ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

65/2021 28 de mayo de 2021

*Fernando Ruiz Domínguez**

Ciberbioseguridad: Implicaciones técnico-jurídicas para la perfecta desconocida en Seguridad y Defensa

Ciberbioseguridad: Implicaciones técnico-jurídicas para la perfecta desconocida en Seguridad y Defensa

Resumen:

Cuando se combina ADN con cuestiones de Seguridad y Defensa el interés está asegurado. Pero, si además se incluyen aspectos técnicos que no se tienen en cuenta en la práctica policial habitual y la regulación normativa, la expectación puede ser máxima. Todo ello posiblemente llevará al lector en una montaña rusa cuyas emociones saldrán o no a la luz dependiendo del puesto de cada uno, de su grado de responsabilidad y de la visión de futuro, o no, que el mismo tenga.

La ciberbioseguridad vino para quedarse.

Palabras clave:

Ciberbioseguridad, ADN, Seguridad, Defensa.

Cyber-biosecurity: Technical-legal implications for the perfect unknown in Security and Defence.

Abstract:

When DNA is combined with Security and Defence issues, the interest is assured. But, if technical aspects that are not considered in the usual police practice and normative regulation are also included, the expectation may be maximum. All this will possibly take the reader on a roller coaster whose emotions will or will not come to light depending on the position of each one, their degree of responsibility and the vision of the future, or not, that they have.

Cyberbiosecurity is here to stay.

Keywords:

Cyberbiosecurity, DNA, Security, Defense.

Cómo citar este documento:

RUIZ DOMÍNGUEZ, Fernando. *Ciberbioseguridad: Implicaciones técnico-jurídicas para la perfecta desconocida en Seguridad y Defensa*. Documento de Opinión IEEE 65/2021. http://www.ieee.es/Galerias/fichero/docs_opinion/2021/DIEEEO65_2021_FERRUI_Ciber.pdf y/o enlace bie[3] (consultado día/mes/año)

Definiendo el entorno

Aunque la biología y la biotecnología hace tiempo que entraron en la era digital, las políticas de seguridad que rodean a estas no han seguido el ritmo del progreso, máxime si se tiene en cuenta que, por regla general, no existe en la sociedad un conocimiento actualizado e individualizado en materia de ciberseguridad física, ciberseguridad lógica y bioseguridad; así que mucho menos si ello se trata de forma conjunta; y una pura fantasía si alguien piensa que estas cuestiones se han contemplado específicamente a nivel jurídico nacional o internacional.

De esta manera, la ciberbioseguridad integra los tres conceptos clave de esta nueva área de interés policial como son:

- Ciberseguridad lógica: Alude a los riesgos de computación y sistemas de redes usados en procesos de gestión y para compartir información, así como la protección de esta.
- Ciberseguridad física: Se refiere a la dependencia de alto grado y consecuencias entre los sistemas físicos y los ordenadores específicos que controlan y monitorizan los mismos.
- Bioseguridad: Describe la contabilidad, control y protección de los materiales biológicos a la hora de prevenir un acceso no autorizado a los mismos, una perdida, un robo, o incluso un uso inapropiado, un desvío o liberación intencionada.

A modo de resumen técnico hay que decir que la ciberbioseguridad en biotecnología tiene su máxima expresión en la automatización, la inteligencia artificial y la biología sintética. Por su parte la ciberbioseguridad dentro de la digitalización de la tecnología tradicional lo hace en campos como la agricultura, la fabricación o las ciencias biomédicas.

Ciberbioseguridad y ADN

Por otra parte, el hecho de que ahora sea fácil leer las secuencias de ADN o de que las mismas estén disponibles en bases de datos públicas, como, por ejemplo, las de las empresas privadas de servicios de genealogía genética u otros servicios bioinformáticos,

así como que la mayoría de proyectos de investigación en materia biológica tengan una dimensión cibernética provocan que surja un nuevo tipo de riesgo.

Para la objetivación de ese riesgo hay que ver si existen vulnerabilidades, si realmente se producen amenazas y cuáles son las posibles consecuencias de todo ello.

