Terrorismo, tecnología y sociedad en el siglo XXI *

Terrorismo, tecnologia e sociedade no século XXI

Terrorism, Technology and Society in the 21st Century

Juan Acerbi **

En materia de seguridad y prevención criminal, la inteligencia artificial y el procesamiento algorítmico de datos vinieron a posibilitar que una buena parte de las actividades y las comunicaciones que a diario realizan millones de personas sean registradas y analizadas en tiempo real con la finalidad de detectar cualquier indicio de actividad delictiva. Entre las ventajas que trae la aplicación de dicha tecnología al campo social y político, se encuentra el manejo seguro y eficiente de los datos y la realización de procesos sin la injerencia de la subjetividad humana. A su vez, el terrorismo, y particularmente el terrorista que surge de la propia sociedad a la que busca atacar, vino a profundizar el debate en torno a la necesidad de contar con un sistema de monitoreo y vigilancia orientado a registrar y analizar las actividades de la población en pos de resguardar el bienestar general y la seguridad pública. En este artículo abordaremos los alcances y las implicancias que tiene sobre las sociedades contemporáneas el uso de nuevas tecnologías aplicadas al campo de la seguridad y, particularmente, a la lucha de este frecuente y particular tipo de terrorismo.

Palabras clave: terrorismo; seguridad; redes sociales, *big data*; algoritmos

---

* Recepción del artículo: 03/08/2020. Entrega de la evaluación final: 18/09/2020.

** Doctor en ciencias sociales por la Universidad de Buenos Aires, Argentina, y licenciado en ciencia política por la misma universidad. Actualmente se desempeña como investigador y profesor en la Universidad Nacional de Tierra del Fuego, forma parte del Centro Ciencia y Pensamiento de la Universidad Nacional de San Martín y es docente de la Especialización en Lenguaje y Comunicación Digital de la Universidad Nacional de Córdoba. Email: juanacerbi@gmail.com.

Em termos de segurança e prevenção criminal, a inteligência artificial e o processamento de dados algorítmicos tornaram possível que grande parte das atividades e comunicações realizadas diariamente por milhões de pessoas fosse registrada e analisada em tempo real, a fim de detectar qualquer sinal de atividade criminal. Entre as vantagens que têm sido destacadas da aplicação desta tecnologia no campo social e político está o manuseio seguro e eficiente dos dados e o fato de que os processos são realizados sem a interferência da subjetividade humana. Ao mesmo tempo, o terrorismo, e particularmente o terrorismo que surge da própria sociedade que ele procura atacar, veio para aprofundar o debate sobre a necessidade de um sistema de monitoramento e vigilância destinado a registrar e analisar as atividades da população, a fim de salvaguardar o bem-estar geral e a segurança pública. Neste artigo vamos abordar o alcance e as implicações para as sociedades contemporâneas do uso de novas tecnologias aplicadas ao campo da segurança e, em particular, à luta contra este tipo frequente e particular de terrorismo.

Palavras-chave: terrorismo; segurança; redes sociais; *big data*; algoritmos

In terms of security and criminal prevention, artificial intelligence and algorithmic data-processing have made it possible for a large part of the activities and communications carried out daily by millions of people to be recorded and analysed in real time in order to detect any sign of criminal activity. Among the advantages that this technology has brought to the social and political field, the safe and efficient handling of data and the fact that these processes are carried out without human interference are two of its main highlights. At the same time, terrorism, and particularly that one which arises from the very society it seeks to attack, came to deepen the debate on the need for a surveillance system aimed at recording and analyzing the activities of the population in order to safeguard general welfare and public security. In this article we will address the scope and implications for contemporary societies of the use of new technologies applied to the field of security and, in particular, to the fight against this frequent and particular type of terrorism.

