Studia Prawnicze. Rozprawy i Materiały 2022, nr 1 (30) • Studies in Law: Research Papers 2022, No. 1 (30)
ISSN 1689-8052 • e-ISSN 2451-0807

DOI: 10.48269/2451-0807-sp-2022-1-002

Silvia Irene Verdugo Guzmán
Professor, Centro de Estudios Universitarios Cardenal Spínola. Fundación San Pablo-CEU, Andalucía/Spain
https://orcid.org/0000-0001-9851-4795
sverdugo@ceuandalucia.es

Ana Ochoa Casteleiro
Professor, Centro de Estudios Universitarios Cardenal Spínola. Fundación San Pablo-CEU, Andalucía/Spain
https://orcid.org/0000-0003-4850-9001
aochoa@ceuandalucia.es

Acciones para combatir el impacto del crimen en el ciberespacio. Prevención y detección con la Inteligencia Artificial

Ciberespacio y el submundo de la Darknet

Hace varias décadas que el uso de Internet se expandió por todo el mundo. Y claro, quienes eran reacios a utilizar una página web, obtener un teléfono móvil o enviar un email, han debido replantarse su existencia social, porque es innegable que la sociedad digital en que estamos inmersos inevitablemente llegó para quedarse, especialmente a partir de la pandemia declarada el 2020 por el virus SARS-CoV-2, comúnmente llamado COVID-19.

De la mano con lo anterior, nuevas formas delictivas acompañan este siglo[1]. Así, el cibercrimen se encuentra presente en toda la sociedad por el fácil acceso a internet, que en general está disponible a cualquier persona. En este sentido, EUROPOL, recuerda que la *Darknet* continuará facilitando mercados delicti-

[1] En este sentido, Miró Llinares, señala, "(e)n relación con el cibercrimen hemos visto cómo ha habido un aumento de algunos ciberdelitos debido al incremento (y al desplazamiento) de oportunidades en el ciberespacio, así como una adaptación de los cibercriminales al contexto COVID-19 tanto en objetivos y métodos como, sobre todo, en ciberlugares de ataque"; F. Miró Llinares, "Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos", *IDP. Revista de Internet, Derecho y Política*, 2021, n.º 32 (marzo), pp. 1–17, esp. p. 12, https://doi.org/10.7238/idp.v0i32.373815.

vos en línea, donde se puede acceder a todo tipo de bienes y servicios ilegales en forma anónima[2]. Las preocupaciones principales a nivel internacional han sido muchísimas, especialmente las dificultades tecnológicas para abordar la ciberdelincuencia dentro de la *Darknet*, y por ello un papel importante está en la I.A, que será un recurso cada vez más poderoso para combatir el cibercrimen[3].

El ciudadano común tiene acceso al Internet superficial o *Surface web*, donde puede realizar gran parte de su vida diaria, como es hasta hoy en día. Sin embargo, existen redes informáticas a las cuales solo pueden acceder determinadas personas y utilizando ciertos soportes del ciberespacio. Se trata de actividades que se realizan en la Internet Profunda o *Darknet*, que solamente están disponible para quienes tengan acceso a un espacio encriptado y oculto que sirve para cometer acciones prohibidas e ilícitas, difícilmente rastreables por alguien que no tenga conocimientos especiales y las herramientas adecuadas. En este sentido, la *Darknet* contiene información de acceso mucho más fácil de manejar para un hacker que podrá cometer ciberestafas, piratería informática, ciber-espionaje, tráfico de armas, drogas o de personas, etc. Y claro, los problemas se producen al existir una amplia variedad de delitos que se realizan cada vez con más frecuencia en el ciberespacio[4], con una difícil y pronta persecución penal especialmente por la difícil geolocalización del ciberdelincuente[5].

---

2 Y señala el informe de EUROPOL, que, en 2017 se cerraron por las autoridades los mercados *Darknet* más grandes: AlphaBay, Hansa y Ramp, donde se transaba con drogas, armas de fuego, herramientas para ciberdelincuencia como los malware, entre otros. Sin embargo, se produjo una migración de los usuarios hacia otros mercados existentes o que fueron creados, utilizando sistemas encriptados; EUROPOL, "Internet Organised Crime Threat Assessment (IOCTA)", 2018, https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018.PDF [acceso: 30 April 2021].