La finalidad de esto está bien clara puesto que, si no hay un riesgo para la Seguridad y la Defensa, no valdrá la pena, entre otras cuestiones, entrar a regular jurídicamente un campo como el de la ciberbioseguridad. Esto es así porque, si bien es cierto que a nivel nacional la reforma operada en el Código Penal en 2015 introdujo novedades con respecto a nuevos delitos informáticos, no lo es menos que no se regularon ciertas cuestiones que, además, la triste realidad actual ha sacado a flote con el estado de alarma y que, igualmente, no conviene perder de vista, ya que este, o se podría volver a producir, o podría ser declarado por otro motivo.

Salvo el robo de datos con aplicaciones falsas simulando la detección de la COVID-19, no existen agravaciones de penas para los delitos vinculados a las nuevas tecnologías (TIC), que se cometan durante un estado de alarma y que además participen de los tres conceptos anteriormente vistos, algo que evidentemente se queda muy corto si se tiene en cuenta que en el Internet Organised Crime Threat Assessment (IOCTA) 2020 de EUROPOL se dice en su página 13 que «[s]i bien han surgido discusiones y modelos durante varias décadas en torno a las amenazas planteadas por una crisis pandémica, el brote de COVID-19 ha demostrado el desafortunado impacto potencial de tales crisis en nuestra vida diaria en todo el mundo».

Por todo ello conviene echar un vistazo a por qué motivo o motivos puede resultar interesante regular las agravaciones delictivas de algunos de los delitos vinculados al ADN y cometidos en el ámbito de la ciberbioseguridad durante, por ejemplo, un estado de alarma.

Las vulnerabilidades

Lo primero que conviene es empezar a hablar de los *hackers* de nueva generación para ver la situación real actual a nivel mundial.

Con las investigaciones de la Agencia de Proyectos de Investigación Avanzados de Defensa (DARPA, por sus siglas en inglés) de EE. UU.[1] respecto a la necesidad de almacenar gran cantidad de información dentro de moléculas de ADN (en este caso sintético), se inició en abril de 2017 una carrera en la que no solo están interesados los militares, sino también empresas informáticas que, entre otras cuestiones, quieren buscar alternativas al silicio.

Esto se consiguió y los resultados son espectaculares, puesto que un solo gramo de ADN sintético es capaz de almacenar 215 petabytes[2] de datos, aunque de momento los precios son prohibitivos para un uso mayoritario y rutinario.

Ahora bien, dicho progreso científico también trajo su caja de Pandora, y esta se abrió con las investigaciones de agosto de 2017 de NEY, Peter, KOSCHER, Karl, ORGANIK, Lee., CEZE, Luis. y KOHNO, Tadayoshi[3], respecto a que mediante la introducción de *malware* (un *exploit*) en dicho ADN sintético comprado *on line* —y por tanto dejando claro que se trata de otro tipo de ADN (distinto al ADN natural falsificado), cuya comercialización es corriente y accesible para el público—, se puede lograr el acceso y control del ordenador que está gestionando el perfil genético analizado (el secuenciador). Es decir, por una parte, se podría lograr el robo de la información que ese ordenador almacene o con la que trabaje, o incluso se podría manipular la misma para que apareciera almacenada de la forma que el *hacker*, de forma remota, desease.

Esto debería ser así máxime cuando ya es posible editar el genoma humano natural con mayor fiabilidad o cuando en el mismo también se puede insertar *malware* mucho más fácilmente que en otro tipo de genes, ya sea para atacar a un ordenador vinculado al perfilado genético e inutilizarlo, o ya lo sea para modificar los resultados de los análisis que este realice, etc. Además, la efectividad de este tipo de ataque ya ha sido probada con éxito igualmente en 2019 mediante estructuras genéticas más simples, tipo bacterias para, por ejemplo, atacar incluso tras cierto tiempo a los perfiladores/secuenciadores genéticos de un Servicio de Salud Pública e Higiene que haya tenido que tomar muestras

[1] "Turning to Chemistry for New "Computing" Concepts", *DARPA*, 23-03-2017. Disponible en https://www.darpa.mil/news-events/2017-03-23 Fecha de consulta 26-04-2021.
[2] Un petabyte equivale a 1 000 000 000 000 000 bytes.
[3] NEY, Peter., KOSCHER, Karl., ORGANIK, Lee., CEZE, Luis. y KOHNO, Tadayoshi. "Privacy, and DNA sequencing: Compromising computers with synthesized DNA, Privacy leaks and more", *UNISEX*, Security Symposium, Computer security, agosto de 2017. Disponible en https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-ney.pdf Fecha de consulta 26-04-2021.