Keywords: *terrorism; security; social networks; big data; algorithms*

Introducción

Uno de los hítos que signó el inicio del presente siglo fue, sin dudas, el atentado ocurrido el 11 de septiembre de 2001 en la ciudad de Nueva York. Como bien ha señalado Münkler (2002), a partir de ese hecho Occidente sería testigo de una inversión del escenario bélico en el que el foco del conflicto dejaría de estar situado exclusivamente en Medio Oriente para ubicarse en nuestros centros urbanos más próximos. Sin embargo, y a pesar de la impronta que las imágenes de los atentados causaron en nuestras retinas, los especialistas han señalado que la mayoría de los atentados terroristas ocurridos en el mundo son cometidos por personas surgidas del mismo seno de la sociedad contra la que buscan atentar. Este hecho vino a significar un nuevo y particular desafío en materia de seguridad, pero también en términos sociales y jurídicos debido a las implicancias que conlleva el hecho de que la figura de la sospecha recaiga ya no de manera exclusiva en el extranjero, sino en cada una de las personas que integran nuestras sociedades. Dicha situación vino a legitimar un conjunto de prácticas ética y jurídicamente objetables como, por ejemplo, el hecho de que cada ciudadano pueda ser investigado sin que existan indicios que lo vinculen con algún tipo de actividad delictiva o criminal. Sin embargo, a los escrúpulos éticos se le sumaría el problema material que supone analizar una cuantiosa cantidad de datos que, a través de correos electrónicos, redes sociales, mensajes instantáneos y transacciones comerciales, se actualizan de manera permanente. De acuerdo con una opinión muy difundida, ambos escollos se vieron superados con la implementación de nuevas tecnologías informáticas, especialmente aquellas desarrolladas para el tratamiento inteligente de datos. Gracias a estas tecnologías fue posible desarrollar sistemas capaces de registrar, almacenar y procesar grandes cantidades de información, posibilitando el monitoreo de grandes poblaciones civiles de una manera eficiente y objetiva, minimizando los dilemas legales y maximizando las probabilidades de detectar actividades que atenten contra el bienestar común y la seguridad pública. Sin embargo, a pesar del avance que de por sí supone el desarrollo de tecnologías como la *big data*, el *machine learning* y el procesamiento algorítmico de datos, cabe preguntarse si resultan el medio más idóneo para resolver muchos de los asuntos humanos, especialmente cuando se trata de dirimir quiénes entre nosotros son esas personas que están dispuestas a actuar contra nuestra propia sociedad.

En este artículo abordaremos, en una primera instancia, las razones por las que este tipo de amenaza terrorista supone un desafío particular tanto para los gobiernos y las fuerzas de seguridad como para el conjunto de la sociedad. En una segunda parte, indagaremos las particularidades lógicas y técnicas que caracterizan a las nuevas tecnologías digitales. Nos centraremos particularmente en aquellos dispositivos dedicados a la detección y prevención de acciones criminales e intentaremos dilucidar si efectivamente pueden dar respuestas a un problema de estas características, garantizando de manera eficiente y objetiva el cumplimiento de las bases jurídicas y legales en materia de garantías civiles y derechos humanos.

1. Límites y abordajes de un problema

En materia de prevención criminal, y particularmente en relación con el terrorismo, es posible realizar una división esquemática entre aquellas teorías y discursos que se centran en combatir este tipo de violencia con una lógica propia del escenario bélico de aquellas otras que buscan comprender los orígenes de dichas acciones con el fin de actuar sobre ellos evitando sus consecuencias. En el primer caso nos encontramos con la doctrina ampliamente difundida que entiende que la prevención del terrorismo se realiza a través de la vigilancia masiva, de los ataques preventivos y, en definitiva, de la aceptación del fracaso de las políticas que buscan, a través del poder blando, sensibilizar a aquellas personas que son pasibles de ser movilizadas por ideologías radicalizadas. Un aspecto de suma relevancia es que, bajo esta perspectiva, nos encontramos con la conceptualización del terrorista como alguien que ha dejado de pertenecer a la esfera de lo humano, sea porque es un representante del mal o porque su enajenación le impide el acceso a la razón, siendo situado más allá del ámbito del derecho, de la justicia y de toda posibilidad de diálogo o negociación. Esto se ha visto reflejado en los discursos y las acciones promovidas por la así denominada *War on Terror*, los "bombardeos humanitarios" y la decisión de muchos Estados de no negociar con terroristas, tal como nos lo recuerdan los hechos ocurridos en el teatro Dubrovka de Moscú y que sirven como una muestra de la forma en la que a diario se define buena parte de las acciones a seguir en la lucha contra el terrorismo. La naturaleza de los argumentos que animan las acciones vinculadas a concebir el terrorismo desde esta perspectiva promueven acciones indiscriminadas en las que la solución suele combinar el uso masivo de dispositivos y recursos de inteligencia gubernamental sobre la población local mientras se dirigen ataques preventivos fuera de las propias fronteras, especialmente en aquellos países proclamados terroristas o vinculados a ellos (Groh, 2019; Seliktar y Rezaei, 2020).

