importancia de la capacitación, los enfoques multidisciplinares y las sinergias entre los interesados pertinentes para comprender los beneficios actuales de las tecnologías y las posibilidades que estas ofrecen para hacer frente a futuras amenazas delictivas, y la necesidad de tener debidamente en cuenta las cuestiones éticas y las salvaguardias de los derechos humanos al utilizar las tecnologías para combatir la delincuencia.

* A/CONF.234/1.

** La Secretaría desea expresar su agradecimiento a los institutos de la red del programa de las Naciones Unidas en materia de prevención del delito y justicia penal, especialmente el Instituto Coreano de Criminología y el Instituto Nacional de Justicia del Departamento de Justicia de los Estados Unidos, por su ayuda en la preparación y organización del seminario.

I. Introducción

1. En 1997, cuando el Programa de las Naciones Unidas para la Fiscalización Internacional de Drogas y el Centro para la Prevención Internacional del Delito se fusionaron para convertirse en lo que más adelante, en 2002, pasó a llamarse la Oficina de Fiscalización de Drogas y de Prevención del Delito (UNODC), una versión mejorada de la computadora "Deep Blue", programada para jugar al ajedrez, se convirtió en el primer sistema informático en derrotar a un campeón del mundo vigente en una partida que se ajustó a los límites de tiempo habituales de los torneos de ajedrez. En ese momento, pese al ritmo imparable de los avances tecnológicos, la delincuencia todavía era relativamente "poco tecnológica" y el impacto de Internet como tecnología decisiva de la "era digital" se estaba empezando a sentir en la sociedad.

2. Poco más de dos decenios después, la rápida expansión de Internet y de las tecnologías de la información y las comunicaciones ha impulsado el crecimiento económico y ampliado el acceso a servicios vitales, pero también creado nuevas oportunidades para las actividades delictivas. Los delincuentes se han convertido en los beneficiarios no intencionados de las nuevas tecnologías y la globalización, ya que esos adelantos les han permitido explotar las actividades transnacionales para cometer delitos y beneficiarse de ellos y ampliar el alcance de sus actividades y empresas ilícitas mediante plataformas digitales que al mismo tiempo reducen los riesgos a los que se exponen, en particular el riesgo de detección[1].

3. Por otra parte, las tecnologías nuevas y las ya existentes ofrecen nuevas oportunidades para la labor de las fuerzas del orden, la investigación criminal y el ejercicio de la acción penal. La mejora de la seguridad pública y el empoderamiento de las autoridades de cumplimiento de la ley y justicia penal para prevenir y combatir la delincuencia mediante los avances tecnológicos podría tener un efecto positivo en el logro de los objetivos de la Agenda 2030 para el Desarrollo Sostenible, en particular el Objetivo 16.

4. En su informe titulado "La era de la interdependencia digital", el Panel de Alto Nivel sobre la Cooperación Digital, establecido por el Secretario General en 2018 para fortalecer la cooperación internacional y entre múltiples interesados y contribuir al debate público sobre cómo lograr un futuro digital seguro e inclusivo para todos, también puso de relieve "las dos caras de Jano". Como se ha señalado, se ha demostrado que las tecnologías digitales tienen capacidad para conectar a las personas superando las barreras geográficas y culturales, propiciar el buen entendimiento y ayudar a las sociedades a ser más pacíficas y cohesionadas. No obstante, también hay casos en que las tecnologías digitales se han utilizado para violar los derechos, atentar contra la privacidad, polarizar a las sociedades e incitar a la violencia[2].

5. El presente documento de antecedentes parte del marco temático del seminario 4 descrito en la guía para las deliberaciones del 14º Congreso[3] y lo amplía. El documento se estructura en secciones independientes que se corresponden con los diferentes ángulos desde los que se examina la cuestión central: las autoridades de cumplimiento de la ley y justicia penal se encuentran en una encrucijada debido a la rapidez con que se producen las innovaciones tecnológicas, que pueden dotar de mayor eficacia a la actuación policial y ser indispensables para superar las carencias que suelen presentar las medidas encaminadas a hacer respetar plenamente el estado de derecho, pero que también se prestan a la explotación con fines delictivos en diferentes ámbitos[4].

[1] Yury Fedotov, "En solo dos decenios, la tecnología se ha convertido en la piedra angular de la delincuencia" [cita traducida], *Huffington Post UK*, 23 de octubre de 2017.

[2] Véase Naciones Unidas, "La era de la interdependencia digital", junio de 2019, pág. 17.

[3] A/CONF.234/PM.1, párrs. 161 a 189.

[4] El uso de las tecnologías digitales y de Internet con fines terroristas y otras cuestiones relacionadas con la ciberdelincuencia se examinan en el documento de trabajo de la Secretaría sobre el tema 6 del programa (A/CONF.234/7).

II. Las tecnologías como herramienta para delinquir y para combatir la delincuencia

A. Criptomonedas y activos virtuales

6. En los últimos años han surgido las criptomonedas y los activos virtuales, que han atraído inversiones en las infraestructuras de pago creadas mediante sus protocolos de *software*[5]. Los usuarios de las criptomonedas las encuentran útiles por diversos motivos, pero también invierten en ese tipo de activos con fines especulativos. A algunos usuarios les interesa la privacidad que ofrece al alto nivel de anonimato de las operaciones con criptomonedas, mientras que otros simplemente quieren evitar que el Estado o los bancos controlen o supervisen sus operaciones legales[6]. Sus defensores señalan que las comisiones que se pagan por las operaciones con criptomonedas son inferiores a las que cobran los bancos tradicionales por las operaciones con monedas nacionales, si bien las pérdidas por diferencias cambiarias y las tarifas de los proveedores de servicios de criptomonedas pueden recortar los ahorros de costos[7]. En los lugares en que no operan los bancos tradicionales, las criptomonedas pueden desempeñar las funciones propias de los servicios de pago tradicionales[8]. Por último, el hecho de que las criptomonedas no sean monedas emitidas por Estados puede facilitar las operaciones transfronterizas[9].

7. No obstante, muchos de los países que permiten el funcionamiento de los mercados de criptomonedas han promulgado leyes para prevenir el blanqueo de dinero, la delincuencia organizada y la financiación del terrorismo[10], si bien, hasta la fecha, no parece que los terroristas estén usando las criptomonedas a gran escala[11]. Esta tendencia a la regulación ha surgido como reacción al uso frecuente de las criptomonedas para efectuar compras ilegales y en el mercado negro en línea[12] y como método de pago en casos de blanqueo de dinero, esquemas de Ponzi, extorsión, chantaje (amenaza de ataques distribuidos de denegación de servicio) y fraude.

8. Los mismos conceptos aplicables al blanqueo de dinero mediante efectivo pueden extrapolarse el blanqueo de dinero mediante criptomonedas[13]. Las operaciones de blanqueo mediante criptomonedas siguen un proceso similar al de las operaciones

---

[5] Sesha Kethineni y Yin Cao, "The rise in popularity of cryptocurrency and associated criminal activity", *International Criminal Justice Review*, 6 de febrero de 2019; Stearns Broadhead, "The contemporary cybercrime ecosystem: a multi-disciplinary overview of the state of affairs and developments", *Computer Law and Security Review*, vol. 34, núm. 6 (diciembre de 2018), págs. 1180 a 1196.

[6] Geoff Goodell y Tomaso Aste, "Can cryptocurrencies preserve privacy and comply with regulations?", *Frontiers in Blockchain*, vol. 2, art. 4 (mayo de 2019), págs. 1 a 20.

[7] Angela S. M. Irwin y Adam B. Turner, "Illicit Bitcoin transactions: challenges in getting to the who, what, when and where", *Journal of Money Laundering Control*, vol. 21, núm. 3 (julio de 2018), págs. 297 a 313.

[8] *Ibid*.

[9] Perri Reynolds y Angela S. M. Irwin, "Tracking digital footprints: anonymity within the bitcoin system", *Journal of Money Laundering Control*, vol. 20, núm. 2 (mayo de 2017), págs. 172 a 189.

[10] Estados Unidos, Biblioteca Jurídica del Congreso, Centro de Investigaciones Jurídicas Mundiales, *Regulation of Cryptocurrency around the World* (Washington D. C., 2018), junio de 2018.

[11] Cynthia Dion-Schwarz, David Manheim y Patrick B. Johnson, *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats* (Santa Mónica, California, RAND Corporation, 2019).