biológicas para analizar las superficies (en este caso posibles patógenos) presentes en un determinado lugar al que ha tenido que acudir por motivos profesionales[4]. Es decir, algo similar a lo que le ocurriría a las FF.CC.S. con los vestigios biológicos encontrados y procesados en una escena de un delito con relevancia geoestratégica (por ejemplo, un asalto a una embajada) y analizados posteriormente en un laboratorio de ADN.

Por otra parte, también hay que tener en cuenta si se producen casos de ataques a las estructuras, sistemas, medios, etc. relacionados con la sanidad en general y con la investigación genética en particular.

Así destacan:

1. Un grupo indeterminado atacando al laboratorio forense privado usado por la policía del Reino Unido en junio de 2019[5].
2. Unos grupos extranjeros no identificados atacando a finales de 2018 la base de datos del Ministerio de Sanidad del Reino Unido (Proyecto 100.000 genomas): ubicada en una instalación militar de alta seguridad del Reino Unido[6].
3. Un grupo extranjero no identificado atacando la base de datos del Servicio de Salud de Noruega en enero de 2018[7].
4. Unos grupos indeterminados atacando de forma histórica los hospitales norteamericanos: La cifra de personas afectadas, 71 millones, duplicó en 2019 a la del año 2018.
5. El 18 de julio de 2020 se produjo un ataque a la base de datos pública GEDMatch mediante el cual no solo los perfiles de ADN de los usuarios que habían decidido que los mismos no estuvieran disponibles para realizar búsquedas familiares[8] por

[4] ISLAM, Mohd Siblee, IVANOV, Stepan, ROBSON, Eric, *et alter*, "Genetic Similarity to counter bio-hacking of DNA-sequencing functionality", *Nature*, artículo 8684, 24-06-2019. Disponible en: https://www.nature.com/articles/s41598-019-44995-6 Fecha de consulta 26-04-2021.
[5] DEVLIN, Hannah. "Hacked forensic firm pays ransom after malware attack", (05-07-2019), *The Guardian*. Disponible en https://www.theguardian.com/science/2019/jul/05/eurofins-ransomware-attack-hacked-forensic-provider-pays-ransom Fecha de consulta 26-04-2021.
[6] BODKIN, Henry. "NHS patient's genetic data targeted as foreign hackers attack high security MoD unit", *The Telegraph,* 05-12-2018. Disponible en: https://www.telegraph.co.uk/news/2018/12/05/nhs-storing-patients-genetic-data-high-security-army-base-due/ Fecha de consulta 26-04-2021.
[7] CIMPANU, Catalin. "Hacker Might Have Stolen the Healthcare Data for Half of Norway's Population", *Bleepingcomputer.com*, 18-01-2018. Disponible en: https://www.bleepingcomputer.com/news/security/hacker-might-have-stolen-the-healthcare-data-for-half-of-norways-population/ Fecha de consulta 26-04-2021.
[8] Técnica de minería de ADN mediante la cual las FF.CC.S. de algunos países (no España) tratan de localizar a familiares de un delincuente buscándolos mediante comparación (y coincidencia parcial) entre los perfiles de ADN obtenidos de vestigios biológicos recogidos en la escena del crimen con los perfiles de ADN inscritos en bases de datos de ADN, ya sean estas policiales o no (como la de GEDmatch y otras).

comparación con los subidos a la base de datos por las FF.CC.S. dejaron de tener esa excepción y por tanto pasaron a poder ser utilizados con ese fin, sino que de la misma forma los perfiles genéticos subidos por las FF.CC.S. fueron accesibles para el resto de los usuarios de manera que los susodichos podían saber qué y a quién estas estaban buscando.

La conclusión de todo lo visto es bien clara. Existen claras vulnerabilidades.