3 *Towards responsible AI innovation. Second INTERPOL–UNICRI Report on Artificial Intelligence for law enforcement*, Torino–Lyon 2020, p. 6, https://www.interpol.int/es/content/download/15290/file/AI%20Report%20INTERPOL%20UNICRI.pdf [acceso: 9 June 2022]; *vid.* S. Verdugo Guzmán, "Expansión del cibercrimen. Las ciberestafas, ataques informáticos, secuestros de información y rescates con criptomonedas, a propósito del COVID-19", [in:] *Retos jurídicos ante la crisis del COVID-19*, eds. E. Atienza Macías, J. Rodríguez Ayuso, Madrid: Wolters Kluwer, 2020, pp. 439–455.

4 Señala en el año 2002 Rovira Del Canto: "[...] el desarrollo y expansión de las modernas tecnologías, entre ellas la informática, está estrechamente vinculada a la creciente significación de la información en la sociedad postindustrial. El desarrollo de la sociedad tecnológica se constituye, por tanto, en la segunda mayor influencia en el cambio de perspectivas de la actual evolución social. [...] La criminalidad informática queda comprendida dentro de la compleja problemática propia de una "sociedad de riesgos", y en cuatro ámbitos diferentes de necesitada regulación: la protección de los derechos de la personalidad, la lucha contra la criminalidad económica específicamente relacionada con el procesamiento electrónico de datos, la protección de la propiedad intelectual, y la reforma del proceso penal"; E. Rovira Del Canto, *Delincuencia informática y fraudes informáticos*, Granada: Editorial Comares, 2002, pp. 18 y ss.

5 En este sentido, confirma Rovira Del Canto, en el ciberespacio es fácil encubrir el hecho delictivo y descubrir a su autor, gracias a la posibilidad de borrar sus huellas; *ibidem*, p. 82.

Conceptos generales de I.A.

Es relativamente reciente el interés por distintos gobiernos y entidades públicas y privadas obtener estrategias preventivas y métodos de enseñanza masificados y al alcance de cualquier persona física o jurídica que pueda acceder a internet, pero que no sabe a ciencia cierta sobre ciberseguridad o cómo actuar frente a un ciberataque. Y aquí es donde la I.A tiene un espacio importante donde desarrollarse.

Pero, primeramente, cabe conceptualizar la I.A. Una definición precisa proviene del DRAE, y expone que es la "disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico"[6].

El Parlamento Europeo se pronuncia sobre la I.A, y se refiere a la habilidad de una máquina que presenta las mismas características del ser humano, esto es, el razonamiento, aprendizaje, creatividad y capacidad para planear. Así, la I.A permite que los sistemas tecnológicos perciban su entorno y se relacionen con él, resuelvan problemas y actúen con un fin específico; en definitiva, recibe los datos preparados anteriormente o recopilados por sus propios sensores, los procesa y responde a estos[7].

La I.A se utiliza hace ya varios años, una tecnología autónoma y adaptable que está inmersa en todas las esferas sociales mediante robots, sistemas de navegación, drones, e incluso en la recomendación de contenidos en plataformas de películas y música, o también para generar o alterar contenidos visuales. En definitiva, nos atrevemos a acercar un concepto, señalando que la I.A es una ciencia presente en cuestiones cada vez más comunes de la vida diaria gracias a sistemas interconectados de procesamiento de datos en programas informáticos mediante algoritmos[8].

Por todo lo señalado, es posible concluir que,

> (l)a IA, que actualmente funciona en laboratorios y en algunos entornos de producción, es capaz de detectar mejor los patrones distribuyendo los nodos de aprendizaje. Esto aumenta su impacto en funcionalidades como el control de acceso. Algunos sistemas de IA son capaces de identificar a los individuos utilizando complejas biohuellas como patrones de escritura o ritmos cardíacos, y detectar incluso las más sutiles desviaciones en el tráfico normal de la red para identificar a los actores maliciosos y malware[9].

---

6 Diccionario de la Real Academia Española (DRAE), sitio web.

7 "¿Qué es la inteligencia artificial y cómo se usa?", Noticias del Parlamento Europeo, 8 September 2020, https://www.europarl.europa.eu/news/es/headlines/society/20200827STO85804/-que-es-la-inteligencia-artificial-y-como-se-usa [acceso: 30 April 2021].