[12] Reynolds e Irwin, "Tracking digital footprints"; Monica J. Barratt, Jason A. Ferris y Adam R. Winstock, "Safer scoring? Cryptomarkets, social supply and drug market violence", *International Journal of Drug Policy*, vol. 35 (septiembre de 2016), págs. 24 a 31.

[13] Chad Albrecht *et al*., "The use of cryptocurrencies in the money laundering process", *Journal of Money Laundering Control*, vol. 22, núm. 2 (mayo de 2019), págs. 210 a 216; Rolf van Wegberg, Jan-Jaap Oerlemans y Oskar van Deventer, "Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin", J*ournal of Financial Crime*, vol. 25, núm. 2 (junio de 2018), págs. 419 a 435.

tradicionales, pero explotan la tecnología para blanquear dinero [14]. Además, las criptomonedas se pueden utilizar para facilitar la evasión de impuestos [15].

9. El robo de criptomonedas también suscita cada vez más preocupación[16], ya que sus usuarios pueden ser víctimas de estafas diseñadas para robar criptomonedas [17]. Además, los ataques con programas secuestradores (*ransomware*) contra particulares, empresas o Gobiernos a menudo recurren a la extorsión y exigen que el pago se efectúe en criptomonedas.

10. La delincuencia relacionada con las criptomonedas se facilita en aquellos entornos que no están suficientemente regulados en lo que respecta a la identificación de los usuarios o la imposición de sanciones y en los que se pueden explotar los vacíos legales. Las diferencias entre las normas sobre criptomonedas de los diferentes países permiten a los usuarios realizar en un país actividades que serían ilegales en otros [18].

11. Para evitar que las criptomonedas se utilicen con fines delictivos se deben estudiar y adoptar medidas de diversa índole. Por ejemplo, las medidas de desanonimización de las operaciones pueden reforzar las funciones de disuasión e investigación. Entre estas figuran el establecimiento de normas que exijan datos que permitan identificar al autor de la operación ("conozca a su cliente")[19] o el análisis de las operaciones mediante técnicas de aprendizaje automático u otras técnicas de vigilancia para detectar operaciones ilegales[20].

12. Los escasos conocimientos y competencias técnicas para detectar o investigar con eficacia los fraudes con criptomonedas allanan el camino para que se multipliquen las oportunidades de utilizar las criptomonedas para llevar a cabo actividades ilícitas [21]. Las iniciativas que, como las emprendidas por las Naciones Unidas, tienen por objeto capacitar a los investigadores encargados de perseguir los delitos que se cometen con criptomonedas contribuyen a la prevención y detección de dichas actividades [22].

13. Los emisores de criptomonedas, los organismos reguladores y las autoridades encargadas de hacer cumplir la ley son agentes clave en la lucha contra la utilización de las criptomonedas para facilitar la comisión de delitos. Es importante establecer un conjunto bien articulado de técnicas de prevención e investigación que pueda adaptarse a los cambios tecnológicos y a las diversas aplicaciones de las criptomonedas a fin de minimizar las amenazas que plantea su utilización indebida con fines delictivos.

---

[14] Denis B. Desmond, David Lacey y Paul Salmon, "Evaluating cryptocurrency laundering as a complex socio-technical system: a systematic literature review", *Journal of Money Laundering Control*, vol. 22, núm. 3 (julio de 2019), págs. 480 a 497.

[15] Albrecht *et al*., "The use of cryptocurrencies in the money laundering process"; Saman Jafari *et al*., "Cryptocurrency: a challenge to legal system", 10 de mayo de 2018.

[16] Garrick Hileman y Michel Rauchs, *Global Cryptocurrency Benchmarking Study* (Cambridge, Reino Unido de Gran Bretaña e Irlanda del Norte, Cambridge Centre for Alternative Finance, 2017).

[17] Desmond *et al*., "Evaluating cryptocurrency laundering as a complex socio-technical system".

[18] Angela S. M. Irwin y Caitlin Dawson, "Following the cyber money trail: global challenges when investigating ransomware attacks and how regulation can help", *Journal of Money Laundering Control*, vol. 22, núm. 1 (enero de 2019), págs. 110 a 131.

[19] Grupo de Acción Financiera, *Estándares Internacionales sobre la Lucha contra el Lavado de Activos y el Financiamiento del Terrorismo y la Proliferación* (París, 2012).

[20] Irwin y Turner, "Illicit Bitcoin transactions"; Goodell y Aste, "Can cryptocurrencies preserve privacy and comply with regulations?".

[21] Sesha Kethineni, Yin Cao y Cassandra Dodge, "Use of Bitcoin in darknet markets: examining facilitative factors on Bitcoin-related crimes", *American Journal of Criminal Justice*, vol. 43, núm. 2 (junio de 2018), págs. 141 a 157.

[22] Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), "UNODC launches training to tackle cryptocurrency-enabled organized crime", 8 de mayo de 2017.

B. La tecnología y los mercados en la web oscura, incluidos los mercados de drogas

14. Internet ofrece nuevas oportunidades para la compraventa ilícita de bienes, tanto en la web visible como en la oscura. A diferencia de la web visible (también conocida como "web de superficie"), que se refiere a la información de acceso público e indexada por buscadores comunes, la web oscura (o "redes oscuras", términos que en lo sucesivo se utilizarán indistintamente) está compuesta por redes encriptadas que permiten tanto a los titulares de los sitios web como a los usuarios permanecer relativamente anónimos e ilocalizables[23].

15. Los mercados de la web oscura (también denominados "criptomercados")[24] ofrecen anonimato a compradores y vendedores por igual y en ellos se utilizan principalmente las criptomonedas como medio de pago para facilitar las operaciones de compraventa de artículos como armas y drogas ilícitas.

16. Según la Agencia de la Unión Europea para la Cooperación Policial (Europol), los datos personales, médicos y financieros vulnerables son un bien muy preciado en los mercados de las redes oscuras y desempeñan un papel crucial en actividades como el fraude, los ataques de *phishing*, el robo de identidad y la apropiación de cuentas. No obstante, si bien en los mercados de la web oscura se ponen a la venta diversos bienes falsificados y pirateados, la mayoría de las operaciones comerciales ilícitas se siguen realizando en la web visible[25]. En la web oscura se recurre cada vez más al amaño de partidos y las apuestas para blanquear dinero, especialmente los grupos delictivos organizados transnacionales[26]. En la Reunión Preparatoria Regional de Europa para el 14º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal también se habló de la necesidad de hacer frente al uso de las redes oscuras para cometer delitos de odio[27].

17. En lo que respecta a las drogas, en el *Informe mundial sobre las drogas 2019* se afirma que las compras de drogas en la web oscura iban en aumento a largo plazo, si bien podrían haber disminuido de 2018 a 2019. De los datos de la Encuesta Mundial sobre Drogas (Global Drug Survey) de 2019 se desprende que la compra de drogas en la web oscura seguía siendo un fenómeno muy reciente y que el 48 % de las personas que habían adquirido drogas por esa vía en 2019 solo llevaban dos años utilizando la web oscura con ese fin y el 29 % había comenzado a hacerlo en los dos años anteriores[28].

18. Los mercados de la web oscura podrían tener capacidad para cambiar los hábitos y la prevalencia del consumo de drogas[29], ya que pueden reducir algunos de los riesgos a que se exponen los compradores y vendedores, como la posibilidad de sufrir encuentros violentos en los barrios en que se venden drogas[30], la coacción y la

[23] Darren Guccione, "What is the dark web? How to access it and what you'll find", *The State of Cybersecurity*, 4 de julio de 2019.

[24] Julian Broseus *et al.*, "Studying illicit drug trafficking on Darknet markets: structure and organization from a Canadian perspective", *Forensic Science International*, vol. 264, 5 de marzo de 2016, pág. 7.

[25] Agencia de la Unión Europea para la Cooperación Policial (Europol), Centro Europeo contra la Ciberdelincuencia, *Internet Organised Crime Threat Assessment (IOCTA) 2018* (La Haya, 2018), pág. 49.

[26] Robin Cartwright y France Cleland Bones, *Transnational Organized Crime and the Impact on the Private Sector: The Hidden Battalions* (Ginebra, Global Initiative against Transnational Organized Crime, 2017), pág. 29.

[27] Véase A/CONF.234/RPM.5/1, párr. 36 g).

[28] *Informe mundial sobre las drogas 2019*: *Panorama mundial de la demanda y la oferta de drogas* (publicación de las Naciones Unidas, núm. de venta E.19.XI.8 (fascículo 2)).