Desde otro punto de vista, el terrorismo es entendido como la expresión final de un proceso en el que intervienen un conjunto de factores —fundamentalmente de naturaleza social, política, económica y jurídica— que resultan determinantes para comprender el origen de buena parte de las causas que provocan que simples ciudadanos se vean radicalizados y movilizados a realizar acciones violentas contra la población civil. Como veremos a continuación, desde esta perspectiva fue posible demostrar que un prejuicio fuertemente arraigado en los discursos políticos y mediáticos, y ampliamente difundido en nuestras sociedades, como el de la insania mental del terrorista no tiene verdadero asidero, mientras que otros aspectos frecuentemente ignorados como la segregación social o el desempleo resultan ser factores que inciden fuertemente en el proceso de radicalización de las personas. Dentro de las principales conclusiones a las que han llegado quienes abordan al terrorismo desde esta perspectiva que por economía textual denominaremos holística, consideraremos con particular atención tres de ellas debido la relevancia que tienen tanto para la comprensión del fenómeno como para el posterior desarrollo de nuestros argumentos. Las tres conclusiones son, sucintamente: i) que el ámbito social, económico y político posee una enorme incidencia en el proceso de radicalización de ciudadanos sin antecedentes penales; ii) que existe un amplio consenso de los especialistas en que no es posible definir un perfil psicológico que permita delinear de manera adecuada y precisa la figura del terrorista; y iii) existe un conjunto de variables externas, eventualmente coyunturales,

que funcionan como factores que impulsan a la persona a llevar adelante ideas que hasta ese momento no habían pensado concretar. Veamos con mayor detenimiento cada una de ellas.

El hecho de considerar que hay factores sociales, económicos y políticos que inciden en la subjetividad de una persona favoreciendo su radicalización viene a modificar la perspectiva que sitúa al terrorista como el origen del problema, para concebirlo, más bien, como la expresión resultante de un conjunto de factores. Desde esta perspectiva, el terrorismo es algo que puede ser combatido y prevenido reduciendo los factores que intervienen en el proceso de radicalización, tales como la marginalización, el aislamiento y la discriminación social (Ravndal, 2017; Heitmeyer, 1993; Albrecht, 2003; Post, 2005; Hebberecht y Baillergeau, 2012), la corrupción de las instituciones públicas (Bjørgo, 2005, 2013; Waldmann, 2005), la vulneración sistemática de los derechos y las garantías civiles (Mohammad, 2005; Stohl, 2005; Gries *et al.*, 2015) los altos niveles de desempleo y pobreza (Falk *et al.*, 2011; Bjørgo, 1997; Medhurst, 2000). Como Heitmeyer sintetiza a partir del estudio de las variables económicas y sociales en torno al atentado de 1995 en Oklahoma, este hecho "es también un ejemplo de cómo funciona el marco social" (Heitmeyer, 2005, p. 150) sobre las personas. La segunda conclusión puede, en parte, deducirse de lo dicho anteriormente, debido a que es posible afirmar que el siempre anhelado perfil psicológico del terrorista típico no existe. Las razones de ello son, precisamente, que no existe una patología vinculada con la personalidad del terrorista.[1] En parte, la imposibilidad de definir un perfil psicológico se explica por el hecho de que, así como no existe un solo tipo de terrorismo sino varios, hay un espectro muy amplio de ideologías que animan las acciones terroristas y cada una de ellas se vincula, a su vez, con tipos de personalidad igualmente diversas. De esta manera nos encontramos con grupos o individuos vinculados a ideologías de extrema derecha (supremacistas, nacionalistas, xenófobos, antiLGTBI, antisemitas, islamofóbicos, etc.), de extrema izquierda (separatistas, independentistas, guerrillas y movimientos revolucionarios, etc.), sin dejar de lado a aquellos que actúan movilizados por causas religiosas, económicas o de odio contra determinados valores o políticas (derechos humanos, estado de bienestar, procesos de paz, etc.). En este sentido, podemos afirmar que las especificidades de cada tipo de terrorismo se corresponden con distintos tipos de motivaciones e ideales que permiten suponer, por lo tanto, un perfil psicológico diferente para cada ideología o motivación particular (Post, 2005). A esta dificultad debemos sumar el hecho nada menor de que el terrorismo es un fenómeno sin una definición consensuada[2] (Schmid *et al.*, 1984, 2005), a la que se le suma el hecho de ser un fenómeno dinámico (Schmid, 2011) y difuso (Acerbi, 2019).

La importancia de la tercera conclusión surge para comprender que hay factores sociales, económicos, políticos y jurídicos que pueden influir en la radicalización de personas que previamente no contaban con antecedentes penales ni estaban

1. De acuerdo a Hamm y Spaaij (2017), el porcentaje de personas vinculadas a actividades terroristas que registraron algún tipo de desequilibrio mental oscila entre 10% y 23% del total de casos.
2. A pesar de su uso frecuente en discursos y documentos oficiales, el término "terrorismo" no cuenta con una definición consensuada ni entre los países que conforman las principales alianzas militares ni a su interior, en los que cada agencia gubernamental utiliza su propia definición. Al respecto, consúltese el ya clásico trabajo de Alex Schmid (1984).

