Knowmad Institut gemeinnützige UG (haftungsbeschränkt)
Joachimsthal | Germany
Register Nr. HRB 14178 FF (Frankfurt Oder district court)
contact@knowmadinstitut.org - **knowmadinstitut.org**

RECOMENDACIONES AL COMITÉ AD HOC ENCARGADO DE ELABORAR UNA CONVENCIÓN INTERNACIONAL COMPRENSIVA SOBRE LA LUCHA CONTRA EL USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES CON FINES DELICTIVOS.

THIRD SESSION: INTERNATIONAL COOPERATION, TECHNICAL ASSISTANCE, PREVENTION MEASURES AND THE MECHANISM OF IMPLEMENTATION

Mayo de 2022

Desde el Instituto Europeo de Estudios Multidisciplinarios Sobre Derechos Humanos y Ciencias - Knowmad Institut consideramos que, un abordaje balanceado y comprensivo que respete el derecho al anonimato –como parte del derecho a la protección de datos personales–, es clave para crear espacios seguros en el ciberespacio y prevenir el uso perjudicial de las tecnologías de la información. La coexistencia con mentes y memorias artificiales aparentemente ilimitadas, y nuestro creciente interés por modificar y ampliar nuestras propias y limitadas mentes humanas, nos obligan a repensar nuestro mundo. En la encrucijada coexisten la privacidad y la dignidad de las personas.

El rápido desarrollo de las Tecnologías de la Información y la Comunicación (TIC) y el Internet de las Cosas (IoT) se ha traducido en:

1. El desplazamiento de algunos delitos del mundo tangible al mundo virtual.
2. La creación de nuevos delitos que solo ocurren en el espacio digital.
3. La hibridación del delito en ambos mundos.

(Canappele & Aebi, 2017) (Kagita et al, 2020)

Cuando se estudia el delito, se hace desde el punto de vista penal, en el cual el principal decidor de lo que es un crimen o no es el Estado y su marco regulatorio. El triángulo del delito de Cohen y Felson (1979) resume en partes básicas los elementos del delito: el autor motivado, una víctima adecuada y un espacio determinado. La suma de las tres partes genera la oportunidad para la comisión del delito. Sin embargo, pocas veces se problematiza al crimen y quien lo comente cuando el perpetrador es el Estado y la víctima es la sociedad o la democracia. En este sentido, es de gran importancia tipificar y regular el rol de los Estados como perpetradores de crímenes o violaciones de derechos en el mundo de las TIC y el Internet de las Cosas.

Específicamente nos referimos a la regulación y tipificación de recolección de información e inteligencia como actividades criminales cuando estas atentan contra la integridad de la ciudadanía y la democracia.

La tercerización de los servicios de espionaje e inteligencia, como el spyware "Pegasus" facilitado por parte de NSO Group y utilizado por gobiernos autoritarios, supone un riesgo a la integridad física de individuos de la sociedad civil, periodistas, activistas, científicos y una amenaza a las democracias.

Estos servicios deberían ser altamente fiscalizados y regulados por órganos autónomos que evalúen la oferta, demanda, ofertantes, consumidores y fines de dicho servicio. Una investigación forense de Amnistía Internacional (2021) demostró que el uso de este software está ligado a fines ilícitos y a abusos de derechos humanos (Scott-Railton, 2022)(Geldenhuys, 2021)(Marczak et al., 2018)(Scott-Railton, 2016).

Por otra parte, la pandemia del COVID-19 ha impulsado la innovación tecnológica y la adaptabilidad hacia un mercado global, en el que estimulantes de tipo anfetamínico y nuevas sustancias psicoactivas (NPS) están disponibles en las redes de internet. Esto podría desencadenar cambios acelerados en los patrones de uso de drogas y tener implicaciones para la salud pública (UNODC, 2021).

El tráfico de sustancias a través de estrategias que presentan los patrones de las TIC es cada día más común, siendo la *darknet* y los criptomercados una notable innovación en el mercado ilícito de sustancias controladas (EMCDDA & Europol, 2017). Pero también las redes sociales evitan la necesidad del ingreso a la *darknet* para adquirir las sustancias (EMCDDA, 2021) lo cual reduce ciertos riesgos.

El análisis de los datos del comercio en los mercados de la red oscura y las redes sociales, puede llevar a desarrollar métodos útiles para detectar sustancias psicoactivas de reciente aparición. Para consolidar espacios seguros en la red, las fuerzas de seguridad y las entidades gubernamentales deben recordar que la privacidad y el anonimato son un derecho fundamental en nuestra sociedad hiperconectada.