[29] Judith Aldridge y David Décary-Hétu, "Hidden wholesale: the drug diffusing capacity of online drug cryptomarkets", *International Journal of Drug Policy*, vol. 35, septiembre de 2016, pág. 12.

[30] Julia Buxton y Tim Bingham, *The Rise and Challenge of Dark Net Drug Markets*, informe de políticas núm. 7 (Swansea, Reino Unido, Observatorio Global de Políticas de Drogas, enero de 2015), págs. 1 a 24.

detención[31]. No obstante, las ventas de drogas facilitadas por Internet conllevan sus propios riesgos y es probable que estos sean mayores durante las actividades "fuera de línea" conexas[32]. Las ventas de drogas por Internet también podrían guardar relación con el aumento de las sobredosis, en cuanto que facilitan la experimentación y aumentan la disponibilidad de drogas de gran potencia[33].

19. Se han llevado a cabo con notable éxito varias operaciones de desmantelamiento de grandes mercados de la web oscura. No obstante, según Europol, los delincuentes están explorando otros medios para eludir la actuación de las fuerzas del orden. Se ha observado una nueva tendencia consistente en la aparición de modelos empresariales en que los delincuentes utilizan múltiples identidades mediante múltiples perfiles en diferentes plataformas en línea, lo cual, a su vez, facilita las operaciones de varias personas en lugar de una sola[34].

20. Las investigaciones en la web oscura conllevan varias dificultades. Uno de los principales problemas es el hecho de que la información en la web oscura no está indexada y, por consiguiente, los investigadores no pueden localizarla con facilidad usando buscadores o palabras clave. Además, los delincuentes albergan sus servidores en plataformas descentralizadas, lo que da lugar a una proliferación de servicios que pueden ser más difíciles de detectar[35].

21. Por otra parte, hay oportunidades para que las fuerzas del orden vigilen los mercados en la web oscura y realicen investigaciones en línea[36]. En este contexto se dispone de diversas herramientas que pueden ofrecer soluciones, como los exploradores web que pueden utilizarse para automatizar la indexación de datos en línea de manera periódica, las herramientas de minería de datos para realizar búsquedas en grandes conjuntos de datos, las herramientas de análisis de criptomonedas para localizar vías de pago y *software* de cadenas de bloques utilizado para rastrear pruebas[37]. La asistencia técnica es importante y la UNODC ha organizado actividades de capacitación centradas en las técnicas de investigación en la web oscura.

C. Armas de fuego: amenazas contra la seguridad relacionadas con la tecnología

1. Utilización de tecnopolímeros para fabricar de armas

22. Es probable que los polímeros industriales asuman un papel cada vez más destacado en la industria armamentística, lo que dificultaría la aplicación efectiva de las disposiciones sobre localización y registros de armas del Protocolo contra la Fabricación y el Tráfico Ilícitos de Armas de Fuego, sus Piezas y Componentes y Municiones, que complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional. La aparición de los polímeros industriales hace que peligre la capacidad

[31] Buxton y Bingham, *The Rise and Challenge of Dark Net Drug Markets*. Véase también David Décary-Hétu, Masarah Paquet-Clouston y Judith Aldridge, "Going international? Risk taking by cryptomarket drug vendors", *International Journal of Drug Policy*, vol. 35, septiembre de 2016, pág. 71.

[32] Judith Aldridge y Rebecca Askew, "Delivery dilemmas: how drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement", *International Journal of Drug Policy*, vol. 41, marzo de 2017, págs. 101 a 109.

[33] Nathaniel Popper, "Opioid dealers embrace the dark web to send deadly drugs by mail", *New York Times*, 10 de junio de 2017.

[34] Europol, Centro Europeo contra la Ciberdelincuencia, *Internet Organised Crime Threat Assessment (IOCTA) 2019* (La Haya, 2019), pág. 45.

[35] Organización Internacional de Policía Criminal (INTERPOL) "Innovation report: anonymous networks and darknet" (septiembre de 2018), págs. 12 y 13.

[36] Observatorio Europeo de las Drogas y las Toxicomanías y Europol, *Drugs and the Darknet: Perspectives for Enforcement, Research and Policy* (Luxemburgo, 2017), págs. 60 y siguientes.

[37] INTERPOL, "Innovation report", pág. 14. Véase también Shira Stein, "Law enforcement adapts to using cryptocurrency to catch criminals", *Securities Regulation and Law Report*, 49 SRLR 1029 (Arlington, Virginia, Bureau of National Affairs, 2017).

de las autoridades competentes para detectar, investigar y enjuiciar adecuadamente los delitos relacionados con las armas.

23. El Compendio de Módulos sobre la Ejecución del Control de Armas Pequeñas (MOSAIC) —en el que se recopilan buenas prácticas no vinculantes para el control de las armas pequeñas basadas en los instrumentos internacionales pertinentes, a saber, el Protocolo sobre Armas de Fuego, el Programa de Acción sobre las Armas Pequeñas y el Instrumento Internacional de Localización conexo y el Tratado sobre el Comercio de Armas—, puede ayudar a los países a hacer frente a las dificultades que se plantean cuando se utilizan polímeros para fabricar las cajas o los cajones de los mecanismos de las armas de fuego.

2. Armas modulares

24. Las nuevas tecnologías y los vacíos legales han dado lugar a la llegada en masa a los mercados, tanto a los lícitos como a los ilícitos, de kits de modificación, conversión y fabricación con que los propietarios de armas que tengan unos conocimientos técnicos básicos pueden transformar sus armas de fuego o incluso fabricar armas completamente funcionales.

25. El Protocolo sobre Armas de Fuego se aplica a las "piezas y componentes", pero los requisitos relativos a las marcas (artículo 8) se aplican solo a las armas de fuego. Esto puede ser especialmente problemático en el caso de las armas modulares[38]. Para solventar este problema es necesario adoptar medidas como las siguientes: designar un componente de control para todas las armas de fuego, sean normales o modulares, a efectos de marcación, registro y localización; determinar qué información debe marcarse en dicho elemento de control para evitar la duplicación de números de serie; y proporcionar orientaciones sobre la identificación única a efectos de localización en particular para las armas modulares[39].

3. Fabricación aditiva (impresión 3D)

26. La fabricación aditiva, que en el lenguaje coloquial se conoce como "impresión tridimensional" o "impresión 3D", es una tecnología emergente con posibles consecuencias para la seguridad local, nacional e internacional a corto y largo plazo. La aparición y expansión de la fabricación aditiva podría acelerar considerablemente la proliferación de armas y podría tener dramáticas consecuencias en lo que respecta a la delincuencia habitual. Además, las armas fabricadas mediante tecnología de impresión 3D podrían restar eficacia a los programas de registro y concesión de licencias de armas de fuego y las bases de datos de balística utilizadas en las investigaciones policiales.

27. El artículo 3 d) y el artículo 5, párrafo 1 a), del Protocolo sobre Armas de Fuego, relativos a la fabricación ilícita de armas de fuego, serían aplicables a las armas de fuego fabricadas mediante tecnología de impresión 3D del mismo modo que se aplican a las armas de fuego de fabricación tradicional. No obstante, la descarga de archivos digitales para la impresión 3D de armas de fuego parecería quedar fuera del ámbito de aplicación del Protocolo, situación que exige medidas legislativas urgentes.

28. Muchas de las leyes en vigor y muchos de los delitos que atañen a la fabricación, creación y posesión de armas de fuego sin licencia abarcan las armas de fuego impresas mediante tecnología 3D, aunque no necesariamente la posesión o distribución de los archivos de diseño[40]. Sería necesario que las leyes relativas a la fabricación ilícita de armas de fuego definieran la responsabilidad de los terceros que pongan el instrumental

[38] Giacomo Persi Paoli, "From firearms to weapon systems: challenges and implications of modular design for marking, record-keeping, and tracing", publicado en *Behind the Curve: New Technologies, New Control Challenges*, documento ocasional de Small Arms Survey, núm. 32, Benjamin King and Glenn McDonald, coords. (Ginebra, Small Arms Survey, 2015), pág. 23.

[39] *Ibid*, pág. 40.

[40] Documento de INTERPOL sobre innovación, "3D and 4D printing", Complejo Mundial de INTERPOL para la Innovación, 2018, pág. 6.

necesario a disposición de personas que desean fabricar armas de fuego mediante técnicas de fabricación aditiva[41].