vinculadas a movimientos de ideología extrema. Por lo tanto, lo prioritario para los investigadores es identificar las variables de contexto que suelen funcionar como catalizadores del accionar violento. En el mismo sentido en el que Horgan (2005) señala el error que se comete cuando se habla de la raíz del terrorismo (lo cual nos conduce a pensar en razones unicausales y, de alguna manera, en soluciones únicas), es necesario comprender que los factores que pueden favorecer el paso de la teoría a la acción del terrorista son múltiples y eventualmente coyunturales. El análisis de la posibles causas, tanto sociales como políticas y económicas, que pueden desempeñar un papel clave en el proceso de radicalización ha llevado a los especialistas a clasificar dichas variables como "precondicionantes" o "precipitantes". Sucintamente, podemos definir los factores precondicionantes como aquellas cuestiones "de naturaleza relativamente general y estructural capaces de producir una amplia gama de resultados sociales de los cuales el terrorismo es solo uno de ellos" (Bjørgo, 2005, p. 258). Mientras que los precipitantes no son en sí mismos factores que puedan explicar el surgimiento de un accionar terrorista, se sostiene que son estos "los que resultan decisivos al momento de desencadenar actos terroristas" (Heitmeyer, 2005, p. 149). Resulta evidente que para los investigadores dedicados a la prevención del terrorismo resulta necesario limitar los posibles precipitantes a un número razonable de factores, dado que las posibilidades abarcan un sinfín de causas que van desde una crisis económica, el desempleo o una justicia corrupta hasta sucesos personales o familiares que puedan ser dolorosos o traumáticos (Nesser, 2010). A su vez, se puede inferir que el no acotar la cantidad de factores y variables que se consideran como precipitantes lleva a justificar la implementación de medidas preventivas de un carácter tan general que se vuelven al mismo tiempo ineficaces y violatorias de los derechos y las garantías civiles. Esto último puede observarse en la forma en la que han coincidido las políticas que luchan contra el terrorismo implementadas tanto por gobiernos democráticos como por aquellos permanentemente denunciados de vulnerar los derechos civiles. En este sentido, resulta necesario precisar las características del tipo de terrorismo que viene a justificar buena parte de las medidas adoptadas en materia de seguridad.

2. El caso particular: el terrorista de cosecha propia

En los estudios especializados existe un amplio consenso en clasificar las acciones terroristas en dos grandes grupos: el terrorismo internacional y el doméstico. Un caso es tipificado como terrorismo doméstico cuando la localidad en la que se produce el atentado coincide con la nacionalidad del terrorista y la del objetivo del ataque (Berkebile, 2015), mientras que si no se cumplen estos requisitos se lo considera terrorismo internacional. Esta clasificación resulta importante para comprender que, a pesar de la impresión que puede provocar la lectura de la prensa internacional, la mayor parte de los atentados producidos en el mundo, al menos desde 1980 hasta nuestros días, se corresponden con la definición de la variante doméstica (Eubank y Weinberg, 2001; Sandler, 2015; Levin, 2006), estimándose que la tasa media de los mismos se encuentra entre el 80% y el 90% de los atentados realizados a nivel global (Berkebile, 2015). La impresión distorsionada causada por la prensa encuentra sus razones en el tratamiento desigual con el que se suele abordar este tipo de hechos, llegándose a comprobar que la amplificación de un tipo determinado de terrorismo (en

la que el perpetrador es musulmán) supera en un 357% l0a cobertura brindada sobre otras formas de terrorismo doméstico (Kearns, Betus y Lemieux, 2019) especialmente si dichos actos se encuentran vinculados a ideologías de extrema derecha o a crímenes de odio (Taylor, 2019; Powell, 2011). Por su parte, en regiones como América Latina resulta llamativa la prácticamente nula atención que ha recibido la gran proliferación de movimientos identificados con la identidad aria, el nazismo y la supremacía racial, incluso cuando muchos de estos movimientos realizan campañas públicas en los que comunican sus ideales y objetivos. Más allá de las particularidades de cada caso y región, el fenómeno general se repite y, por lo tanto, no debe ser menospreciada bajo la premisa de que se trata de un hecho que atañe exclusivamente a los medios de comunicación, sino que debe ser concebida como parte de una política adoptada por gobiernos que, como si se tratara de una política de Estado, han decidido no utilizar la tipificación de terrorismo doméstico a pesar de padecerlo. Un exjefe de la fiscalía antiterrorista de Nueva York reconoce que existe terrorismo doméstico en los Estados Unidos, pero advierte que no se utiliza debido a que el gobierno y los funcionarios norteamericanos se sienten "más cómodos exportando esa etiqueta, viendo al terrorismo como algo que solo viene del exterior" (Aaronson, 2019). En definitiva, el tratamiento desigual que políticos y medios de comunicación otorgan a los atentados hace que la percepción general se dirija hacia una parte del problema cuyo impacto sobre la realidad de nuestras sociedades es, al menos en términos estadísticos, significativamente menor que aquella otra que suele ser prácticamente ignorada. Sin embargo, el problema aún reviste una cuestión de insoslayable importancia que se relaciona con la identidad del terrorista y con las implicancias jurídicas, políticas y sociales que dicha particularidad posee a la hora de delinear las estrategias vinculadas con la prevención del terrorismo.

