Prevención y persecución de Ciberdelitos: ¿Un nuevo terreno para la Inteligencia Artificial?

Pastorini, Joselina
Abogada, Profesora Adjunta de Derecho Penal
Universidad Católica de La Plata, Argentina[1]
joselinapastorini@hotmail.com

Abstract

"El avance de las Nuevas Tecnologías (TIC's) está modificando dramáticamente la dinámica de nuestras sociedades. El derecho, como ciencia social, no puede permanecer indiferente frente a este fenómeno. Una parte de los desafíos que este nuevo escenario introduce se manifiestan en el surgimiento de nuevas formas de criminalidad que reclaman una respuesta ágil y eficaz desde la política criminal.

La presente comunicación persigue, por un lado, analizar cuáles son las dificultades -en torno a la prevención e investigación- que plantean los delitos informáticos y, en función de ello, proponer una instancia de posible solución a dichos inconvenientes: la implementación de sistemas de Inteligencia Artificial (IA) como mecanismo de combate cibercriminal.

Asimismo, se pretende realizar un desarrollo de Derecho Comparado, en relación a países donde se han implementado diversos sistemas de Inteligencia Artificial (IA) con fines preventivos y/o investigativos – España, Holanda, Estados Unidos, a efectos de poder evaluar la viabilidad de aplicación de los mismos en países de América Latina, como Argentina y Uruguay".

Palabras Claves

Ciberdelitos. Investigación. Persecución. Inteligencia Artificial. Argentina. Uruguay

Introducción

El avance de las nuevas tecnologías ha dado surgimiento a nuevos tipos de delitos, asicomo también a la comisión de delitos tradicional delitostradicionales mediante el uso de las TIC's (todos aquellos recursos, herramientas y programas que se utilizan para procesar, administrar y compartir la información mediante diversos soportes tecnológicos: computadoras, teléfonos, portátiles de audio y video, etc).

Estos delitos no convencionales pueden tener alcances y resultados indeterminados, atento a su carácter "transnacional" y la inexistencia de límites geográficos, lo cual rompe la barrera clásica de la "ley territorial".

Las nuevas tecnologías constituyen un desafío para los conceptos jurídicos existentes y los procesos de investigación que se llevan adelante en países de América Latina, como Argentina y Uruguay.

[1] Profesora Adjunta de Derecho Penal. Este trabajo de investigación fue realizado en el marco del programa *Becas Iberoámerica Jóvenes Profesores Investigadores 2018-2019*, en la Universidad San Pablo CEU Madrid, Enero- Marzo 2019 "Ciberdelitos: España-Argentina".-

Postulamos aquí que la implementación de sistemas de Inteligencia Artificial, puede representar una herramienta valiosa a la hora de procurar una persecución ágil y eficaz de esta particular forma de criminalidad.

El presente trabajo propone, en primer lugar, detectar cuáles son los inconvenientes y dificultades que los ciberdelitos plantean en torno a su investigación y persecución.

Como segundo eje, se pretenden analizar algunos sistemas de inteligencia artificial que se encuentran operativos en otros Estados -para la prevención e investigación criminal- sus ventajas e inconvenientes tanto desde una perspectiva práctica como jurídica.

Así se tomará del modelo Español el "sistema VERIPOL"; del modelo penal Holandés el "sistema SWEETIE" Y "VALCRI" (Visual Analytics for Sense-making in Criminal Intelligence analysis) , y del modelo Estadounidense el sistema "COMPSTAT". Si bien algunos de estos sistemas han sido creados y/o utilizados para la investigación de delitos tradicionales, el estudio en este caso, se hará desde una perspectiva "cibercriminal".

Por último, se realizará un análisis en torno a las posibilidades reales de uso de estos sistemas de Inteligencia Artificial en países de Latinoamérica -como Argentina y Uruguay-, ello en función de la posibilidad o no de colisionar con sus derechos fundamentales.

¿Ciberdelito o Cibercrimen?