29. Todo enfoque normativo amplio tendría que incluir a los agentes nacionales e internacionales, así como a los sectores público y privado. El posible uso dual de la fabricación aditiva hace que sea imposible frenar la expansión de esta tecnología sin recortar también sus muchos beneficios[42]. Al igual que sucede con cualquier otra tecnología emergente, será importante adoptar medidas para capacitar y formar al personal de las fuerzas del orden.

4. Tráfico de armas de fuego en la web oscura

30. La web oscura puede llegar a convertirse en el foro predilecto de los grupos delictivos organizados y las personas que desean adquirir armas de fuego de forma anónima o con fines ilegales[43]. En un estudio presentado por la Oficina de Asuntos de Desarme de las Naciones Unidas a la Primera Comisión de la Asamblea General en 2018, elaborado en el marco de un proyecto de investigación más amplio dirigido por RAND Europe en 2017[44], se puso de relieve la necesidad urgente de renovar la cooperación internacional para combatir las ventas ilícitas de armas facilitadas por el anonimato de la web oscura[45].

31. La proporción de ventas de armas que tienen lugar en la web oscura parecería ser menor que la de otros artículos ilícitos[46]. Un estudio reciente centrado únicamente en los listados de la web oscura relacionados con las armas reveló que estos eran los más comunes y constituían el 42 % de todos los listados publicados en la web oscura, seguidos de los listados de productos relacionados con las armas, digitales (27 %) o de otro tipo, como la munición (22 %)[47].

32. Para comprender el volumen y el alcance del comercio ilícito de armas en la web oscura es esencial entender mejor la gravedad de esa amenaza y lo que implica para las fuerzas del orden. A nivel nacional, los encargados de formular políticas deben garantizar que las fuerzas del orden cuenten con el personal, la capacitación y el equipo adecuados para hacer frente a esa actividad. Los marcos jurídicos en vigor, en particular la Convención contra la Delincuencia Organizada y su Protocolo sobre Armas de Fuego, pueden servir de base para adoptar enfoques amplios para hacer frente a ese fenómeno. Es preciso analizar en profundidad las normas vigentes sobre corretaje, que dimanan del Protocolo sobre Armas de Fuego (artículo 15) y del Tratado sobre el Comercio de Armas (artículo 10), para determinar si serían aplicables[48].

---

[41] N. R. Jenzen-Jones, “Small arms and additive manufacturing: An assessment of 3D-printed firearms, components, and accessories”, publicado en *Behind the Curve: New Technologies, New Control Challenges*, documento ocasional de Small Arms Survey, núm. 32, Benjamin King y Glenn McDonald, coords. (Ginebra, Small Arms Survey, 2015), págs. 63 y 64.

[42] Trevor Johnston, Troy D. Smith y J. Luke Irwin, “Additive manufacturing in 2040: powerful enabler, disruptive threat”, documento núm. PE-283-RC (Santa Mónica, California, RAND Corporation, 2018), pág. 17.

[43] RAND Europe, “International arms trade on the dark web” (2019), sección de conclusiones, párr. 8.

[44] Giacomo Persi Paoli *et al.*, *Behind the Curtain: The Illicit Trade of Firearms, Explosives and Ammunition on the Dark Web* (Santa Mónica, California, RAND Corporation, 2017).

[45] Giacomo Persi Paoli, *The Trade in Small Arms and Light Weapons on the Dark Web*, Oficina de Asuntos de Desarme de las Naciones Unidas (UNODA), *Documentos Ocasionales*, núm. 32 (publicación de las Naciones Unidas, núm. de venta E.19.XI.1), pág. ix.

[46] Damien Rhumorbarbe *et al.*, “Characterising the online weapons trafficking on cryptomarkets”, *Forensic Science International*, vol. 283, diciembre de 2018, págs. 16 a 20.

[47] RAND Europe, “International arms trade on the dark web” (2019), sección de conclusiones, párr. 4.

[48] Simonetta Grassi y Mareike Buettner, “Overview of international legal instruments and their applicability to illicit firearms trafficking on the dark web” (anexo), publicado en Paoli *et al.*, *Behind the Curtain*, pág. 101.

5. Armas autónomas letales

33. Si bien no se ha reconocido oficialmente la existencia de armas plenamente autónomas, la idea de utilizar la inteligencia artificial para controlar esas armas ha suscitado intensos debates. En 2016, la Quinta Conferencia de Examen de las Altas Partes Contratantes en la Convención sobre Prohibiciones o Restricciones del Empleo de Ciertas Armas Convencionales que Puedan Considerarse Excesivamente Nocivas o de Efectos Indiscriminados estableció el Grupo de Expertos Gubernamentales sobre las Tecnologías Emergentes en el Ámbito de los Sistemas de Armas Autónomos Letales. En su período de sesiones de 2019, el Grupo recomendó que las Altas Partes Contratantes hicieran suyos los principios rectores establecidos por el Grupo[49].

D. Trata de personas

34. Las investigaciones realizadas en los últimos años y las pruebas directas han puesto de manifiesto que los tratantes de personas están utilizando la tecnología en todas las etapas del delito, como la captación, el control y la explotación de las víctimas.

35. Uno de los motivos por que los traficantes utilizan la tecnología es porque les permite actuar de manera anónima y ocultar su identidad. Además, las criptomonedas permiten a los traficantes realizar operaciones financieras y mover activos de origen delictivo al amparo del anonimato. Otro motivo es que la tecnología facilita la captación y explotación de las víctimas por los tratantes. La trata de seres humanos utiliza conductos como los anuncios clasificados en línea y las redes sociales[50].

36. Además, el uso indebido de la tecnología puede hacer que resulte más fácil para los tratantes entablar relaciones con los usuarios, adentrarse en nuevos mercados y ampliar sus operaciones delictivas. Los tratantes pueden usar las emisiones en directo para llegar a un mercado más amplio de clientes que podrían no llegar a tener contacto físico con la víctima[51].

37. Además, el uso indebido de las tecnologías puede ayudar a los tratantes a controlar y coaccionar a las víctimas. Los traficantes podrían recurrir al seguimiento de la ubicación para facilitar la explotación de las víctimas. Aun si las víctimas logran escaparse, los tratantes pueden dar con su paradero mediante dispositivos de seguimiento instalados en los teléfonos celulares de las víctimas.

38. Las fuerzas del orden, por su parte, también utilizan dispositivos de seguimiento para detectar la ubicación de los supuestos tratantes o de otras personas involucradas en redes de trata. La utilización de los datos de seguimiento de la ubicación de las víctimas es la otra cara de la misma moneda, dado que las víctimas pueden ser consideradas “bases de datos de pruebas andantes”[52].

39. El uso de intervenciones tecnológicas en la lucha contra la trata exige una colaboración intersectorial. La industria de las tecnologías de la información y las comunicaciones y las organizaciones internacionales se han aliado para estudiar cómo aprovechar las tecnologías para prevenir la trata de personas y apoyar la rehabilitación de las víctimas. Tech Against Trafficking, coalición integrada por empresas tecnológicas líderes, instituciones académicas y la Organización Internacional para las Migraciones, proporciona una lista de soluciones tecnológicas utilizadas para combatir la trata[53].

---

[49] CCW/GGE.1/2019/3, anexo IV.

[50] Mark Latonero, “Human Trafficking Online: The Role of Social Networking Sites and Online Classifieds”, *Research Series* (Universidad del Sur de California, Centro de Políticas y Liderazgo en materia de Comunicación, Los Ángeles, septiembre de 2011), pág. 8.

[51] Grupo Interinstitucional de Coordinación contra la Trata de Personas, “Human trafficking and technology: trends, challenges and opportunities”, boletín informativo núm. 7 (2019), págs. 1 y 2.

[52] Felicity Gerry, Julia Muraszkiewicz y Niovi Vavoula, “The role of technology in the fight against human trafficking: reflections on privacy and data protection concerns”, *Computer Law and Security Review*, vol. 32, núm. 2 (abril de 2016), págs. 210 y 211.

[53] Business for Social Responsibility, “List of technology tools and initiatives identified by tech against trafficking”, 15 de enero de 2019.

40. Para afrontar los retos que plantea la utilización de la tecnología en la trata de personas es esencial capacitar a todos los agentes implicados en la lucha contra esa actividad delictiva. Es preciso reflexionar detenidamente sobre la elaboración, el uso, el mantenimiento, el seguimiento y la evaluación de la tecnología utilizada por los profesionales para combatir la trata de personas[54]. No obstante, quienes desarrollan las herramientas necesarias deben tener presentes las diferencias que existen entre los usuarios en riesgo y darles cabida[55].