Al abordar específicamente el terrorismo doméstico, resulta conveniente especificar el tipo de terrorista que se encuentra asociado a él. Comúnmente se denomina como "terrorista de cosecha propia" o "terrorista de cuño propio" al terrorista que surge del propio seno de la sociedad contra la que busca atentar y que, por su especificidad, se encuentra típicamente asociado al terrorismo doméstico. Dentro de los diversos motivos que suelen movilizar a los terroristas de cosecha propia nos encontramos con que los nacionalismos, el racismo, la xenofobia, la islamofobia, los partidarios de Estados "fuertes" y los reivindicadores de actitudes antidemocráticas[3] encarnan la expresión mayoritaria de la ideología que se encuentra detrás del terrorismo doméstico (Hainsworth, 2008; Piazza, 2017; Freilich *et al.*, 2018; Koehler, 2017, 2018, 2019). Por todo lo expuesto, es posible afirmar que la mayor parte de los atentados terroristas que ocurren en el mundo son motivados por sentimientos de odio vinculados a ideales de extrema derecha y cometidos por terroristas de cosecha propia.

En los últimos años, los crímenes de odio han alcanzado gran repercusión mediática debido al uso de Internet y de las redes sociales como medio para difundir manifiestos o

3. Esta clasificación —con excepción de las expresiones islamofóbicas— es la establecida en el documento "*Far-Right Extremism. A practical Introduction*", publicado por la Radicalisation Awareness Network de la Unión Europea, disponible en: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/ran-papers/docs/ran_fre_factbook_20191205_en.pdf.

incluso transmitir los atentados vía *streaming*. Dos casos han resultado paradigmáticos de esta forma de proceder. Por una parte, el doble atentado perpetrado el 22 de julio de 2011 por Anders Behring Brevik en Oslo, el cual dejó un saldo de 77 personas muertas, siendo la mayoría de ellos niños y adolescentes que disfrutaban de un campamento organizado por el Partido Laboral Noruego. Por otra parte, el caso de Brenton Tarrant, autor del atentado realizado el 15 de marzo de 2019 contra dos mezquitas en la ciudad neozelandesa de Christchurch, dejando como resultado 51 personas muertas y decenas de heridos. En ambos casos los autores de los atentados difundieron manifiestos vía Internet con la intención de inspirar a otras personas a replicar este tipo de acciones. De hecho, el *modus operandi* y el objetivo de Tarrant no solo se ajusta a lo prescripto por Breivik (2011), sino que confiesa en su manifiesto el haberse inspirado en él e incluso haberlo contactado con el fin de "recibir las bendiciones" para llevar a cabo su misión (Tarrant, 2019, p. 18). Un aspecto particularmente relevante, que surge tanto de los manifiestos como de las declaraciones brindadas por ambos terroristas en los interrogatorios, es la importancia que reviste el hecho de actuar con sigilo durante toda la etapa en la que se planifica y se disponen los elementos necesarios para realizar el atentado. Entre las cuestiones más relevantes se destacan las ventajas de actuar como lobo solitario con el fin de pasar desapercibidos ante la policía, los servicios de inteligencia y los vecinos. El propio Breivik especifica con claridad la relación que se establece entre el trabajo requerido para llevar adelante un atentado y el riesgo de ser atrapado por las autoridades en los casos en los que la persona no se encuentra bajo sospecha. De acuerdo con sus cálculos (Breivik, 2011, p. 1471), mientras doce días alcanzan para realizar el trabajo si participan cinco personas, el riesgo de ser descubiertos oscila entre el 90% y el 95%; en cambio, si participan tres personas el tiempo se extiende cuatro días, pero el riesgo solo desciende al 85%, mientras que el accionar en solitario extiende los plazos a 30 días, pero el riesgo se sitúa en el 30%. La dificultad que este tipo de accionar representa para los servicios de inteligencia se encuentra reflejada, tal como había previsto el terrorista noruego, en la alta tasa de éxito que tienen los individuos que actúan como lobos solitarios frente a grupos terroristas de dos o más integrantes (Simon, 2013; Hemmingby y Bjørgo, 2018; Jurczak, Łachacz y Nitsch, 2020).