8 Algoritmo: conjunto ordenado y finito de operaciones que permite hallar la solución de un problema. DRAE, *op. cit.*

9 "La inteligencia artificial en el juego del cibercrimen", Globb Security, 22 April 2020, https://globbsecurity.com/la-inteligencia-artificial-en-el-juego-del-cibercrimen-45631 [acceso: 30 April 2021].

La I.A frente al cibercrimen

En principio la I.A ha sido creada y desarrollada para ser utilizada con buenos fines y para colaborar con el bienestar del ser humano. Sin embargo, una manipulación maliciosa de sus algoritmos, puede ser una herramienta muy peligrosa e incluso mortal. Y claro, mediante el uso de Internet es posible que hackers de toda índole puedan acceder al uso de la I.A, como ha sucedido en varias ocasiones, por ejemplo, interrumpiendo sistemas informáticos controlados mediante I.A, también generando noticias e imágenes falsas, y usando sistemas autónomos a modo de armas. Lamentablemente, existen casos de coches autónomos que han sido manipulados por ciberdelincuentes, produciendo accidentes de tráfico al excederse los límites de velocidad sin que el conductor tenga alguna posibilidad de reacción. Así también, por ejemplo, la compañía Nokia demostró hace un tiempo que las redes de *bots* impulsadas por la I.A se estaban utilizando para encontrar vulnerabilidades específicas en dispositivos Android y luego usarlas cargando malware de robo de datos que, por lo general, solo se detectan una vez que se ha hecho el daño[10].

Los avances que conlleva el uso de las nuevas tecnologías de la información también acarrean problemas en el ciberespacio, y los sistemas de I.A pueden ser de gran ayuda identificando las potenciales amenazas y ciberataques de toda clase. En este sentido,

> [...] (s)u implementación en las redes actuales requerirá el despliegue de nodos de aprendizaje a nivel regional mejorados por la IA que pueden recoger y procesar datos locales para obtener respuestas rápidas a los eventos, y también compartir esos datos con un cerebro central de IA para lograr una correlación más profunda. De esta manera no solo se mejorará la detección de los patrones de comportamiento sospechosos, sino que también permitirá responder de forma inmediata antes de que un ataque pueda formarse completamente[11].

Es importante utilizar la I.A con acierto, y así, uno de los objetivos de su utilización es trabajar en línea y coordinación con los datos que se recopilan, porque es muy probable que el uso de la I.A reconozca patrones comunes al entorno delictivo, adelantándose a los hechos, con lo cual podrían impedirse ataques diversos. Además servirá para acelerar la persecución policial de los responsables de un delito especialmente gracias al Big Data y la elaboración de mapas de criminalidad en las ciudades, que servirán para obtener datos tan variados como los índices de delincuencia, tipos de delitos más frecuentes

---

[10] *Nokia Threat Intelligence Report – 2019*, p. 7, https://blog.drhack.net/wp-content/uploads/2018/12/Nokia_Threat_Intelligence_Report_White_Paper_EN.pdf [acceso: 30 April 2021].

[11] "La inteligencia artificial en el juego del cibercrimen"..., *op. cit.*

en ciertas zonas, los horarios en que se incrementan los riesgos, y otros que faciliten las tareas de prevención y persecución[12]. Se podría hablar del uso de drones que facilitan la labor de quienes buscan infringir las normas de tráfico, pero por temas de espacio quedará pendiente. Simplemente cabe destacar que su uso puede ser de gran ayudar para el hombre, pero en algunos casos, puede ser perjudicial su uso en relación al derecho de privacidad y la protección de datos de las personas.

Otro uso importante de la I.A es para delitos que consisten en la suplantación de identidad o falsedades en documentos oficiales -como los pasaportes-, ya existen por ejemplo en China, gafas que incorporan unas cámaras que gracias a la I.A están conectadas con base de datos policiales, ayudando a identificar personas buscadas por algún delito o que utilicen documentación que no coincida con las bases mediante el reconocimiento facial[13]. Claro, al otro lado de la balanza se puede encontrar la probable vulneración de derechos humanos y de la privacidad de las personas, pero es un tema que no podemos abordar ahora.

INTERPOL expone que la I.A servirá para alterar y mejorar la vigilancia, por ejemplo, para identificar a personas de interés en espacios concurridos; pronosticar y predecir la violencia; ordenar, etiquetar y clasificar automáticamente datos operativos policiales de gran tamaño, como pruebas o materiales nocivos; incluso monitorear los impulsores de la radicalización o potenciales terroristas[14].