E. Tráfico ilícito de migrantes

41. Las tecnologías de la información y las comunicaciones se han convertido en una importante herramienta muy utilizada para transmitir información sobre rutas, servicios y precios, tanto por los migrantes como por quienes los captan[56]. Además, los medios sociales han aumentado la capacidad de los traficantes para modificar las rutas en función de las respuestas de las fuerzas del orden de los países de tránsito, lo que ha incrementado la eficacia de las operaciones de tráfico y obstaculizado la investigación y el enjuiciamiento de esos delitos[57].

42. La rápida evolución de la tecnología móvil puede influir en la relación entre migrantes y traficantes. En varios grupos de Facebook, los migrantes pueden comprobar la fiabilidad de determinados traficantes e intercambiar información sobre a quién conviene contratar. Esto se ha descrito como una "jerarquía de fiabilidad"[58].

43. Las tecnologías también se pueden utilizar para efectuar pagos, ya que los pagos a los traficantes se hacen mayormente a través de plataformas de pago en línea. Las criptomonedas pueden ayudar a los traficantes a recibir, ocultar y mover el dinero con más facilidad. Ese tipo de monedas puede propiciar el blanqueo y ayudar a los traficantes a eludir las investigaciones y la detención, ya que preserva el anonimato de los usuarios y hace que sea innecesario llevar encima grandes sumas de efectivo.

44. La tecnología también desempeña un papel esencial en lo que respecta a los documentos de viaje o de identidad fraudulentos que facilitan el tráfico ilícito de migrantes. Para crear, alterar o copiar pasaportes de forma fraudulenta se utiliza equipo de diversa índole. En algunos casos se han utilizado herramientas tecnológicamente avanzadas para crear falsificaciones de pasaportes de gran calidad que a simple vista son idénticos a los originales[59].

45. No obstante, las innovaciones tecnológicas pueden considerarse desde diversos puntos de vista y no solo desde la perspectiva de los beneficios que obtienen los traficantes. La digitalización reduce las lagunas de información que explotan los traficantes en beneficio propio. Es posible utilizar Internet para ayudar a los migrantes a entrar en contacto con redes sociales de apoyo e información. Una tendencia que se está perfilando recientemente a raíz de un cambio propiciado por la tecnología es el hecho de que cada vez son más los migrantes que emprenden el proceso de migración

[54] Grupo Interinstitucional de Coordinación contra la Trata de Personas, "Human trafficking and technology", pág. 4.

[55] Véase Mark Latonero, Bronwyn Wex y Meredith Dank, T*echnology and Labor Trafficking in a Networked Society: General Overview, Emerging Innovations, and Philippines Case Study* (Universidad del Sur de California, Centro Annenberg de Políticas y Liderazgo en materia de Comunicación, Los Ángeles, 2015), pág. 11.

[56] Europol e INTERPOL, "Migrant smuggling networks: executive summary" (mayo de 2016), pág. 8.

[57] CTOC/COP/WG.7/2018/2, párr. 25.

[58] Judith Zijlstra e Ilse van Liempt, "Smart(phone) travelling: understanding the use and impact of mobile technology on irregular migration journeys", *International Journal of Migration and Border Studies*, vol. 3, núms. 2 y 3 (marzo de 2017), págs. 176 a 177.

[59] Oficina Regional de la UNODC para Asia Sudoriental y el Pacífico, *Facilitators of Smuggling of Migrants in Southeast Asia: Fraudulent Documents, Money Laundering, and Corruption* (Bangkok, 2019), pág. 26.

de manera autosuficiente y que dependen en menor medida de los traficantes. Eso les da mayor autonomía y reduce su vulnerabilidad a la explotación[60].

46. El uso que los migrantes hacen de los medios sociales difiere en función de su nacionalidad, etnia, región de procedencia y formación académica, así como del acceso a Internet de que dispongan[61]. Se ha demostrado que existe una brecha digital entre los grupos de migrantes causada por las desigualdades en cuanto al acceso físico a la tecnología digital y la utilización de esta, las competencias técnicas necesarias para utilizar las diferentes tecnologías de manera eficaz y la capacidad para pagar esos servicios[62].

47. Desde la perspectiva del cumplimiento de ley, hay un interés cada vez mayor en encontrar el modo de explotar la tecnología para desmantelar las redes de tráfico ilícito de migrantes. Además, el uso de pruebas obtenidas en los medios sociales o mediante el uso de la tecnología puede servir para respaldar las declaraciones de los migrantes objeto de tráfico en los procesos penales pertinentes.

48. El uso adecuado de la tecnología ayuda a los Gobiernos, el sector privado y las organizaciones no gubernamentales a prevenir y mitigar el tráfico de migrantes en sus respectivos ámbitos de competencia. Por lo tanto, es indispensable aumentar la eficacia de las medidas de justicia penal y crear incentivos y alianzas con los proveedores de servicios en línea a fin de mejorar la vigilancia, detección y denuncia de los contenidos relacionados con el tráfico ilícito.

F. Explotación y abusos sexuales de niños, niñas y adolescentes en línea

49. Si bien el abuso y la explotación sexuales de niños, niñas y adolescentes ya ocurrían antes de la llegada de Internet, la dimensión digital que han adquirido estos delitos permite a los autores interactuar y obtener imágenes de explotación sexual de niños, niñas y adolescentes en línea. Además, el hecho de que los niños y niñas acceden a Internet a edades cada vez más tempranas brinda a los delincuentes la oportunidad de entablar contacto con ellos más fácilmente, en comparación con el entorno fuera de línea, y eso, a su vez, ha influido considerablemente en el *modus operandi* de esos delitos.

50. Los avances tecnológicos se han hecho indispensables para la explotación sexual de niños, niñas y adolescentes con fines comerciales. Los turistas sexuales que buscan el contacto con niños, niñas y adolescentes pueden valerse de la computación en la nube para almacenar imágenes y vídeos y, de ese modo, evitar los riesgos que conlleva el transporte físico de imágenes de explotación sexual de niños, niñas y adolescentes. Asimismo, la tecnología de telefonía móvil conecta a los organizadores, las víctimas y los consumidores de imágenes de explotación y abusos sexuales de niños, niñas y adolescentes, por lo que se reduce la necesidad de que los productores y distribuidores estén presentes durante las transacciones, lo que a su vez los protege mejor de la detección.

51. Entre las principales formas de explotación y abusos sexuales de niños, niñas y adolescentes facilitadas por las tecnologías de la información y las comunicaciones figuran la exposición a la pornografía, el ciberacoso con fines sexuales y las provocaciones sexuales en línea no deseadas, y en muchos de esos actos de explotación están presentes actividades sexuales inapropiadas con niños, niñas y adolescentes. La UNODC llevó a cabo un estudio sobre el tema en el que se ponen de relieve algunas

[60] UNODC, Declaración de Doha, Educación Superior, Serie de Módulos Universitarios, Trata de Personas y Tráfico Ilícito de Migrantes, "Módulo 14: Vinculaciones entre la ciberdelincuencia, el tráfico ilícito de migrantes y la trata de personas". Puede consultarse en www.unodc.org/e4j/index.html.

[61] Comisión Europea, "The use of social media in the fight against migrant smuggling", estudio de la Red Europea de Migración (REM) (septiembre de 2016).

[62] Alam Khorshed y Sophia Imran, "The digital divide and social inclusion among refugee migrants: a case in regional Australia", *Information Technology and People*, vol. 28, núm. 2 (junio de 2015), pág. 344 y siguientes.

formas nuevas de explotación y abusos sexuales, como el contenido generado por usuarios, el contenido autogenerado, como el sexteo, la transmisión de abusos sexuales en directo y las imágenes de abusos sexuales de niños, niñas y adolescentes preparadas por encargo[63].

52. Según Europol, la transmisión de abusos sexuales en directo se ha convertido en una amenaza muy presente. La transmisión se realiza a través de aplicaciones de medios sociales, aplicaciones de videochat, plataformas de juego y salas de chateo en línea y, además, parecería estar trasladándose de los ordenadores a los teléfonos inteligentes y las tabletas, y de Internet por cable a wifi e Internet móvil[64].