El caso de Breivik, en parte por las particularidades que lo han caracterizado, ha permitido comprender muchas de las lógicas que operan detrás de los ideales, de la planificación y la ejecución de un atentado perpetrado contra una parte de su propia comunidad.[4] El estudio del caso permite comprender algo que puede parecer trivial, pero que no lo es en absoluto si pretendemos comprender las complejidades que encierra este tipo de terrorismo al que comúnmente se denomina como crímenes de odio. La cuestión es que el término "odio" es utilizado como un eufemismo para explicar lo que no puede ser explicado racionalmente, pero tampoco puede ser atribuido al accionar de una persona mentalmente incapaz. Es ese accionar —incomprensible, reprochable y atroz para el común de las personas, pero racional y meticuloso de acuerdo a los fines que se ha propuesto el terrorista— lo que se vuelve difícil de

4. Las particularidades a las que aludimos refieren a la infrecuente supervivencia del terrorista al atentado. Por otra parte, Breivik se mostró bien predispuesto a hablar sobre los detalles del atentado y de su planificación además de haber difundido sus ideas y experiencias en un manifiesto de más de 1500 páginas. En particular, recomendamos al lector interesado los trabajos de Raffaello (2011) y Hemmingby y Bjørgo (2016, 2018).

anticipar o comprender. Incluso cuando se cuenta con las pruebas suficientes y el propio testimonio del terrorista resulta difícil para los profesionales dedicados a la seguridad establecer criterios que permitan evitar un nuevo atentado. La suma de todos los elementos que hemos expuesto es lo que nos permite comprender en buena medida los desafíos a los que se enfrentan las fuerzas policiales, servicios de inteligencia y de seguridad gubernamentales cuando se trata de lidiar con la amenaza que supone el terrorista de cuño propio. Si nos guiamos por la casuística, todo ciudadano, aunque no tenga antecedentes psiquiátricos ni criminales, que busque gestionar varias tarjetas de crédito o que decida convertirse en un pequeño emprendedor vinculado al sector agrícola, debería ser considerado como una amenaza pública bajo la sospecha de ser un potencial terrorista.[5] Este, evidentemente, es el camino que se ha adoptado a nivel mundial en materia de seguridad antiterrorista y es la razón por la que se ha justificado prorrogar los límites de la vigilancia compulsiva sobre el total de la población, sin importar si existen razones fundadas para hacerlo (Acerbi, 2019) y vulnerando todo tipo de derechos y garantías.

Como es de esperar, esta situación afecta la vida cotidiana de las personas tanto en lo que refiere a las relaciones interpersonales como al hecho de contribuir a reforzar la sensación de que la violación sistemática de derechos que se produce cada vez que las comunicaciones y las acciones de las personas son monitoreadas y registradas son un mal menor pero necesario a la hora de evitar un posible atentado. La solución que se suele presentar ante el supuesto dilema de combatir el terrorismo doméstico de manera eficaz y a la vez evitar los excesos que suelen cometerse cuando se busca erradicarlo es el uso de nuevas tecnologías informáticas. De esta manera, la inteligencia artificial y el uso de *machine learning* y del procesamiento de datos a través de algoritmos se presenta como una forma óptima y segura de procesar monumentales cantidades de datos obteniendo información a partir de la parametrización de variables complejas y realizar diagnósticos o predicciones sobre las personas y sus conductas. A continuación, analizaremos algunos supuestos, tanto en lo que refiere a la supuesta capacidad de dichas tecnologías para prevenir atentados terroristas como a su supuesta eficiencia y objetividad.

3. La tecnología y sus matices

La eficiencia y la objetividad con la que se proclama que las nuevas tecnologías computacionales pueden ser aplicadas al campo social, y particularmente a la lucha contra el terrorismo, debe ser cuidadosamente ponderada antes de permitir que su avance siga extendiéndose. Cualquier intento por precisar los alcances de dicha tecnología no puede obviar los resultados y las conclusiones a las que llegan los profesionales informáticos y los analistas de datos, incluso cuando dichas conclusiones se opongan a nuestros deseos de dar con una tecnología capaz de resolver o lidiar

5. La referencia corresponde al accionar de Breivik sobre la forma en la que evitó llamar la atención al momento de comprar grandes cantidades del fertilizante que utilizaría para fabricar la bomba que explotaría en la zona céntrica de Oslo. También reconocería que, habiendo agotado sus ahorros, gestionó diez tarjetas de crédito para contar con los fondos necesarios para ultimar los detalles del atentado. Ambas cuestiones provocaron, con posterioridad al hecho, que el gobierno noruego revisara diversas normativas.

muchos de nuestros problemas. Como veremos a continuación, y a diferencia de lo que se suele promocionar, la tecnología no es —al menos por ahora— verdaderamente capaz de anticipar acciones criminales y menos aún atentados terroristas; y, aunque es de esperarse que los algoritmos mejoren su desempeño con el tiempo, resta aún analizar la supuesta objetividad de sus procedimientos.