Además, a finales de 2019 se publicó un trabajo de EDGE, Michael D. y COOP, Graham[9] sobre las vulnerabilidades de las empresas de servicios de genealogía genética que permiten al público almacenar perfiles genéticos en sus bases de datos, pero sin mencionar a ninguna de ellas en concreto como objeto preciso de un posible ataque. Sin embargo, muy poco tiempo después, a principios de 2020, se conoció una brecha de seguridad legal que afectaba concretamente a GEDmatch[10] a la que mediante la introducción en la misma base de datos de ADN de ciertos perfiles genéticos creados para el ataque y a través de un tipo de consultas múltiples a la base de datos pública se podía obtener información de otros usuarios en porcentajes que no solo superaban al 90% de los usuarios, sino que incluso lo hacían en porcentajes similares de fiabilidad de la información obtenida.

Es decir, que mediante una docena de archivos de ataque se podían inferir casi todos los marcadores de ADN reales del perfil objetivo (en este caso igualmente creados para la prueba), a pesar de que los mismos en principio deberían ser privados.

La minería de ADN constituye una técnica estratégica a la que las FF.CC.S. en España prácticamente no le han prestado atención. Baste mencionar la posibilidad de que miembros del crimen organizado puedan encontrar a un testigo protegido o a un agente encubierto mediante búsquedas familiares en una base de datos pública de ADN, incluso aunque a este se le haya practicado una operación de cirugía plástica en su rostro, se le haya facilitado una nueva identidad, etc.[11].

[9] EDGE Michael.D., COOP, Graham. "Attacks on genetic privacy via uploads to genealogical databases", *BioRxiv*, 22-10-2019. Disponible en: https://www.biorxiv.org/content/10.1101/798272v1.full Fecha de consulta 26-04-2021.
[10] NEY, Peter, CEZE, Luis, KHONO, Tadayoshi, et alter. "Genotype Extraction and False Relative Attacks: Security Risks to Third-Party Genetic Genealogy Services Beyond Identity Inference", University of Whashington, 2020. Disponible en: https://dnasec.cs.washington.edu/genetic-genealogy/ney_ndss.pdf Fecha de consulta 26-04-2021.
[11] O tenga una identidad falsa, o haya cambiado de domicilio, etc.

Las amenazas

Otro de los aspectos de la ciberbioseguridad es que determinados tipos de ataques en materia de Seguridad y Defensa pueden servir para derribar a un candidato presidencial, un presidente electo de un gobierno, etc.

La técnica es bien sencilla y no por conocido desde hace años el tipo de daño que puede generar[12] resulta incluso mucho más fácil de ejecutar hoy en día, dada la democratización de los servicios genéticos y sus precios muy reducidos y asequibles para, en este caso, cualquier tipo de atacante.

Consistiría en que dicho atacante obtuviera ADN de la víctima. Algo relativamente sencillo dado que no requiere ni siquiera entrar en contacto con esta o aproximarse excesivamente a la susodicha ya que, como se sabe, su ADN se puede obtener de cualquier objeto que incluso la misma haya rozado levemente.

Una vez obtenido el vestigio biológico, simplemente el interesado tendría que solicitar el análisis del ADN que hubiera remitido por correo postal a cualquier empresa de servicios *on line*, siendo numerosas las que ofrecen todo tipo de pruebas para determinar, entre otras cuestiones, la posible predisposición genética de una persona a padecer un determinado tipo de enfermedad.

Con dichos resultados (como también se podría centrar sobre la genealogía de dicho objetivo para ver sus orígenes), el resto del trabajo lo harían «las granjas de trolls»[13] ubicadas en terceros países que se dedicarían a difundir en las redes sociales, principalmente, el rumor de que dicho objetivo tiene tal o cual enfermedad (o predisposición genética a tenerla)[14].

No hay más que recordar para el caso de las enfermedades, y por pura analogía, cómo en 1972 en EE. UU. George McGovern fue forzado a reemplazar a su compañero

[12] GREEN, Robert C., ANNAS, George J. "The genetic privacy of presidential candidates", *The New England Journal of Medicine*, 20-11-2008. Disponible en: https://www.nejm.org/doi/full/10.1056/NEJMp0808100 Fecha de consulta 26-04-2021.