53. Una de las amenazas más importantes de la distribución en línea de imágenes de explotación sexual de niños, niñas y adolescentes es el continuo aumento de la utilización de la web oscura. Según Internet Watch Foundation, los sitios web encubiertos que utilizan un "itinerario digital" que parte de otros sitios web para ocultar las imágenes de abusos sexuales siguen constituyendo un grave problema. Asimismo, según ha podido constatar esta organización, en los últimos años se ha registrado un aumento constante de las direcciones web en que se muestran abusos sexuales de niños, niñas y adolescentes, de 68.092 en 2015 a 105.047 en 2018[65].

54. También suscita preocupación el hecho de que los autores de abusos a niños, niñas y adolescentes en línea tienen cada vez más conocimientos tecnológicos, por lo que seguirán tratando de encontrar nuevas vías para evitar ser detectados. Gracias a la utilización de aplicaciones de mensajería móvil con cifrado de extremo a extremo, los pequeños grupos de usuarios han comenzado a desplazar a los grandes foros.

55. Varios países carecen de disposiciones legales para regular las formas emergentes de abusos a niños, niñas y adolescentes y las diferencias entre las leyes que protegen a los menores y definen la edad de consentimiento plantean problemas importantes y reducen la probabilidad de detectar, investigar y enjuiciar con éxito los abusos.

56. La tecnología también puede proporcionar a las fuerzas del orden medios para combatir estos problemas[66]. La innovación en métodos y técnicas como la minería y el análisis de datos mejoran los procesos forenses para que las investigaciones avancen. Las técnicas basadas en la tecnología de la información deberían aplicarse respetando los límites de la protección de los derechos humanos debido al carácter traumático de la explotación sexual de niños, niñas y adolescentes y a la edad de los testigos y su vulnerabilidad.

57. Se han creado bases de datos en las que se cargan imágenes de abusos sexuales de niños, niñas y adolescentes con fines de investigación, como la base de datos internacional sobre explotación sexual de menores de la Organización Internacional de Policía Criminal. En los Estados Unidos de América, la base de datos del Centro Nacional para Menores Desaparecidos y Explotados se utiliza como archivo central de imágenes de abusos sexuales de niños, niñas y adolescentes[67].

58. Los esfuerzos encaminados a combatir con eficacia la explotación y los abusos de niños, niñas y adolescentes facilitados por la tecnología de la información y las comunicaciones exigen la adopción de un enfoque de múltiples interesados que incluya e implique de forma activa a los niños, las familias, las comunidades, los Gobiernos, la sociedad civil y el sector privado[68].

---

[63] UNODC, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children* (Viena, 2015), págs. 21 y siguientes.

[64] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2018*, pág. 35.

[65] Internet Watch Foundation, *Once Upon a Year* (Cambridge (Reino Unido), 2018), págs. 19 y 43.

[66] Victoria Brains, "Online child sexual exploitation: towards an optimal international response", *SSRN Electronic Journal*, 29 de agosto de 2018.

[67] UNODC, Declaración de Doha, Educación Superior, Serie de Módulos Universitarios, Ciberdelincuencia, "Módulo 12: Ciberdelitos interpersonales: explotación y abusos sexuales de niños en línea". Puede consultarse en www.unodc.org/e4j/index.html.

[68] UNODC, *Study on the Effects of New Information Technologies.*

G. Inteligencia artificial y robótica

59. Después de que Internet y la tecnología móvil impulsaran la “tercera revolución industrial”, las tecnologías de inteligencia artificial, alimentadas por la inteligencia de datos, están impulsando la “cuarta revolución industrial”[69]. Esto puede ser positivo para el desarrollo mundial y el cambio social, además de contribuir al logro de los Objetivos de Desarrollo Sostenible, pero también da lugar a inquietudes y a retos de carácter jurídico, ético y social. En lo que respecta al cumplimiento de la ley, los avances de la inteligencia artificial pueden brindar tanto oportunidades como riesgos, por lo que es preciso adoptar un enfoque estratégico y no escatimar en esfuerzos y recursos[70].

60. En casi todas las reuniones preparatorias del 14º Congreso se puso de relieve la necesidad e importancia de estudiar el modo de lograr que los profesionales de la justicia penal y las fuerzas del orden pudieran utilizar y sacar el máximo partido de las tecnologías en evolución, como la inteligencia artificial y las tecnologías de la información y las comunicaciones, incluida la inteligencia de datos, en la lucha contra la delincuencia[71].

61. Se están celebrando debates en relación con, entre otras cosas, el uso de la inteligencia artificial para realizar autopsias virtuales, los sistemas de predicción de delitos para ayudar a la policía a optimizar recursos, las herramientas de detección conductual, las técnicas de rastreo basadas en cadenas de bloques que respetan la privacidad y los vehículos de patrulla autónomos[72]. Cada vez son más las fuerzas del orden que, alentadas por los avances en inteligencia artificial que han hecho la robótica más “inteligente” y capaz de reemplazar a los seres humanos en muchas funciones y tareas, incorporan esos avances tecnológicos en varias de sus operaciones. El grado de utilización de la robótica dista de ser homogéneo, ya que algunos países están más avanzados en lo que respecta a la investigación y el uso de esas tecnologías[73].

62. La inteligencia artificial y el aprendizaje automático parecen proporcionar un escudo cada vez más eficaz contra el blanqueo de dinero. Al igual que los algoritmos que ayudan a los minoristas en línea a seleccionar posibles clientes, la inteligencia artificial y el aprendizaje automático pueden servir de base para formular políticas de diligencia debida mejor informadas y más precisas mediante la interpretación de los indicios de actividad delictiva y el análisis de cantidades de datos mucho mayores, y hacerlo de manera más fiable. Además, las plataformas de medios sociales están empleando cada vez más el aprendizaje automático para bloquear contenidos ilícitos y noticias falsas. Las empresas están utilizando la inteligencia artificial para reforzar la gestión de riesgos y la capacidad de respuesta al fraude a fin de predecir posibles delitos y prevenirlos.

---

[69] Victor Mayer-Schönberger y Kenneth Cukier, *Big Data: A Revolution that Will Transform How We Live Work and Think* (Londres, John Murray, 2013).

[70] El Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia (UNICRI) ha establecido un Centro de Inteligencia Artificial y Robótica en La Haya que servirá como centro internacional de recursos sobre cuestiones relativas a la inteligencia artificial y la robótica.

[71] Véase A/CONF.234/RPM.1/1, párr. 61 j). Véase A/CONF.234/RPM.2/1, párr. 79 k). Véase A/CONF.234/RPM.3/1, párr. 56 f). Véase A/CONF.234/RPM.4/1, párr. 57 e).

[72] INTERPOL y UNICRI, “Artificial intelligence and robotics for law enforcement” (Turín, Italia, 2019), pág. v.

[73] *Ibid.*, pág. 6.

63. No obstante, la inteligencia artificial es en gran medida un arma de doble filo, ya que puede propiciar grandes cambios en el modo en que las fuerzas del orden abordan la actuación policial, pero también mejora los *modus operandi* de los grupos delictivos y terroristas e incluso puede dar lugar a la aparición de nuevas formas de delincuencia[74]. En estas circunstancias, que bien podrían describirse como "la supervivencia del más apto", la prioridad puede resumirse como sigue: promover la actuación policial facilitada por la inteligencia artificial para combatir los delitos facilitados por la inteligencia artificial[75].

H. La cooperación internacional en asuntos penales y el uso de la tecnología

64. Un tema que sigue siendo objeto de debate en el ámbito de la cooperación internacional en asuntos penales es cómo pueden beneficiarse plenamente las autoridades centrales del uso de la tecnología moderna. Desde el punto de vista de las políticas, en 2016 la Conferencia de las Partes en la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional alentó a los Estados partes a que aprovecharan al máximo y con la mayor eficacia la tecnología disponible para facilitar la cooperación entre las autoridades centrales[76].

65. La necesidad de fortalecer la cooperación internacional es cada vez más acuciante, pero está condicionada por disponibilidad de recursos, incluidos "recursos tecnológicos", como redes para transmitir información de manera segura, equipo para facilitar la comunicación (por ejemplo, teleconferencias y videoconferencias) y sistemas de gestión de casos para hacer un seguimiento de las solicitudes que se envían y se reciben. La creciente necesidad de recursos también puede obedecer a la mayor eficiencia de la gestión de las solicitudes de asistencia judicial recíproca que implica el manejo de pruebas electrónicas (por ejemplo, mediante el establecimiento de unidades especializadas en las autoridades centrales).