Antes de entrar al tema de fondo parece pertinente efectuar algunas precisiones en cuanto a la nomenclatura que se utilizará, pues en este campo la terminología no está del todo asentada.

A nivel mundial no se ha establecido ninguna definición general y consensuada de los términos "Ciberdelitos"y "Cibercrimen", ni tampoco la doctrina ha llegado a un consenso de si ambos conceptos significan o pueden ser utilizados para referirnos a lo mismo: criminalidad a través de medios informáticos.

Ello, puede estar dado por el hecho que la palabra se define por sí misma, o porque como todo concepto jurídico, no se llega a un acuerdo internacional sobre su definición exacta.

En el presente trabajo, asumiendo mi posición de considerar a ambos términos como sinónimos, y así evitar detener mi objeto de estudio en una mera discusión conceptual, - atento a que son otros los aspectos relativos al tema que resultan más contradictorios y requieren de un exhaustivo análisis- se entenderá por "Delito Informático", "Ciberdelito",o "Cibercrimen", a aquella *conducta típica*

antijurídica y culpable, cuyo medio de comisión o cuyo objeto es la informática.

En el primero de los casos, vamos a referirnos a delitos tradicionales, pero que por el avance de las TICs han cambiado su modalidad de comisión, convirtiéndolos en delitos más complejos. Por su parte, el segundo plantea la aparición de nuevos tipos penales, nuevas figuras delictivas, a raíz del surgimiento de estas nuevas TICs dando lugar a nuevos delitos no convencionales.

Es decir, que cuando hablemos de Ciberdelitos, vamos a hablar de nuevas figuras delictivas que nacen a través del surgimiento de la informática, y también de delitos tradicionales, ya regulados en nuestra legislación, que dado el medio tecnológico utilizado para su comisión, requiere la adaptación de dichos conceptos convencionales, a los nuevos requerimientos que la cibercriminalidad propone.

Problemática en torno a su prevención e investigación

Los Ciberdelitos, ya sea por su naturaleza desconocida, por su espacio indefinido, o por la rapidez con que se han instalado, poseen particulariades propias que no sólo los convierten en delitos no convencionales -que desestructuran las barreras tradicionalmente conocidas-, sino que también resultan un nuevo desafío a la hora de poder criminalizarlos.

Entre algunas de las dificultades que presentan encontramos:

I- Indeterminación del espacio físico: Ciberespacio

Las consecuencias de los delitos informáticos pueden tener mayor alcance, dado que las mismas no estan restringidas por los limites geográficos o las fronteras nacionales.

Las características de este tipo de agresiones permiten a sus ejecutores actuar a nivel global y de manera anónima, adquiriendo así una capacidad y un alcance que parecieran no tener límites, dando lugar a la instauración de redes mundiales de ciberdelincuencia.

II- Jurisdicción y Ley aplicable:

Las nuevas tecnologias constituyen un desafío para los conceptos jurídicos existentes.

La información y la comunicación fluyen con facilidad por todo el mundo. Las fronteras han dejado de ser barreras para ese flujo. Los delincuentes se encuentran cada vez menos en los lugares en donde se producen los efectos de sus actos. Sin embargo la lesgislación nacional esta destinada a un territorio específico.

En delitos cometidos a través de Internet lo corriente será que se trate de “delitos a distancia” en los que la conducta no se inicia o no tiene lugar en el mismo Estado

que la consumación, o de “delitos de tránsito”, donde tanto la conducta como la consumación tienen lugar en país extranjero, sirviendo el Estado de que se trate solamente de lugar de tránsito (por ejemplo, porque la información pasa por un servidor ubicado allí). En estas clases de delito resulta necesaria una elaboración teórica para determinar cuál o cuáles son los Estados facultados para ejercer su jurisdicción y aplicar su derecho penal sobre el caso. De esta característica común a los delitos en cuestión surge entonces este problema al que cabe dar una solución jurídicamente fundamentada.