[13] Personal técnico informático cualificado dedicado por turnos a realizar estas labores en ubicaciones generalmente clandestinas y contando con gran cantidad de medios tecnológicos conectados en red para poder hacer uso de la ingeniería social a gran escala. Se les asocia habitualmente a las noticias falsas, a la propaganda del interés del mejor postor o a cualquier otro interés, generalmente de carácter político-económico ya sea lícito o ilícito.

[14] La difusión de noticias falsas (*fake news*) solo se encuentra agravada durante el estado de alarma, si las mismas están vinculadas a los artículos 284,1. 2º y 285 del Código Penal, los cuales hacen referencia a que las mismas estén en relación al mercado y los consumidores.

Thomas Eagleton (candidato demócrata para la Vicepresidencia) después de que se reveló que este había sido hospitalizado por problemas de salud mental[15].

De hecho, y según parece, los datos analizados provenientes de EE. UU. indican que, por ejemplo, en dicho país se cuida que el ADN de su presidente no sea captado y, además, si es posible, se trate de captar el ADN de los dirigentes de otros países.

Así, por ejemplo, consta en el libro del autor de trabajos de no ciencia ficción más vendidos, Ronald Kessler, titulado *In the President´s Secret Service*, publicado en 2009 y respecto a Barack Obama.

Igualmente, no hay que perder de vista que para el 20 de febrero de 2020 se publicitó una subasta en Nueva York de objetos con ADN o directamente material biológico, como pelos, etc. al parecer utilizados o pertenecientes y abandonados por los asistentes a la cumbre mundial de Davos, Suiza, en 2018 (entre ellos Donald Trump o Angela Merkel)[16].

Las consecuencias

Otra de las cuestiones de interés viene de la mano de a quién más le puede interesar el minado de datos a partir del ADN y ahí es donde entran otros actores, que, si bien tienen una estructura y funcionamiento habitual dentro de la legalidad, en algún momento y circunstancias no podría ser así.

De esta manera, en este trabajo se plantean varios sectores y actores por las consecuencias que ello implica:

1. Aseguradoras: El hecho de que, por ejemplo, en EE. UU. las aseguradoras de salud no puedan realizar, por ley[17], discriminaciones basadas en el ADN de los clientes[18] no es óbice para que de forma encubierta lo pudieran hacer (por

[15] THURBER Jon. “Thomas Eagleton, 77; vice presidential candidate left race over health reports”, *Los Angeles Times*, 05-03-2007. Disponible en: https://www.latimes.com/archives/la-xpm-2007-mar-05-me-eagleton5-story.html Fecha de consulta 26-04-2021.
[16] Lista completa de los objetos disponibles en https://issuu.com/theearnestproject/docs/the_davos_collection_v5.1 Fecha de consulta 26-04-2021.
[17] U.S. Code, Título 42 Capítulo 6A Subcapítulo XXV, Parte A, Subapartado I § 300gg–5, disponible en https://www.law.cornell.edu/uscode/text/42/300gg-5, fecha de consulta 26-04-2021.
[18] En un estudio inicial de la empresa 23andMe se utilizó 750.000 perfiles de su base de datos de ADN y en junio de 2020 estaba estudiando 10 000 perfiles nuevos (ajenos a su base de datos y recabados de entre voluntarios que habían padecido la COVID-19 mediante *kits* de análisis de ADN gratuitos) para determinar si existe predisposición genética (gen ABO) que permita determinar la probabilidad de padecer la enfermedad y superarla o no.

ejemplo, basadas en la predisposición genética para contraer o ser inmune a una determinada enfermedad).

2. Financieras y bancos: La hipótesis es bien clara, ya que obtener una base de datos de ADN de miles o millones de clientes potenciales, les permitiría decidir las mejores estrategias para, por ejemplo, conceder préstamos personales o hipotecarios de larga duración a clientes que pudieran sobrevivir a una pandemia.
3. Empresas sanitarias rivales[19].
4. Empresas farmacéuticas que están desarrollando una vacuna contra la COVID-19[20] y que además la información genética podría ser crucial.
5. Gobiernos extranjeros[21].