66. Huelga decir que la gestión de casos por las autoridades centrales refleja los progresos, adelantos o deficiencias del conjunto de los mecanismos institucionales de justicia penal de los Estados Miembros, en función de la capacidad de cada uno. En muchos países donde se siguen llevando registros en papel, la realización de búsquedas y el envío de los documentos correspondientes a los países solicitantes puede ser una ardua tarea. En los países que se encuentran en el extremo opuesto, la tecnología permite utilizar plataformas electrónicas para gestionar las solicitudes de asistencia judicial que se envían y reciben o recopilar datos estadísticos sobre casos y tendencias[77].

67. En lo que respecta a la transmisión de solicitudes de asistencia judicial recíproca, en la Reunión Preparatoria de la Región de América Latina y el Caribe para el 14º Congreso se habló del uso de medios electrónicos con ese fin, que se destacó como buena práctica en algunos países de la región[78]. La Reunión Preparatoria recomendó promover el uso de la tecnología para hacer más eficiente la cooperación internacional en asuntos penales, teniendo en cuenta, entre otras cosas, los acuerdos entre las

[74] En un informe publicado en 2018 se examinó el uso delictivo de la inteligencia artificial y las amenazas conexas se clasificaron en las siguientes tres categorías principales: a) amenazas asociadas a la seguridad digital; b) amenazas asociadas a la seguridad física; y c) amenazas asociadas a la seguridad política (proliferación de noticias falsas y desinformación automatizada o campañas para influir en el comportamiento de los votantes y, posiblemente, socavar la capacidad para mantener un debate público sincero). Véase Miles Brundage *et al.*, *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation* (febrero de 2018).

[75] Documento de INTERPOL sobre innovación, "Artificial intelligence", Complejo Mundial de INTERPOL para la Innovación, 2018, pág. 2.

[76] Resolución 8/1 de la Conferencia.

[77] Banco Asiático de Desarrollo y Organización de Cooperación y Desarrollo Económicos, *Mutual Legal Assistance in Asia and the Pacific: Experiences in 31 Jurisdictions* (2017), pág. 31.

[78] Véase A/CONF.234/RPM.3/1, párr. 72.

autoridades centrales para la transmisión electrónica de las solicitudes de cooperación internacional de conformidad con la legislación interna[79].

68. La UNODC ha emprendido medidas para promover la cooperación internacional, entre otras cosas mediante las siguientes herramientas e innovaciones tecnológicas a medida: el portal de gestión de conocimientos titulado Intercambio de Recursos Electrónicos y Legislación sobre Delincuencia (SHERLOC), el directorio de autoridades nacionales competentes y la nueva versión del Programa para Redactar Solicitudes de Asistencia Judicial Recíproca[80].

69. La UNODC ha apoyado activamente los procesos intergubernamentales en que la cooperación internacional en materia de pruebas electrónicas se ha perfilado como una prioridad jurídica y de política. Como ejemplos de esos procesos cabe mencionar el grupo intergubernamental de expertos de composición abierta encargado de realizar un estudio exhaustivo del problema del delito cibernético[81], el debate temático sobre ciberdelincuencia que tuvo lugar en el 27º período de sesiones de la Comisión de Prevención del Delito y Justicia Penal, celebrado en mayo de 2018[82], y la labor al respecto del Grupo de Trabajo sobre Cooperación Internacional de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional.

I. Consideraciones éticas: salvaguardas procesales y de los derechos humanos

70. Las herramientas tecnológicas pueden ser un punto de partida útil para hacer frente a las amenazas relacionadas con la delincuencia. No obstante, al utilizar esas herramientas con determinados fines se ha de actuar con cautela para garantizar que se usen de manera responsable y ética y evitar consecuencias no deseadas. Esto reviste especial importancia en vista de que muchas de las tecnologías presentes y futuras pueden tener graves consecuencias para la privacidad personal y las libertades civiles.

71. Los profesionales de las fuerzas del orden utilizan *software* de reconocimiento facial, por ejemplo, para identificar más rápidamente a los sospechosos. No obstante, a los detractores de esta tecnología les preocupa que su uso pueda dar lugar a una vigilancia gubernamental abusiva y a manipulación empresarial y que pueda suponer el final de la privacidad. Además, los sistemas biométricos tienen un componente de retención de datos que puede hacer que peligre la privacidad debido al uso indebido de estos[83].

72. Otro ejemplo es el de la vigilancia policial predictiva o los análisis predictivos. En los últimos años cada vez son más las fuerzas de seguridad que utilizan *software* para analizar datos estadísticos, reconocer conexiones entre diversas actividades y casos e incluso predecir dónde aparecerá la próxima amenaza. No obstante, existe el riesgo de que el uso de la vigilancia policial predictiva para elaborar perfiles pueda dar lugar a la estigmatización de determinadas personas y grupos y, por consiguiente, a formas de discriminación basadas en algoritmos[84].

---

[79] *Ibid*., párr. 79 n).

[80] Disponible en https://www.unodc.org/mla/en/index.html.

[81] La información sobre las reuniones del grupo internacional de expertos puede consultarse en el sitio web de la UNODC (https://www.unodc.org/unodc/es/index.html).

[82] Véase la guía para el debate temático (E/CN.15/2018/6).

[83] Max Snijder, *Biometrics, Surveillance and Privacy* (Ispra (Italia), Red Europea de Referencia para la Protección de Infraestructuras Vitales (ERNCIP), Grupo Temático de Biométrica Aplicada para la Seguridad de las Infraestructuras Vitales, 2016), págs. 4 y siguientes.

[84] Véase Eva Schlehahn *et al*., "Benefits and pitfalls of predictive policing", publicado en *2015 European Intelligence and Security Informatics Conference: EISIC 2015*, Joel Brynielsson y Moi Hoon Yap, coords. (Piscataway, Nueva Jersey, Instituto de Ingenieros Electricistas y Electrónicos, Inc, 2015), págs. 145 a 148; Albert Meijer y Martijn Wessels, "Predictive policing: review of benefits and drawbacks", *International Journal of Public Administration*, vol. 42, núm. 12 (febrero de 2019).

73. En el ámbito de la trata de personas y al estudiar cómo afecta el uso de la tecnología a los derechos humanos y a la protección de datos[85] es esencial reforzar la protección de las víctimas. Las soluciones contra la trata se deben concebir bajo estrecha supervisión de modo que no sobrepasen los límites del derecho a la privacidad o se centren indebidamente en determinados grupos[86], velando siempre por que las víctimas tengan acceso seguro a la tecnología[87].

74. Otro factor importante es el respeto de las salvaguardas procesales para que las pruebas obtenidas mediante técnicas de investigación especiales, incluidas las que implican el uso de tecnología, sean admisibles ante los tribunales. El uso de técnicas de investigación especiales está sujeto a las disposiciones pertinentes del derecho interno y a los instrumentos multilaterales aplicables[88]. En la mayoría de las jurisdicciones, la obtención de pruebas mediante esas técnicas exige una adhesión estricta a las salvaguardias contra el abuso de autoridad, como la supervisión judicial o independiente y la observancia de los principios de legalidad, subsidiariedad y proporcionalidad[89]. Para que sean admisibles, las pruebas electrónicas deben ajustarse a los procedimientos establecidos[90]. La aplicación de los principios generales del derecho procesal y la jurisprudencia de cada país sobre la admisibilidad de las pruebas obtenidas mediante investigaciones forenses sobre criptomonedas es un ámbito nuevo y complejo que exige un análisis más detallado y un intercambio de experiencias al respecto[91].

75. A medida que se generaliza el uso de la inteligencia artificial y la robótica por las fuerzas de seguridad, se hace más patente la importancia de que este sea ético. Se han puesto en marcha iniciativas de "derecho blando" que tienen por objeto minimizar el riesgo de que la utilización de sistemas de inteligencia artificial por las fuerzas del orden atente contra derechos fundamentales y despejar la ambigüedad que surge en torno al uso ético de la inteligencia artificial y la robótica en general en lo que se refiere a la responsabilidad jurídica[92].

76. No obstante, una cuestión fundamental es si la sociedad en general está dispuesta y bien preparada para aceptar prácticas como el establecimiento de una red amplia de dispositivos de vigilancia, aun cuando se utilicen en aras de la seguridad pública[93]. Las decisiones relativas a la tecnología deberían fundamentarse en un diálogo social amplio sobre costos y beneficios y sobre las normas aplicables. Convencer a la población de los beneficios de la tecnología en los ámbitos del cumplimiento de la ley y la justicia penal forma parte de un debate general que nunca debe dejar de celebrarse a fin de que las autoridades competentes no pierdan la confianza que en ellas han depositado las comunidades y los ciudadanos cuya protección les ha sido encomendada. Ese debate también debe tener presente "la otra cara de la moneda", es decir, el

[85] Grupo Interinstitucional de Coordinación contra la Trata de Personas, "Human trafficking and technology", pág. 5.