IV- Dificultad y desconocimiento en la investigación del delito informático:

La evidencia digital es volátil e intangible, es decir, puede desaparecer o ser alterada muy rápido, por lo que las investigaciones que involucran este tipo de pruebas deben ser rápidas y precisas. Para esto,se requiere un proceso penal ágil y eficiente,con esfuerzo organizado por parte de los países.

Si bien el fenómeno de las “nuevas tecnologías” ya no es tan nuevo, los operadores jurídicos suelen no estar familiarizados con su análisis jurídico. Parece imprescindible romper esta tendencia, pues el fenómeno de la informática y los denominados ciberdelitos o cibercrímenes han irrumpido en las ciencias jurídicas

Las nuevas tecnologías requieren de una capacitación constante de los operadores judiciales, policiales y/o administrativos en la materia.

V- Indeterminación del bien jurídico protegido:

El tratamiento legislativo brindado a los delitos informáticos en su generalidad, plantea problemas de interpretación, dado que las conductas típicas, a diferencia de otros delitos, involucran a más de un bien jurídico, por lo que quedan vinculados sus elementos típicos a los parámetros comunes de interpretación de los delitos con los que se encuentran agrupados.[2]

En consonancia con la preocupación que en el ámbito internacional existe, parece haberse iniciado un camino —al menos en el ámbito doctrinal— en el que se entiende que este tipo de delitos tienen por objeto de protección un bien jurídico de primer orden relacionado con las nuevas tecnologías, pudiendo proteger, además, otros bienes jurídicos que se manifiesten con menor intensidad (intimidad, patrimonio, etc.). En virtud de ello, la ubicación de los delitos informáticos en la normativa interna de cada Nación dependerá de su

[2] GALÁN MUÑOZ, A., “Expansión e intensificación del derecho penal de las nuevas tecnologías: un análisis crítico de las últimas reformas legislativas en materia de criminalidad informática”, en *Revista de Derecho y Proceso Penal*, núm. 15, 2006, p. 23, señala con razón que “este concepto [criminalidad informática] se delimita atendiendo al hecho de que todos los delitos que se incluyen en su senoafectarían a un bien jurídico colectivo común, con independencia del concreto valor individual que también se pudiese lesionar o poner en peligro por tal conducta”.

reconocimiento como una clase autónoma y/o novedosa que requiere un tratamiento diferenciado, o por otro lado, podrá ser considerado e incluído como parte de los delitos tradicionales pero con características distintas en su mecanismo de comisión.

Nuevas Tecnologías contra el Cibercrimen del Siglo XXI: Inteligencia Artificial

Los Ciberdelitos, tal como se ha hecho mención, requieren la adopción de nuevos mecanismos para su combate eficaz.

El derecho nunca va por delante de la tecnología, por lo cual es necesario que el mismo, se adapte a las nuevas realidades que las TICs plantean.

Los sistemas basados en Inteligencia artificial (IA) pretenden cambiar el concepto de la investigación de los delitos, logrando encontrar conexiones que los humanos a menudo pasan por alto.

Como resultado, la inteligencia criminal podría anticiparse a la delincuencia y apoyar la investigación de casos individuales, logrando tal como se ha verá en el derecho comparado, resultados positivos en las investigaciones criminales.

Mecanismo de Inteligencia Artificial con fines preventivos y/o investigativos en el Derecho Comparado

ESPAÑA

Sistema VERIPOL

El Sistema VeriPol es una herramienta informática diseñada por la Policía Nacional de España, para estimar la probabilidad de que una denuncia – en principio por robo con violencia e intimidación o hurto con tirón (RVI-HT)- sea falsa. Constituye una herramienta que predice con alta efectividad si una denuncia es falsa o verdadera y desde fines del año 2018 se utiliza el programa en todas las Comisarías de Policía del mencionado país.

Tal como hiciera referencia, el sistema VeriPol fue desarrollado por iniciativa de la Policia Nacional de España, mediante un proyecto con la Universidad Complutense y la Carlos III de Madrid, y La Sapienza de Roma. Juntos han desarrollado un programa por el que pasan todas las denuncias escritas para que detecte ciertos patrones y los clasifique, tal y como hace, inconscientemente, el policía más experimentado.