---

[12] Y así, existe la vigilancia predictiva, gracias al conjunto de datos de eventos históricos de unos 2 a 5 años se utilizan para entrenar el algoritmo de una ciudad, el cual se va actualizando a diario con nuevos eventos a medida que se van recibiendo, utilizando solo 3 tipos de datos (delito, ubicación del delito y fecha/hora del delito) para crear sus predicciones. Todo esto es trasladado a Google Maps, que en recuadros establece las áreas de mayor riesgo para cada día y turno de día, tarde o noche. Con esto, se incrementan las labores de vigilancia además de la eficiencia en el sistema de prevención delictual, en PREDPOL, "Los tres pilares de la vigilancia basada en datos", https://predpol.com/law-enforcement/#predPolicing [acceso: 30 April 2021].

[13] Señala un reportaje periodístico que, "[...] (e)n los últimos años, China ha dado un impulso significativo a la inteligencia artificial. Algunas de sus aplicaciones, especialmente las que se basan en el reconocimiento facial, empiezan a tomar forma en cuestiones relacionadas con la seguridad nacional. A este caso en Henan se le suma, por ejemplo, la identificación de conductores que violan las normas de tráfico en Shanghái, el hallazgo en pocas horas de un niño que había sido secuestrado en Shenzhen o la detención de personas buscadas por la policía en grandes eventos como el Festival Internacional de la Cerveza de la ciudad costera de Qingdao. Otras tecnologías de empresas especializadas en reconocimiento de voz han permitido a las fuerzas de seguridad desarticular redes dedicadas a las estafas telefónicas en la provincia de Anhui o la identificación de narcotraficantes"; "La policía china usa gafas con reconocimiento facial para identificar a sospechosos", *El País*, 8 February 2018, https://elpais.com/internacional/2018-/02/07/mundo_global/1518007737_209089.html [acceso: 30 April 2021].

[14] *Towards responsible AI innovation*..., p. 5.

Aprendizaje autónomo y dilemas pendientes en la prevención delictiva

Los próximos desafíos tecnológicos plantean varias interrogantes. Una de ellas, consiste en la capacidad de los sistemas de aprendizaje automático de I.A que contribuirá a reducir la creciente brecha de conocimientos en materia de ciberseguridad. Al trasladar las responsabilidades a procesos autónomos de autoaprendizaje que funcionen de forma similar a los sistemas autoinmunes humanos -cazando, detectando y respondiendo a los eventos de seguridad de forma autónoma y en tiempo real- se podrán centrar en la planificación y desarrollo de estrategias de orden superior y que ayudará a mejorar la seguridad de los mercados digitales del futuro[15].

Otra interrogante que se plantea, será la posibilidad de atribuir responsabilidad penal por ejemplo a un robot que 'destruya' un ser humano por un fallo en su sistema o porque lo detecte como un error (como ya sucedió en Japón hace unos años), pues por ahora no se puede aplicar la teoría del delito a la I.A, ni siquiera se puede hablar de persona jurídica o robótica. Quizás, se puede hablar de imprudencia por parte del responsable del robot, siguiendo el ejemplo descrito. Y, como acertadamente señala Miró Llinares, "resulta esencial monitorizar la evolución de la IA desde una perspectiva de atribución de responsabilidad para evitar llegar a situaciones en las que el aprendizaje de las máquinas no permita decir que nadie haya tomado una decisión negligente pese a que existan daños"[16].

Finalmente, cabe referirse brevemente a la importancia de a la ciberseguridad. La implementación de una tecnología coordinada y homogénea a nivel mundial puede ayudar a que se obtenga una sociedad globalizada más segura y que permita realizar todo tipo de transacciones sin ser víctima de delitos digitales. Lo primordial es que en el ciberespacio se logre una red global de ciberseguridad que otorgue mayor certeza a la detección de problemas en tiempo y lugar. En este sentido, estrategias preventivas como la ciberseguridad son importantes en la sociedad de riesgos informáticos en que nos encontramos inmersos. Así, por ejemplo, realizar copias de la información y datos contenidos en ordenadores hacia unidades externas -y no solamente en la nube-, poseer y actualizar antivirus, comprobar que se accede efectivamente a un sitio web oficial, proteger los correos electrónicos, contraseñas, y no utilizarlas en cualquier sitio web, son algunas recomendaciones o estrategias de prevención frente al peligroso escenario del cibercrimen del siglo XXI.