Por todo esto, es necesario replantear las estrategias actuales y priorizar la concentración de los recursos policiales en mejorar las competencias de las incipientes unidades especializadas en ciberdelitos, agilizar las investigaciones y fomentar la financiación para investigar los crímenes más peligrosos y nocivos que amenazan al público en general a través del internet, más no en los mercados de sustancias recreativas, donde el campo emergente de la *"deflection"* puede crear espacios seguros en el ciberespacio y reducir la presión sobre las fuerzas del orden especializadas.

El enfoque de reducción del delito en el espacio digital y físico por medio de nuevas prácticas de reducción de daños y de la implementación de la *deflection* puede reducir el impacto social, comunitario y familiar del consumo de sustancias controladas, la financiación del terrorismo y mermar la liquidez de organizaciones criminales transnacionales. La *deflection* aplicada en los espacios virtuales puede facilitar la cooperación y la aplicación de la ley, tendiendo puentes entre agentes biopsicosociales, la comunidad y las fuerzas de seguridad pública.

Estudios recientes indican que las personas que usan drogas (PQUD) y que adquieren las sustancias mediante el uso de Tecnologías de la Información y la Comunicación (TIC) (Aldride et al., 2018), tienden a adoptar prácticas de reducción de daños, así como promover un "uso responsable" bajo la autodeterminación y gestión de placeres con privacidad y mayor seguridad, al practicarse además en sus lugares de residencia (Mason & Bancroft, 2018). Esto no implica descuidar las amenazas reales como el auge de los mercados de opioides, las falsificaciones de medicamentos controlados, el tráfico de armas y el material de abuso sexual de niños, niñas y adolescentes distribuido en línea (Interpol, 2022) (ECPAT International, 2016).

En el contexto de pandemia, crisis económica y cambios sociopolíticos abruptos, abordar la situación de las personas migrantes debería considerarse como una prioridad para la comunidad internacional (por su especial vulnerabilidad a ser víctimas de redes de trata donde el uso de las TIC es cada vez más común). Sólo el año 2022, se han estimado 281 millones de migrantes internacionales, de los cuales 26,4 millones en calidad de refugiados, según datos de la Organización Internacional para las Migraciones. Esta situación urge a abordar la migración desde una perspectiva multidimensional, generando sinergias en términos de justicia, seguridad, derechos humanos y desarrollo.

Desde el Instituto Europeo de Estudios Multidisciplinarios sobre Derechos Humanos y Ciencias - Knowmad Institut - instamos a esta comisión y a los Estados Miembros a:

- Que la Convención internacional sobre la lucha contra la utilización de las TIC con fines delictivos reconozca las consecuencias negativas y aprendizajes del enfoque actual sobre los crímenes relativos a las sustancias fiscalizadas.
- Realizar una revisión e impulsar una terminología apropiada sobre los delitos relacionados a las TIC y la IoT. El lenguaje preciso ayuda a "desintoxicar" las narrativas actuales y deconstruye mitos legitimados en torno al uso de estas tecnologías, el derecho al anonimato, el uso legítimo de la Inteligencia de fuentes abiertas (OSINT), la adopción de Bitcoin, las criptomonedas y los

mercados digitales de sustancias controladas para usos recreativos, por mencionar algunos.

- Reconocer que en el caso de las sustancias controladas, la fiscalización eficiente es problemática cuando el mercado no está regulado por los Estados, y sí por el Crimen Organizado; asimismo que para educar y reducir los daños es fundamental el respeto a la autodeterminación de las personas y la búsqueda de una regulación balanceada y humanitaria de las sustancias ilegalizadas.
- Considerar desde un enfoque multidimensional la amenaza que representan los ciberdelitos relacionados con drogas (especialmente las de uso recreativo), así como a responder en consecuencia con una visión humanitaria que ponga primero la dignidad y seguridad de las personas.
- Establecer puentes entre la sociedad civil y las fuerzas de seguridad para el empleo de la OSINT en los programas de seguridad de infraestructura crítica y prevención del terrorismo.
- Admitir que el análisis forense de la cadena de bloques es una de las mejores herramientas de los gobiernos para combatir las organizaciones terroristas financiadas con criptomonedas. Las organizaciones terroristas utilizan *crowdfunding* criptográfico para financiar sus operaciones en todo el mundo y es imperativo que los gobiernos estén actualizados (Grauer, 2022). Para las fuerzas de seguridad es más fácil la trazabilidad de estas operaciones que las realizadas por la banca tradicional.
- Tomar en cuenta en la capacitación de quienes aplican la ley, a profesionales multidisciplinarios, agentes biopsicosociales y actores de la sociedad civil, -como la coalición que conforma el "*Rome Consensus 2.0*"- y que cuenten con el acompañamiento del Departamento de Ciberdelincuencia, Prevención de Blanqueo de Capitales y Lucha contra la Financiación del Terrorismo de Naciones Unidas.