VeriPol ha sido presentado, como una herramienta novedosa para la detección de denuncias falsas, dentro del campo de la “Policía Predictiva”, y su nacimiento estuvo dado a partir de la idea de crear un sistema de combate ante el alto porcentaje de denuncias falsas en delitos de robo con violencia o hurtos -sobre todo de teléfonos móviles de alta gama- que registraba el mencionado país, lo que implicaba despliegue en la investigación policial-

judicial, gasto de tiempo y de recursos públicos.

El sistema inteligente creado, analiza el lenguaje de la denuncia, e indica la probabilidad de que esta no sea verídica. Se trata de un análisis automático de las declaraciones de denunciantes utilizando técnicas de procesamiento del lenguaje natural y aprendizaje automático.

Además, se ha integrado perfectamente con el sistema SIDENPOL (sistema policial de almacenamiento y gestión de denuncias). Es decir, la entrada del sistema consiste en el documento de cada denuncia, desde el cual se extrae el texto descriptivo de la misma. Estas características se pasan a un modelo matemático que estima la probabilidad de falsedad de la denuncia. La salida del programa es la probabilidad de que la denuncia introducida sea falsa.

De comprobaciones empíricas realizadas sobre el sistema VERIPOL, se logró demostrar que el mismo logró reducir el nivel de subjetividad presente en la toma de denuncias, mejorar la calidad de las decisiones y aumentar el nivel de satisfacción de los policías involucrados[3]

A partir de dos conjuntos de denuncias, verdaderas en uno y falsas en el otro, VeriPol aprende automáticamente las características más salientes de cada conjunto y así entrena un modelo estadístico. Por ejemplo, se sabe que en los casos de robo, las declaraciones verdaderas presentan más detalles, descripciones e información personal, frente a la insistencia exclusiva en el objeto extraído y la omisión de detalles sobre el atacante o cómo sucedió el incidente de las falsas. A partir de este análisis lingüístico, Veripol es capaz de crear un patrón eficaz.

Para estudiar su eficacia antes de implantarlo en las comisarías nacionales, los científicos llevaron a cabo un estudio piloto en dos provincias españolas en el mes de Junio del año 2017, y en tan solo una semana, se detectaron y cerraron 49 casos de hurto falsos, mientras que entre 2008 y 2016 fueron de 3,33 y 12,14 en Murcia y Málaga, respectivamente. La eficacia del estudio piloto fue de un 83%.

La aplicación en la Policía de una herramienta basada en VeriPol es doble: por un lado desalentar a los ciudadanos a presentar denuncia falsas; y por otro, evitar el uso de recursos policiales en situaciones en las que no es necesario, optimizando esfuerzo y tiempo.

Se traduce en una reducción del ruido debido a las denuncias falsas en las bases de datos de la policía, ayudando a la limpieza de casos de simulaciones de delito por RVI-HT.

[3] Lara Quijano-Sánchez, Federico Liberatore, José Camacho-Collados, Miguel Camacho-Collados. “Applying automatic textbased detection of deceptive language to police reports: Extracting behavioral patterns from a multi-step classification model to understand how we lie to the police”. Knowledge-Based Systems Vol 149, Junio 2018. DOI: 10.1016/j.knosys.2018.03.010

Si bien VeriPol se ha desarrollado para detectar denuncias falsas por los delitos de robos con violencia e intimidación, hurto/tirón, actualmente la Policia Nacional se encuentra adaptando el sistema VeriPol para que pueda ser utilizado en la totalidad de denuncias que a diario se reciben en los destacamentos policiales -a excepción de las denuncias por violencia de género-.

HOLANDA

Sistema VALCRI

VALCRI (Visual Analytics for Sense-making in Criminal Intelligence Analysis) es un proyecto creado por la policía de West Midlands (Reino Unido) y de Amberes (Bélgica)- financiado por la Unión Europea- basado en el sistema de Inteligencia Artificial, desarrrollado para lograr agilidad y eficacia en la investigación policial de los delitos criminales.