---

15 "La inteligencia artificial en el juego del cibercrimen"..., *op. cit.*

16 F. Miró Llinares, "Inteligencia artificial y Justicia Penal. Más allá de los resultados lesivos causados por robots", *Revista de Derecho Penal y Criminología*, 2018, n.º 20, p. 96.

Conclusiones

Lamentablemente son cada vez más constantes los delitos informáticos cometidos en el ciberespacio bajo el anonimato y la astucia en el uso de la *Darknet*. Adiestrados ciberdelincuentes intentan poner en marcha sus actividades ilícitas de la más variada índole, principalmente con una motivación económica. Los mercados digitales ofrecen toda clase de bienes y servicios en que difícilmente puede ser rastreado su origen. Las estafas informáticas son un claro ejemplo de cibercrimen, donde hackers han obtenido datos e información de sus víctimas, lo que se traduce en grandes cantidades de dinero e información de las víctimas, que pueden movilizar con relativa facilidad por el ciberespacio.

A efectos de la prevención delictiva, un elemento clave es la implantación de la I.A basada en la confianza entre todos los interesados en combatir la ciberdelincuencia. En este sentido, confirma EUROPOL[17] que, sería útil el establecimiento de plataformas de colaboración entre los distintos países miembros y partes interesadas de la UE siempre basados en la confianza y ciberseguridad de todos, mediante la comprensión de los componentes básicos de la I.A y su interacción.

Por el contrario, en el caso de que la I.A se encuentre con datos o algoritmos manipulados, es fundamental contar con algoritmos de aprendizaje automáticos efectivos, es decir, que los datos de entrenamiento sean relevantes y se pueda controlar el proceso de aprendizaje para evitar cualquier anormalidad.

La gran cantidad y distintas categorías de datos que son recopilados en el ciberespacio mediante el uso de algoritmos que sirven para la persecución y represión del cibercrimen, es posible manipularlos maliciosamente para cometer delitos con los consecuentes problemas que ya han sido expuestos. Lo importante es que se establezcan estadísticas transparentes, específicas y coherentes entre ellas y con el compromiso de todos los interesados en la lucha contra el cibercrimen.

Es clave la implementación de una tecnología coordinada y homogénea a nivel mundial de I.A que puede ayudar a una sociedad globalizada más segura y que permita realizar todo tipo de transacciones digitales sin ser víctima de delitos. Lo primordial es que en el ciberespacio se logre una red global de ciberseguridad que otorgue mayor certeza a la detección de problemas en tiempo y lugar frente al escenario del cibercrimen del siglo XXI.

---

[17] EUROPOL, "La IA fiable requiere una ciberseguridad sólida", 25 October 2019, https://www.europol.europa.eu/newsroom/news/trustworthy-ai-requires-solid-cybersecurity [acceso: 30 April 2021].

Bibliografía

EUROPOL, "Internet Organised Crime Threat Assessment (IOCTA)", 2018, https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018.PDF [30 April 2021].

EUROPOL, "La IA fiable requiere una ciberseguridad sólida", 25 October 2019, https://www.europol.europa.eu/newsroom/news/trustworthy-ai-requires-solid-cybersecurity [acceso: 30 April 2021].

"La inteligencia artificial en el juego del cibercrimen", Globb Security, 22 April 2020, https://globbsecurity.com/la-inteligencia-artificial-en-el-juego-del-cibercrimen-45631/ [acceso: 30 April 2021].

"La policía china usa gafas con reconocimiento facial para identificar a sospechosos", *El País*, 8 February 2018, https://elpais.com/internacional/2018-/02/07/mundo_global/1518007737_209089.html [acceso: 30 April 2021].

Miró Llinares F., "Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos", *IDP. Revista de Internet, Derecho y Política*, 2021, n.º 32 (marzo), pp. 1–17, https://doi.org/10.7238/idp.v0i32.373815.

Miró Llinares F., "Inteligencia artificial y Justicia Penal. Más allá de los resultados lesivos causados por robots", *Revista de Derecho Penal y Criminología*, 2018, n.º 20, pp. 87–130.