Como bien reflejan los estudios basados en diversas técnicas algorítmicas para detectar tempranamente actos delictivos o revueltas en espacios públicos, se pueden observar algunas mejoras relativas respecto a los tiempos de respuesta de las agencias de seguridad y de la policía. Por ejemplo, utilizando *machine learning* para llevar a cabo el proceso de *clustering*, desambiguación y resumen de los mensajes publicados en Twitter, Alsaedi, Burnap y Rana (2017), se logró mejorar significativamente el proceso de detección de eventos tales como actos de vandalismo, revueltas o protestas. La aplicación de dicha tecnología permitió, circunscribiendo su radio de análisis a un determinado municipio londinense, anticiparse 14 minutos a la policía ante un caso de disturbios en la vía pública o 36 minutos cuando se producía el ataque a un comercio por parte de un grupo de jóvenes. El tiempo máximo se logró con una diferencia de una hora y 12 minutos de anticipación en un caso de saqueos a un negocio, debido a que un usuario subió rápidamente una foto de lo que estaba sucediendo a la red social (Alsaedi, Burnap y Rana, 2017, p. 21). La comparación resulta apabullante, ya que solo unos minutos representan una enorme diferencia en materia de seguridad; sin embargo, los resultados no pueden ser proyectados a una escala global y sobre cualquier tipo de delito. Por una parte, el estudio acota su análisis a un determinado municipio, por lo que su potencia es reducida mientras que, por otra parte, los datos utilizados para el procesamiento de la información son mensajes que han sido intencionalmente publicados y publicitados mediante el uso de *hashtags* en una red social, lo cual es un aspecto que cabe esperar que no se producirá con otro tipo de delitos. A su vez, otras técnicas de procesamiento algorítmico de datos aplicadas a Twitter muestran también avances relativos, pero aún con muchas limitaciones en el alcance y la efectividad como para aspirar a que puedan ser utilizadas de manera masiva (Benigni, Kenneth y Carley, 2017; Alvari, Sarkar y Shakarian, 2019).

Tal vez los casos más ilustrativos de las limitaciones a las que se enfrenta la tecnología en condiciones reales sean brindados por una de las mayores *big tech* de nuestros tiempos. A pesar de su poder tecnológico y del esfuerzo económico realizado para eliminar de su plataforma contenido vinculado a actividades criminales, Facebook se ha transformado en los últimos años en una de las plataformas privilegiadas para difundir propaganda vinculada al terrorismo (Levitt, 2018; Sikkens *et al*., 2016) y se ha convertido en el lugar "por excelencia para la promoción del Jihadismo entre las mujeres" (Carvalho, 2016, p. 49). Una de las razones es que la estructura de la red social y sus algoritmos la vuelven el lugar ideal para las operaciones de scouting (Awan, 2017; Ratnam *et al*., 2018) en las que se busca incorporar a nuevos miembros en grupos y organizaciones vinculadas a acciones delictivas o terroristas, debido a que permite fácilmente tomar contacto y establecer vínculos con personas que no confían en nadie por fuera de su red de contactos (Sikkens *et al*., 2016). A su vez, y a pesar de los logros que la empresa pueda anunciar sobre su capacidad de detectar contenido vinculado al terrorismo jihadista para removerlo rápidamente (Facebook Newsroom, 2018), el gigante tecnológico no fue capaz de detectar ni impedir que

Brenton Tarrant difundiera su manifiesto y transmitiera en vivo —sin interrupciones y siendo replicado por centenares de usuarios— la matanza de 51 personas en marzo de 2019 a través de su servicio de *streaming* Facebook Live.