El origen del proyecto encuentra su respuesta en la necesidad de abordar la creciente preocupación que despierta la inseguridad y la delincuencia en toda Europa.

El sistema, se encarga de analizar la escena de un delito escaneando en cuestión de segundos millones de fuentes de información de distintos formatos, -tales como registros, imágenes e interrogatorios-, detecta todos los patrones sospechosos y en virtud de ello capaz de reconstruir escenas delictivas, así como un “mapa del delito”. Utiliza un software de reconocimiento facial asistido con tecnologías de Inteligencia Artificial, con el que detecta e identifica a personas concretas tomando como fuentes cámaras de circuito cerrado de televisión. En tiempo real, logra una interacción analítica entre los datos de análisis visuales confrontados contra los datos contenidos en el Big Data utilizando herramientas de IA.

La combinación de la inteligencia artificial y el análisis visual, sumado al software de reconocimiento facial, permite detectar e identificar -con alta probabilidad- al posible autor de un delito. Para que sea efectivo, es indispensable digitalizar los antiguos archivos policiales.

El sistema VALCRI, ha logrado un gran avance en las investigaciones criminales, logrando que las mismas se desarrollen con más velocidad y precisión, y sobre todo con menos despliegue de recursos.

Sistema SWEETIE

El proyecto Sweetie fue desarrollado en Holanda a finales del año 2013 por La ONG Tierra de hombres[4], con el objeto de verificar el alcance y la gravedad del problema de “turismo sexual infantil” a través de internet y demostrar que métodos

[4] “Tierra de Hombres”es una ONG fundada en 1960 por Edmond Kaiser, tiene como objetivo, y mediante la acción, promover el desarrollo de la infancia defendiendo sus derechos, sin discriminación de orden político, racial, confesional y de sexo. https://www.tierradehombres.org

de investigación “novedosos”y amoldados a los requerimientos que las nuevas tecnologías plantean, resultan ser más eficaces en la lucha contra este particular tipo de criminalidad.

“Sweetie” fue el nombre dado a esta menor virtual de diez años de origen filipino, creada a través de técnicas de animación avanzadas que captan los movimientos y la voz de una persona real (de una niña), para poder llegar hasta los miles de delincuentes sexuales que navegan cada día por la web.

Del proyecto -que duró un total diez semanas- el equipo “Tierra de Hombres”, constató que Sweetie atrajo en la red, a través de chats públicos, a 20.000 adultos dispuestos a que la niña realizara actos sexuales ante su webcam a cambio de dinero. De esta cifra, 1000 pudieron ser identificados y localizados gracias a las huellas digitales que las redes sociales dejan en las web.

Los datos de estos adultos identificados, pertenecientes a 71 países diferentes, fueron enviados por parte de la ONG a la Interpol para intentar que las autoridades policiales y judiciales, intervinieran en la cuestión.

En la actualidad, se ha registrado la primera condena, gracias al 'cebo' de la niña virtual Sweetie. Se trata de un ciudadano australiano que había contactado con ella pensando que era una niña real de nueve años, y fue condenado a un año de prisión por iniciar y mantener conversaciones telefónicas deshonestas a través de chat con Sweetie, tenencia de pornografía infantil y envío de fotos obscenas.

En la sentencia, la magistrada interviniente manifestó no importar que Sweetie fuera una niña virtual, atento a que el condenado en todo momento creyó que estaba manteniendo contacto con una niña de diez años, y por dicha circunstancia, “para la ley, eso es suficiente".

El sistema, reitero, creado en el ámbito privado por medio de una ONG, demostró un gran avance de la tecnología para la protección del menor y la seguridad en la red, y evidenció la necesidad de adoptar políticas de investigación proactivas que otorguen a las agencias de aplicación de la ley el mandato de patrullar activamente los puntos de acceso a Internet donde este abuso infantil se produce todos los días y a escala mundial.