Suplantación de identidad y falsificación de ADN

Continuando con la cuestión jurídica que afecta a lo técnico y viceversa, tenemos que la suplantación de identidad mediante datos biométricos (lo cual incluye el uso del ADN), como la falsificación de ADN (ya sea física[22] o virtual) generan dos nuevas especialidades delictivas que convendría analizar, por cuanto puede que el juzgador tenga la información actualizada suficiente como para tener su propio criterio y sin tenerse que ver limitado por la opinión del perito a la hora de valorar la prueba del ADN.

El robo de identidad mediante datos biométricos es extremadamente difícil de solucionar y podría afectar seriamente a derechos del individuo tal y como reconoce la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos.

Entre sus descubrimientos se encontraron evidencias de que el grupo sanguíneo juega un papel en relación con el desarrollo de la COVID-19 en el ser humano.
"23andMe finds evidence that blood type plays a role in COVID-19", *23andMeblog*, 08-06-2020. Disponible en: https://blog.23andme.com/23andme-research/23andme-finds-evidence-that-blood-type-plays-a-role-in-covid-19/ Fecha de consulta 26-04-2021.

[19] SIERRA, Marcos., FRESNO, Diana. "EEUU recibe una histórica oleada de ataques de ciberseguridad en sus hospitales", *Voz Populi*, 20-02-2020. Disponible en: https://www.vozpopuli.com/economia-y-finanzas/estados-unidos-ataques-ciberseguridad-hospitales_0_1329467297.html Fecha de consulta 26-04-2021.

[20] SEALS, Tara. "COVID-19 Vaccine-Maker Hit with Cyberattack, Data Breach", *Threat post*, 23-10-2020. Disponible en: https://threatpost.com/covid-19-vaccine-cyberattack-data-breach/160495/ Fecha de consulta 26-04-2021.

[21] RUIZ DOMÍNGUEZ, Fernando. *ADN, seguridad y defensa: un cóctel clásico con una nueva dosis de adrenalina,* Documento de Opinión IEEE 96/2020, 02-07-2020, disponible en http://www.ieee.es/Galerias/fichero/docs_opinion/2020/DIEEEO96_2020FERRUI_ADN.pdf Fecha de consulta 26-04-2021.

[22] Incluso del ADN natural mediante al menos dos técnicas.

Por otra parte, entre otras cuestiones, la falsificación de ADN puede generar falsos positivos o llevar a la investigación de un sospechoso inexistente (investigación en la dirección equivocada).

La historia de la investigación policial a veces recoge episodios sobre testimonios forenses falsos en materia de ADN, pruebas falsas de ADN colocadas en el escenario del delito (de hecho, se ha detectado cómo en determinadas prisiones se instruía a los presos sobre la forma más adecuada de hacerlo), o incluso ADN falsificado, lo que ha llevado en diferentes ocasiones a que se solicite una reevaluación de la admisibilidad y fiabilidad de la prueba de ADN, aunque sin ningún éxito en España[23].

Básicamente esto es cierto por cuanto ninguno de los informes sobre ADN que se realizan por parte de las FF.CC.S. españolas tienen en cuenta ni la posible falsificación de ADN ni el potencial uso que se le haya podido dar al ADN, sea este: auténtico, pero de otra persona, o falsificado; y con el objetivo de o bien suplantar la identidad de una persona, o bien el de incriminar o exculpar penalmente a un sospechoso.

De hecho, esto es así porque ni siquiera dichas FF.CC.S. disponen de kits para detectar ADN falso.

Y si todo lo anterior puede ser interesante en materia de Seguridad no hay más que pensar, por ejemplo, en un simple ataque de falsa bandera para entender la importancia de ello en materia de Defensa.

¿Futuro utópico? Encriptación mediante ADN

En otro orden de aspectos, pero continuando con las cuestiones que generan la ciberbioseguridad respecto al ADN en general y a las búsquedas familiares realizadas por las FF.CC.S. de algunos países (no España) en particular, se puede decir que ciertamente se está lejos de poder encriptar y desencriptar automáticamente la información de un dispositivo personal mediante el ADN, pero no hay más que echar la vista atrás cuando en 1995 los dispositivos móviles como los *smartphones* no existían y hoy no se concibe un mundo sin estos.