Finalmente, hacemos un llamado a la comisión *Ad Hoc, stakeholders* y a los gobiernos que ustedes representan, a tomar conciencia e iniciar acciones que garanticen una transición sana durante la adopción y estandarización de las tecnologías emergentes en la cuarta revolución industrial.

Referencias

- Aldridge, J., Stevens, A., & Barratt, M. J. (2017). Will growth in cryptomarket drug buying increase the harms of illicit drugs? *Addiction*, *113*(5), 789–796. https://doi.org/10.1111/add.13899
- Caneppele, S., & Aebi, M. F. (2017). Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes. *Policing: A Journal of Policy and Practice*, *13*(1), 66–79. https://doi.org/10.1093/police/pax055
- Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: a Routine Activity Approach. *American Sociological Review*, *44*(4), 588–608. https://doi.org/https://doi.org/10.2307/2094589
- ECPAT International. (2016). *Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales*. ECPAT Luxembourg. https://ecpat.org/wp-content/uploads/2021/05/Terminology-guidelines_Spanish_version-electronica_FINAL.pdf
- *European Drug Report 2021: Trends and Developments | www.emcdda.europa.eu*. (2021, June). Www.emcdda.europa.eu; European Monitoring Centre for Drugs and Drug Addiction (EMCDDA). https://www.emcdda.europa.eu/publications/edr/trends-developments/2021_en
- Geldenhuys, K. (2021). Spyware. *Servamus Community-Based Safety and Security Magazine*, *114*(10), 15–17. https://doi.org/10.10520/ejc-servamus_v114_n10_a5
- Grauer, K. (2022). *The 2022 Crypto Crime Report Original data and research into cryptocurrency-based crime Introduction 2*. https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf
- Interpol. (2022). *Terminología apropiada*. Interpol.int. https://www.interpol.int/es/Delitos/Delitos-contra-menores/Terminologia-apropiada
- Kagita, Mohan Krishna, Thilakarathne, N., Gadekallu, Thippa Reddy, Maddikunta, Praveen Kumar Reddy, & Singh, S. (2020). *A Review on Cyber Crimes on the Internet of Things*. ArXiv.org. https://arxiv.org/abs/2009.05708
- Krajowe Biuro Ds. Przeciwdziałania Narkomanii, European Monitoring Centre for Drugs and Drug Addiction, & Europol. (2020). *Drugs and the darknet : law enforcement, research and policy perspectives*. European Monitoring Centre for Drugs and Drug Addiction. https://www.emcdda.europa.eu/system/files/publications/6585/TD0417834ENN.pdf
- Marczak, B., Scott-Railton, J., McKune, S., Abdul Razzak, B., & Deibert, R. (2018). Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries. *Tspace.library.utoronto.ca*. https://hdl.handle.net/1807/95391
- Masson, K., & Bancroft, A. (2018). "Nice people doing shady things": Drugs and the morality of exchange in the darknet cryptomarkets. *International Journal of Drug Policy*, *58*, 78–84. https://doi.org/10.1016/j.drugpo.2018.05.008
- *PTACC | police treatment community collaborative*. (2022). Ptaccollaborative.org. https://ptaccollaborative.org/
- Rome Consensus 2.0. (2020). *Rome Consensus 2.0: Towards a Humanitarian Drug Policy*. Romeconsensus.com. http://romeconsensus.com/documents/
- Scott-Railton, J. (2016). The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender. *Www.academia.edu*. https://www.academia.edu/31849184/The_Million_Dollar_Dissident_NSO_Groups_iPhone_Zero_Days_used_against_a_UAE_Human_Rights_Defender?bulkDownload=thisPaper-topRelated-sameAuthor-citingThis-citedByThis-secondOrderCitations&from=cover_page
- Scott-Railton, J. (2022, January 13). *Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware - The Citizen Lab*. The Citizen Lab. https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/
- Scott-Railton, J., Marczak, B., Nigro Herrero, P., Abdul Razzak, B., Al-Jizawi, N., Solimano, S., & Deibert, R. (2022, January 13). *Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware*. The Citizen Lab. https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/
- United Nations. (2021). *World Drug Report 2021*. United Nations : Office on Drugs and Crime. https://www.unodc.org/unodc/en/data-and-analysis/wdr2021.html