ESTADOS UNIDOS

Sistema COMPSTAT

El modelo COMPSTAT, es un mecanismo desarrollado por la Policia Nacional de los Estados Unidos, para ser utilizado en la prevención e investigación en el ámbito policial, y se basa en cinco principios: 1). Objetivos específicos; 2). Inteligencia oportuna y precisa; 3). Estrategias y tácticas efectivas; 4). Despliegue rápido de personal y recursos;

1- Objetivos específicos: Al contar con información precisa y oportuna, el Sistema define prioridades, qué problemas son dignos de atención y esfuerzo, y cuáles no.

2-El componente esencial de COMPSTAT es el análisis científico y el uso de información oportuna y de calidad. La data es recolectada a partir de una variedad de fuentes, incluyendo información generada externa e internamente.

3-Uno de los componentes más interesantes del modelo COMPSTAT es el desarrollo de tácticas efectivas basadas en zonas geográficas y no en unidades específicas. En este sistema se procura dar mayor información a todos los involucrados en una zona para que actúen de forma mancomunada. Sumado al énfasis en las unidades especializadas, en muchos casos la política tradicional se ha enfocado en los distintos turnos de trabajo. Así, el Comandante del turno "mañana" está al tanto de todos los delitos acaecidos durante su turno. Sin embargo, el Comandante del turno "mañana" podría no estar enterado de los delitos sucedidos fuera de su jornada laboral (como el turno noche o turno tarde). La rendición de cuentas geográfica, hace a los responsables del área de revisar todos los reportes de los delitos ocurridos en su zona asignada, más allá del lapso específico en el que ocurrieron. Esto reviste especial importancia en la identificación de patrones y tendencias de la actividad delictiva, puesto que los delincuentes no limitan sus actividades en coincidencia con los turnos de un Comandante determinado.

4-Despliegue rápido de Personal y Recursos: Una vez que un plan de acción fue desarrollado es esencial que la estrategia sea implementada cuanto antes. Una vez más, la llave de este componente es la coordinación de las distintas unidades especializadas junto con las operaciones de patrulla, en miras a la obtención de un objetivo común. Uno de los puntos fuertes de COMPSTAT es la "rendición de cuentas". Una vez que un problema ha sido identificado y una estrategia ha sido desarrollada, es responsabilidad del oficial pertinente el asegurarse de que los pasos necesarios sean adoptados. Si no lo hace, en el marco del concepto original de COMPSTAT, el Oficial puede ser reasignado o incluso degradado por su falta de atención y compromiso con el proceso de COMPSTAT.

¿Es posible la adopcion de estos sistemas en países de América Latina?

En el año 2001, fue firmado en el seno de la Unión Europea, el Convenio sobre Cibercriminalidad en Budapest, el cual planteó entre sus principales objetivos 1- Armonizar los elementos de los delitos conforme al derecho sutantivo penal de cada país en materia de delitos informáticos; 2- Establecer conforme

al derecho procesal penal de cada país los poderes necesarios para la investigación y el procesamiento de dichos delitos informaticos, 3- Establecer un régimen rápido y eficaz de cooperación internacional.

Dicho instrumento internacional constituye el primero en su especie en regular esta nueva modalidad de criminalidad informática. Si bien el tratado fue creado en el seno de una Institución Europea, está abierto para que otros Estados puedan adherirse. Actualmente, hay 56 Estados parte que provienen de los cinco continentes. Por el lado de América Latina, ya son parte Chile, Costa Rica, República Dominicana, Panamá, Mexico, Argentina[5]. Uruguay hasta el momento, no ha ratificado el mencionado Convenio.

Por tal, desde el punto de vista jurídico internacional, se evidenció la necesidad de emplear nuevas herramientas para el combate del cibercrimen, y por sobre todo crear conciencia de Cooperación Internacional a los fines de poder combatir este nuevo fenómeno, adoptando nuevos procedimientos dado que los mecanismos tradicionales resultan insuficientes a la hora de hacer frente, a este nueva forma de criminalidad.