[23] BOLDEN, Kristen., "DNA Fabrication, A Wake Up Call: The Need to Reevaluate the Admissibility and Reliability of DNA Evidence", *Georgia State University Law Review*, volumen 27, tema 2, artículo 15, (2011). Disponible en: https://readingroom.law.gsu.edu/cgi/viewcontent.cgi?article=1018&context=gsulr Fecha de consulta 26-04-2021.

Igualmente sucederá previsiblemente con la encriptación de la información mediante otros datos biométricos donde sí se ha ido pasando por diferentes estadios previos en los que se han hecho un hueco la voz, el iris, las huellas dactilares, etc., en algún momento y circunstancias concretas surgirá la cuestión del ADN utilizado para proteger información con el tratamiento legal que ello suscita.

Es decir, ya se pasaría a tener en cuenta cómo la información de cualquier tipo, y no solo la personal, contenida en un dispositivo electrónico estaría protegida por una información personal contenida en un elemento biológico como es una célula.

Mientras ese futuro utópico llega[24], o no, queda más cerca uno más sencillo pero que genera ciertas dudas reales y es la protección de la información mediante el perfil genético de una persona. A fin de cuentas, es una secuencia de datos que se puede expresar de múltiples formas pero que, en definitiva, pone sobre la mesa una pregunta ¿Qué pasa cuando la clave para desencriptar la información de un dispositivo es a su vez una información personal como lo es el perfil de ADN de una persona?

Una de las pistas la pueden dar:

- Por una parte, la sentencia Maryland v. King (2013) del Tribunal Supremo Federal de EE. UU., por la que se dictamina que el ADN es comparable en algunos aspectos identificativos con las huellas dactilares. De esta manera parece evidente que la policía podría solicitar al detenido su ADN.
- Y, por otra parte, la decisión del juez estatal de Virginia, EE. UU., Steven C. Frucci en el caso Virginia v. Baust (2014), al dictaminar que un sospechoso «no puede ser obligado [por la policía] a facilitar su código de acceso para acceder a su

[24] Ya existen dispositivos compactos del tamaño de una impresora doméstica que son capaces de analizar el ADN en menos de 60 minutos, por lo que superan a los que utilizan varios cuerpos policiales (España no) que lo analizan en 90 minutos.
De hecho, Donald Trump llegó a afirmar el 27-10-2019, con motivo de su comparecencia por la neutralización del líder terrorista Abu Bakr al-Baghdadi, que la identificación de este mediante ADN «Fue una llamada muy rápida que tuvo lugar unos 15 minutos después de su muerte y fue positiva. Fue 'esto es una confirmación, señor'». (en inglés en el original, traducido por el autor de este trabajo) por lo que según parece, al menos a nivel militar, en EE. UU. se dispondría de una tecnología que permitiría el análisis de ADN y confirmación de la identidad de un sujeto fuente en unos 15 minutos.
President Trump's full announcement on the death of Abu Bakr al-Baghdadi, Disponible en: https://www.youtube.com/watch?v=Q6YvsrGILrw Fecha de consulta 26-04-2021.
XU, Huan., XIA, Anyue., WANG Dandan., ZHANG, Yiheng., DENG, Shaoli., et alter. "An ultraportable and versatile point-of-care DNA testing platform", *American Association for the Advancement of Science*, 06-02-2020. Disponible en https://advances.sciencemag.org/content/6/17/eaaz7445/tab-article-info Fecha de consulta 26-04-2021.

smartphone, pero puede ser obligado a facilitar su huella dactilar para hacer lo mismo»[25].

Es decir, la sentencia Virginia vs. Baust, supone una paradoja tecnológica y jurídica, ya que si la sentencia Maryland vs. King supuso equiparar ADN y huella dactilar, en la sentencia de Virginia aplicada a la encriptación de datos supone que mientras la información contenida en un dispositivo se desencripte mediante un código (que puede ser introduciendo directamente la secuencia de ADN de un individuo) no se puede obligar al detenido a que lo facilite; pero si en el futuro existiera un dispositivo que se desencriptara mediante el análisis del ADN efectuado por el propio dispositivo (lo mismo que se desencripta con una huella dactilar analizada por el propio dispositivo), sí que se podría obligar al individuo a que lo facilitara por aquello de que la huella dactilar y el ADN se encuentran equiparados a nivel judicial según la sentencia Maryland vs. King.