[86] Mark Latonero *et al.*, *The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking*, Research Series on Technology and Human Trafficking (noviembre de 2012), pág. 38.

[87] Gerry, Muraszkiewicz y Vavoula, "The role of technology in the fight against human trafficking", pág. 211.

[88] Véanse el artículo 20 de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y el artículo 50 de la Convención de las Naciones Unidas contra la Corrupción.

[89] La jurisprudencia pertinente del Tribunal Europeo de Derechos Humanos puede consultarse en "Article 50: special investigative techniques", de Dimosthenis Chrysikos, publicado en *The United Nations Convention against Corruption. A Commentary*, Cecily Rose, Michael Kubiciel y Oliver Landwehr, coords., Oxford Commentaries on International Law Series (Oxford, Oxford University Press, 2019), págs. 507 y siguientes.

[90] E/CN.15/2018/6, párr. 30.

[91] Michael Fröwis *et al.*, "Safeguarding the evidential value of forensic cryptocurrency investigations" (2019).

[92] El Instituto de Ingenieros Electricistas y Electrónicos (IIEE) ha publicado un tratado global relativo a la ética de los sistemas autónomos e inteligentes (diseño conforme a normas éticas) para ajustar las tecnologías a los valores morales y los principios éticos. Véase IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems* (Pascataway, Nueva Jersey, 2019).

[93] INTERPOL y UNICRI, "Artificial intelligence and robotics for law enforcement", pág. 14.

argumento crítico de que la dependencia excesiva de la tecnología también podría generar una dependencia excesiva de estrategias coercitivas de vigilancia y control[94].

77. El Panel de Alto Nivel sobre la Cooperación Digital recomendó que el Secretario General pusiera en marcha un examen en todos los organismos del sistema de la aplicación de los instrumentos y normas internacionales de derechos humanos a las nuevas tecnologías digitales. Se debería invitar a la sociedad civil, los Gobiernos, el sector privado y los ciudadanos a exponer su opinión sobre cómo aplicar los instrumentos de derechos humanos existentes en la era digital como parte de un proceso proactivo y transparente[95].

78. Es preciso adoptar un enfoque equilibrado para encontrar soluciones en los casos en que la tecnología y el derecho a la privacidad u otros derechos humanos parecerían ser irreconciliables. Para evitar el uso de las tecnologías como "caballo de Troya" de posibles violaciones de los derechos fundamentales, el desarrollo tecnológico se debe someter a una vigilancia continua y se debe evaluar su impacto.

III. Conclusiones y recomendaciones

79. Inspirándonos en la mitología griega, cabría formular así la cuestión: ¿Será la tecnología la panacea (nombre de la hija de Asclepio con que se denomina el remedio que cura todas las enfermedades) para la prevención del delito? ¿O se trata más bien de la caja de Pandora, un proceso que traerá graves consecuencias al abrir nuevas vías para la delincuencia (similar al mito de Pandora, de cuya tinaja escaparon todos los males del mundo)?

80. La verdad está en el medio, más allá de respuestas maniqueas. La tecnología es, inevitablemente, un arma de doble filo. Las autoridades de cumplimiento de la ley y justicia penal se benefician de los avances tecnológicos. Al mismo tiempo, la explosión de las innovaciones tecnológicas abona el terreno para que prospere la delincuencia. El panorama delictivo ha experimentado un cambio drástico impulsado por varias aplicaciones tecnológicas, y las autoridades competentes no deben quedarse a la zaga.

81. El resultado del pulso entre los delincuentes y los adalides del estado de derecho dependerá en gran medida de si se invierte en capacitación y de si las estrategias de prevención del delito y justicia penal se adaptan continuamente a las amenazas emergentes sin perder de vista los aspectos éticos y de derechos humanos.

82. El 14º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal tal vez desee considerar las siguientes recomendaciones:

a) Los Estados Miembros deberían encontrar y subsanar las lagunas en sus ordenamientos jurídicos para poder investigar y enjuiciar de manera eficaz los delitos facilitados por la tecnología, por ejemplo, mediante la aprobación de nuevas leyes o la actualización de las leyes en vigor con un lenguaje neutro desde el punto de vista de la tecnología y el fortalecimiento de la cooperación internacional;

b) Los Estados Miembros deberían promover y ampliar las alianzas y sinergias con diversas partes interesadas, como las organizaciones internacionales y regionales, la sociedad civil, el sector privado y el mundo académico, a fin de impulsar la investigación, la innovación, el desarrollo y el uso de la tecnología en los ámbitos del cumplimiento de la ley y la justicia penal;

c) Los Estados Miembros deberían detectar y evaluar los riesgos de blanqueo de dinero y financiación del terrorismo que entrañan las actividades u operaciones en que participan los proveedores de servicios de activos virtuales; adoptar un enfoque basado en los riesgos para que las medidas de prevención o mitigación del blanqueo de

[94] James Byrne y Gary Marx, "Technological innovations in crime prevention and policing: a review of the research on implementation and impact", *Cahiers Politiestudies*, vol. 20, núm. 3 (2011), pág. 30.

[95] Naciones Unidas, *The Age of Digital Interdependence: Report of the Secretary-General's High-level Panel on Digital Cooperation* (junio de 2019), recomendación 3A.

dinero y la financiación del terrorismo sean acordes con los riesgos detectados; y exigir a los proveedores de servicios de activos virtuales que determinen, evalúen y adopten medidas eficaces para mitigar los riesgos de blanqueo de dinero y financiación del terrorismo;

d) Los Estados Miembros deberían invertir cada vez más en formación adecuada para mejorar la capacidad para afrontar con eficacia las dificultades que plantean las criptomonedas durante las investigaciones;

e) Los Estados Miembros deberían incluir en su legislación disposiciones pertinentes a la posesión, publicación y transferencia de material digital que pudiera llegar a utilizarse para fabricar armas y organizar actividades de capacitación para prevenir, detectar, investigar y perseguir judicialmente esos actos, así como el tráfico de armas de fuego en la web oscura;

f) La UNODC debería continuar promoviendo reuniones periódicas de las comunidades de profesionales para que los investigadores estén al tanto de los nuevos *modus operandi* de fabricación y transferencia de armas de fuego y de las correspondientes técnicas de investigación;

g) Los Estados Miembros deberían dedicar especial atención al fortalecimiento de los conocimientos técnicos y la capacidad de las autoridades competentes en todos los sectores pertinentes de modo que puedan hacer un uso óptimo de la tecnología para combatir la trata de personas y proteger los derechos víctimas;

h) La UNODC debería seguir ampliando las orientaciones y apoyo técnicos que ofrece a los Estados Miembros para determinar y aplicar con mayor eficacia medidas de justicia penal basadas en la tecnología a fin de prevenir, investigar y perseguir judicialmente la trata de personas y el tráfico ilícito de migrantes;

i) Los Estados Miembros deberían adoptar medidas legislativas o de otro tipo para facilitar la detección, por los proveedores de servicios de Internet y de acceso a Internet y otras entidades pertinentes, de material que muestre explotación y abusos sexuales de niños, niñas y adolescentes y para garantizar que ese material se denuncie y se retire;

j) Los Estados Miembros deberían aplicar políticas e intercambiar mejores prácticas, como los programas de apoyo a las víctimas y la incorporación de la perspectiva de género, a fin de proteger a los niños, niñas y adolescentes de la explotación y abusos sexuales;

k) Los Estados Miembros deberían informar y concienciar sobre los riesgos que conlleva el uso malintencionado de la inteligencia artificial y estar al corriente en todo momento de los avances de las nuevas tecnologías para garantizar la preparación, la rendición de cuentas, la transparencia y la integridad; promover el uso ético de esas tecnologías; y lograr que los ciudadanos y las comunidades confíen en ese uso;

l) Los Estados Miembros, en cooperación con la UNODC y otras organizaciones internacionales, deberían promover la asistencia técnica y la capacitación para mejorar las aptitudes de los profesionales y las autoridades centrales para utilizar la tecnología con miras a agilizar la cooperación internacional.