Nokia Threat Intelligence Report – 2019, https://blog.drhack.net/wp-content/uploads/2018/12/Nokia_Threat_Intelligence_Report_White_Paper_EN.pdf [acceso: 30 April 2021].

PREDPOL, "Los tres pilares de la vigilancia basada en datos", https://predpol.com/law-enforcement/#predPolicing [acceso: 30 April 2021].

"¿Qué es la inteligencia artificial y cómo se usa?", Noticias del Parlamento Europeo, 8 September 2020, https://www.europarl.europa.eu/news/es/headli-nes/society/20200827STO85804/-que-es-la-inteligencia-artificial-y-como-se-usa [acceso: 30 April 2021].

Rovira Del Canto E., *Delincuencia informática y fraudes informáticos*, Granada: Editorial Comares, 2002.

Towards responsible AI innovation. Second INTERPOL–UNICRI Report on Artificial Intelligence for law enforcement, Torino–Lyon, 2020, https://www.interpol.int/es/content/download/15290/file/AI%20Report%20INTERPOL%20UNICRI.pdf [acceso: 9 June 2022].

Verdugo Guzmán S., "Expansión del cibercrimen. Las ciberestafas, ataques informáticos, secuestros de información y rescates con criptomonedas, a propósito del COVID-19", [in:] *Retos jurídicos ante la crisis del COVID-19*, eds. E. Atienza Macías, J. Rodríguez Ayuso, Madrid: Wolters Kluwer, 2020.

Resumen

Acciones para combatir el impacto del crimen en el ciberespacio. Prevención y detección con la Inteligencia Artificial

Los últimos dos siglos hemos visto nuevos tipos de delitos que han pasado a un primer plano, y que los delitos tradicionales han adoptado diferentes formas o un alcance completamente nuevo, especialmente digital. La especificidad de distintos ciberdelitos se encuentra en la internet profunda o *Darknet*, tales como el fraude informático, los ataques informáticos, abuso sexual y la explotación sexual de niños a través de sistemas informáticos etc. La aparición del nuevo coronavirus SARS-CoV-2 a fines del 2019 y la pandemia declarada por COVID-19 causada por el virus a comienzos del 2020, han servido para subrayar la importancia del combate al cibercrimen. La denuncia e investigación de delitos es crucial para las unidades policiales y las partes interesadas en la comprensión y análisis del ciberdelito. Entonces, gracias al desarrollo de la Inteligencia Artificial (I.A) y la recopilación de datos estadísticos son utilizados para realizar evaluaciones de delitos, castigos o sanciones, e identificar a las personas investigadas o perseguidas. La construcción de la cooperación en I.A con las partes interesadas en todo el sector público, la industria, la academia, así como las entidades de seguridad relacionadas, agencias de inteligencia etc., es un próximo paso esencial. También, cabe referirse a la ciberseguridad, que juega un papel importante en la defensa de las personas, de empresas e infraestructuras. Los proveedores de seguridad digital se enfocan en usuarios, dispositivos, redes, datos, aplicaciones o empresas para brindar soluciones con el fin de detectar y responder ante una amenaza cibernética.

Palabras clave: inteligencia artificial, internet oscura, cibercrimen, ciberdelincuente, ciberseguridad

Abstract

Actions to combat the impact of crime in cyberspace. Prevention and detection with Artificial Intelligence

Over the past two centuries, we have seen emerging types of crimes coming to the fore and traditional crimes taking on different forms or an entirely new scope altogether. Specificity of various cybercrimes are on the darknet, how computer fraud, computer attacks, the sexual abuse and sexual explotation of children through computer systems, etc. The emergence of the novel SARS-CoV-2 coronavirus in late 2019 and the ongoing COVID-19 pandemic caused by the virus on 2020, has served to underscore the importance of combat to cibercrime. The reporting and research of crimes is crucial for police units and stakeholders in understanding and analysis cybercrime. So, the I.A and collection of stadistical data information are used to evaluations of crime, punishments or sanctions and identifying the people investigated or persecuted. Building cooperation on I.A with stakeholders throughout the public sector, industry, academia, as well as

related security entities, intelligence agencies and so on, is an essential next step. Also, the cybersecurity plays an important role in defending individuals, industry and infrastructure. Security vendors focus on users, network, data, application or entire enterprises to provide solutions to detect and respond to cyber threats.
Key words: artificial intelligence, darknet, cibercrime, hacker, cibersecurity