Indudablemente, la disparidad de criterios de los tribunales de cada Estado norteamericano, y la posible casuística, tarde o temprano llevará el tema a que se tenga que pronunciar el Tribunal Supremo Federal de EE. UU., pero seguramente debido a la teoría del mosaico[26] la expectativa de privacidad será mayor tratándose de *smartphones* que de células humanas por mucho que las mismas pertenezcan a un sospechoso o a un familiar del mismo y que estas se equiparen a las huellas dactilares en algunos aspectos.

Conclusiones

El ejemplo más claro de cómo el mundo digital puede afectar al mundo físico se tiene en cómo en 2010 el virus informático Stuxnet fue capaz de paralizar el programa nuclear iraní.

[25] WINTERBOTTOM, Ken. y LONG, Yixuan. "Court Rules Police May Compel Suspects to Unlock Fingerprint-Protected Smartphones", *Jolt Digest*, 12-11-2014. Disponible en: https://jolt.law.harvard.edu/digest/court-rules-police-may-compel-suspects-to-unlock-fingerprint-protected-smartphones ("*cannot be compelled [by the police] to produce his passcode to access his smartphone but he can be compelled to produce his fingerprint to do the same.*"), (en inglés en el original, traducido por el autor de este trabajo) Fecha de consulta 26-04-2021.

[26] La teoría del mosaico se originó a raíz del caso Riley vs. California de 2014, según la cual el acceso a la información contenida en un *smartphone* (sin contar con una orden de investigación de la Cuarta Enmienda de la Constitución de EE. UU.) podría permitir a las FF.CC.S. de dicho país reconstruir los detalles de los movimientos, intereses, comunicaciones, actividades, etc. de su titular, mediante elementos relacionados e interconectados que ningún otro medio de prueba podría hacer por sí solo, incluido un propio vídeo.

Hoy en día la fusión del mundo digital con el biológico plantea nuevos retos y amenazas, tal y como se ha visto, puesto que la misma afecta a cuestiones tan estratégicas como son la creación de organismos con nuevas capacidades, la seguridad alimentaria, la automatización del desarrollo de fármacos o la decodificación del genoma humano.

De hecho, una de las múltiples y posibles teorías sobre la diseminación de la COVID-19, y que en este caso afecta al mundo sanitario, tiene su base en estos planteamientos y que el mismo, que potencialmente se podría haber creado en un laboratorio chino, hubiera sido liberado por algún tipo de virus informático que hubiera afectado a los mecanismos de seguridad física y contención dentro de dicho laboratorio.

Sea como fuere, dicho planteamiento teórico lleva igualmente a poner sobre la mesa las cuestiones jurídicas al respecto que afectan a la Seguridad y la Defensa (como los ataques informáticos a los sistemas de análisis, gestión y almacenamiento de perfiles de ADN, las suplantaciones de identidades, la falsificación del ADN, etc.), y donde evidentemente destaca una global que resulta de sumo interés. ¿Qué mecanismos legales existen para poder exigir una investigación internacional exhaustiva y de campo que, en su caso, permitiera exigir responsabilidades de todo tipo por una pandemia? Según parece, y vista la ausencia regulatoria generalizada a nivel nacional e internacional de la ciberbioseguridad, ninguno más allá del mero ejercicio de la diplomacia y la política[27].

Es decir, en definitiva, y según parece, al menos potencialmente, dicha pandemia tendría que servir como reflexión general y debería ser un punto de partida para articular medidas jurídicas que permitan, en su caso, dar respuesta a los nuevos retos que plantean algunas de las posibles consecuencias derivadas de las amenazas a la ciberbioseguridad

*Fernando Ruiz Domínguez**
Subinspector especialista de Policía Científica
Doctorando en Derecho

[27] "China amenaza a Australia con boicotear su vino si investiga el origen del Covid-19", La Información, (27-04-2020). Disponible en: https://www.msn.com/es-es/noticias/internacional/china-amenaza-a-australia-con-boicotear-su-vino-si-investiga-el-origen-del-covid-19/ar-BB13gU0l Fecha de consulta 26-04-2021.