Y es en función de ello, que la adopción de mecanismos de Inteligencia Artificial, para enfrentar a las nuevas TICs utilizadas para cometer delitos por parte de los delincuentes parecería ser una decisión acertada, analizando previo a su implementación, los derechos fundamentales que cada ordenamiento jurídico propone a efectos de evitar colisiones normativas.

Asimismo, y repito, tal como fue planteado en el Convenio de Budapest, al ser los ciberdelitos de carácter de transnacional, es necesaria la cooperación entre países, y la adopción por parte de los mismos de nuevos mecanismo en las formas de obtención de las prueba, dado que como principal particularidad que presentan es que la evidencia ya no es física -por lo general-, sino digital.

Si bien los sistemas analizados, en su mayoría han sido creados con fines preventivos de delincuencia convencional, parecería que su adopción a la criminalidad informática no resulta algo ilógico, sino por el contrario, se adaptan a la nueva realidad que el Siglo XXI y la nueva criminalidad nos plantean.

Sistemas como VERIPOL, VALCRI, COMPSTAT, constituyen -tal como ha surgido de las estadísticas arrojadas- herramientas válidas a las fuerzas policiales y judiciales en las investigaciones delictivas. A su vez su implementación, y sobre todo sus buenos resultados, han sido posible por ir los mismos acompañados de

[5] Argentina ratificó el Convenio de Budapest mediante Ley 27.411 el 15/12/2017.

otras herramientas, tales como un fuerte resguardo de protección de datos personales -lo que impide que la obtención de pruebas resulte nula por aplicación de mal procedimiento, y a su vez asegura que los derechos de los individuos se vean respetados-, y una política criminal comprometida.

No escapa a la realidad de la transnacionalidad de los delitos informáticos[6], que dado a que la investigación y recolección de evidencia -digital- requiera muchas veces de la cooperación internacional, se debieran implementar sistemas cuyo funcionamiento traspase las "barreras nacionales", y el Ciberconvenio de Budapest constituye un primer camino hacía esos fines, más allá que el mismo haya quedado desactualizado -dado que fue firmado en el año 2001-, y hasta el momento no se ha realizado ninguna adecuación a la realidad tecnológica en las que nos encontramos inmersos.

Distinto parecería ser el caso del sistema SWEETIE, el cual fue creado y utilizado en el ámbito privado, por una ONG, y cuya obtención de prueba – de la cual se logró una sentencia condenatoria-, a la luz del respeto de los derechos fundamentales, resulta al menos dudoso.

Si bien el Sistema SWEETIE fue utilizado en esa única oportunidad, y logró "demostrar"que mecanismos de avance, van de la mano con efectividad en las investigaciones criminales, no volvió a utilizarse. Su aplicación en países Argentina y Uruguay, no resultaría viable sin que ello colisionara con derechos fundamentales de alcance internacional tales como principio de legalidad, defensa en juicio, igualdad, entre otros.

Conclusión

Los Sistemas de Inteligencia Artificial pretenden cambiar el concepto de investigación de los delitos criminales. Los delitos informáticos, por su ya mencionada "no convencionalidad", y rápidez con que nacen y se expanden en ese nuevo llamado "Ciberespacio" requieren necesariamente de la adopción de mecanismos de combate, tecnológicos, rápidos y eficaces.

El siglo XXI exige otro tipo de herramientas para garantizar la prevención y persecución que las nuevas tecnologías plantean. Emplear mecanismos de prevención e innovación en las investigaciones policiales y judiciales en la realidad que hoy nos encontramos, resulta una necesidad inmediata a los fines

[6] Los delitos que se cometen en y a través de la red suelen tener carácter transnacional, ya sea porque son cometidos por personas que operan en diferentes países, porque las víctimas están en un país distinto o porque la prueba está alojada en servidores ubicados en países distintos al que lleva adelante la investigación

de poder combatir el fenómeno de la cibercriminalidad.

La tecnología en constante avance, nos demuestra que el Derecho debe cumplir su función de acompañar el desarrollo tecnológico para un progreso sostenido y seguro de nuestra sociedad,y ello resulta posible con la adopción de nuevas herramientas, tales como la aquí reseñada: Inteligencia Artificial, tanto en la prevención como en la persecución de esta nueva forma de criminalidad que parecería no tener límites claros.

La inteligencia artificial constituye un mecanismo acertado en la lucha contra el cibercrimen, pero para que pueda lograr su eficacia, es necesario que dichos instrumentos puedan ir acompañados del respeto a la legalidad y derechos fundamentales de una Nación. Utilizada esta IA de otro modo, puede constituir una herramienta libre para abusos y malas prácticas, y violatoria de todas las garantías constitucionales de los ciudadanos, lo cual no sólo no cumpliría con los objetivos propuestos, sino que generaría la peor de las vulneraciones en una Nación: inseguridad jurídica.

Referencias

[1] CÁRDENAS, Claudia. “El lugar de comisión de los denominados ciberdelitos”.Polít. crim., N° 6, 2008, A2-6, pp. 1-14.

[2] GONZÁLEZ HURTADO, Jorge Alexandre *“La seguridad en los sistemas de información como un bien jurídico de carácter autónomo. Perspectiva europea y española”,* Revista Penal México 9-Septiembre 2015

[3] GALÁN MUÑOZ, A., *“Expansión e intensificación del derecho penal de las nuevas tecnologías: un análisis crítico de las últimas reformas legislativas en materia de criminalidad informática”,* en Revista de Derecho y Proceso Penal, núm. 15, 2006, p. 23

[4]*”Ciberseguridad y Derecho Internaciona”*, Revista Española de Derecho Internacional Sección FORO. Vol. 69/2, julio-diciembre 2017, Madrid, pp. 291-299. *http://dx.doi.org/10.17103/redi.69.2.2017.2.02*

[5]DÍAZ GÓMEZ, A., *“El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest”*, *REDUR* 8, diciembre 2010, págs. 169-203. ISSN 1695-078X

[6] TEMPERINI Ma. B.C,Macedo *“La cifra negra de los delitos informáticos: Proyecto ODILA”*.

[7]RIQUERT, M.A *“Legislación contra la delincuencia informática en MERCOSUR”*, “Revista General de Derecho Penal” (España), dirigida por los Dres. Ignacio Berdugo Gómez de la Torre y José R. Serrano-Piedecasas, con referato, versión electrónica disponible en www.iustel.com, Nº 9 de mayo de 2008, Sección Apuntes de Derecho Comparado ”

[8] *“La Convención de Cibercrímen de Budapest y América Latina: Breve guía acerca de su impacto en los derechos y garantías de las personas”*, Trabajo de investigación realizado por el Área Digital Asociación por los Derechos Civiles. Ref: https://adcdigital.org.ar

[9] *"Sociedad Digital y Derecho"*, Publicación Boletín Oficial del Estado, Madrid 2018. Dirección Tomás de la Quadra-Salcedo Fernández del Castillo y José Luis Piñar Mañas. Ref: NIPO BOE: 786-18-069-0

[10] LARA QUIJANO-SÁNCHEZ, FEDERICO LIBERATORE, JOSÉ CAMACHO-COLLADOS, MIGUEL CAMACHO-COLLADOS."*Applying automatic textbased detection of deceptive language to police reports: Extracting behavioral patterns from a multi-step classification model to understand how we lie to the police"*. Knowledge-Based Systems Vol 149, Junio 2018. DOI: 10.1016/j.knosys.2018.03.010

[11]Páginas de Consulta:

https://www.ba-csirt.gob.ar/
http://www.poderjudicial.es
https://www.incibe.es/
https://www.aepd.es/
https://sbarrera.es/
https://www.fiscal.es
https://www.tierradehombres.org

Datos de Contacto:
Joselina Pastorini. Universidad Católica de La Plata (UCALP). Calle 65- 370 (1H) La Plata, Buenos Aires, Argentina.(CP 1900)
joselinapastorini@hotmail.com