Sin dudas, la cantidad de información que minuto a minuto se vuelca en las plataformas supera la capacidad de procesamiento actual de la *big data*, a pesar de todo lo que se ha insistido sobre sus virtudes para el tratamiento masivo de información (Corvalán, 2017; Aquaro, 2019; Alzahrani *et al*., 2018). Pero el problema de fondo no es la cantidad de información que circula en Internet y las redes sociales, sino algunos aspectos o limitaciones propias de la lógica algorítmica que no suelen ser mencionadas con el mismo énfasis con el que se promocionan sus virtudes. Por ejemplo, el uso del procesamiento de textos por medio de técnicas que emplean lenguaje natural funciona eficientemente en los casos en los que el lenguaje es utilizado correctamente, pero se ha mostrado inútil cuando se enfrenta a un texto en el que el lenguaje es utilizado informalmente (Becker *et al*., 2011; Farzindar y Wael, 2015; Vieweg *et al*., 2014), o cuando hay "irregularidades, abreviaturas (o) un gran número de faltas de tipeo o errores gramaticales" (Alsaedi, 2017, p. 2), a lo que hay que agregar como problemas la mezcla de idiomas y la alteración de las estructuras de las oraciones (Alsaedi, 2017). Se podrá argumentar, sin dudas, que la tecnología informática aún no ha llegado al grado de desarrollo necesario para sortear estos inconvenientes y detectar de manera rápida y eficiente los mensajes, videos e imágenes que alientan a cometer todo tipo de crímenes. Sin embargo, no debemos perder de vista que aún nos encontramos en los dominios de la circulación pública —o semipública— de contenidos, lo cual significa que resta un largo camino hasta llegar a aspirar a detectar a quienes actúan como lobos solitarios y evitan las redes sociales y utilizan servicios de una *Virtual Private Network* (VPN) para enmascarar sus conexiones a Internet y ocultar el contenido consultado. Por lo tanto, es posible —y necesario— poner en cuestión el supuesto imperio de la *big data* y los algoritmos para llevar adelante procesos a escala masiva y de manera eficiente para, entre otras razones, no delegar la búsqueda de soluciones a problemas que son acuciantes y que interpelan de manera inmediata a los profesionales de las ciencias computacionales, pero también, y muy especialmente, a los investigadores provenientes de las ciencias sociales y las humanidades. Debemos comprender que la creencia generalizada "de que los grandes conjuntos de datos ofrecen una forma superior de inteligencia y conocimiento que puede generar percepciones que antes eran imposibles, con el aura de verdad, objetividad y precisión" (Boyd y Crawford, 2012, p. 663) es falaz debido no solo a sus limitaciones técnicas actuales, sino a la esencia misma en la que se asienta el proceso algorítmico.

Buena parte del nivel de aceptación que tiene la aplicación de las nuevas tecnologías informacionales al campo social, jurídico y político se debe al largo idilio que las ciencias sociales vienen manteniendo con las ciencias exactas y naturales (Adorno, 2001; Savage y Borrows, 2007; Latour, 2009). Sin embargo, la naturaleza de la estadística y la matemática utilizadas por los algoritmos dista en un punto esencial de la utilizada tradicionalmente por las ciencias sociales para llevar a cabo el análisis de un determinado fenómeno social (Andrejevic, 2013, p. 12; Hilbert, Liu, Luu y Fishbein, 2019). Siguiendo a Bolin y Andersson Schwarz (2015), diremos que mientras que las ciencias sociales se centraban:

> "… en variables socio-económicas tales como la edad, el género, la etnia, la educación y sus preferencias (...) la tecnología *Big Data* registra opciones de consumo, posicionamientos geográficos, datos de navegación e información vinculada con el comportamiento de una manera tecnológicamente tan compleja que resulta abstracta para las personas que no son especialistas" (Bolin y Andersson Schwarz, 2015, p. 1).

Es decir, las variables y la posterior codificación que se realiza de las mismas durante el procesamiento algorítmico escapa al entendimiento de la mayor parte de los profesionales que luego aplican, sin ninguna capacidad analítica, las sugerencias que surgen de dicho proceso. En este punto es posible comprender que se realizan, al menos, dos procesos de codificación significativos para el profesional ajeno al campo de la matemática computacional. Al final del proceso de codificación y al establecimiento de correlaciones que se producen al inicio del proceso, se realiza una nueva recodificación para que esos resultados —incomprensibles en sí mismos para los seres humanos– se transformen en un dictamen legible, en una opinión sobre inversiones bursátiles o en el perfil de un sospechoso. Aún con todas las implicancias que tiene este hecho, esto es solo una parte del problema.

Quienes suelen mostrarse a favor de la implementación de esta tecnología para tomar decisiones más inteligentes, veloces y eficientes sobre una población suelen dar por descontado el hecho de que tanto la recolección de datos como su procesamiento se encuentran en evidente relación con la realidad (van Dijck, 2014), sin objetar la naturaleza del dato ni las implicancias éticas o judiciales que acarrea el delineamiento de los *proxys* que operan detrás de la identificación de determinados perfiles (O'Neil, 2016; Pasquale, 2015) —criminales o no— o la más evidente de todas las cuestiones: que la programación es realizada por empleados que trabajan para empresas con intereses que no siempre se corresponden con los ideales de la democracia, la justicia y la virtud cívica (Mager, 2012; O'Neil, 2016). Pero, aunque nada de esto sea simple y se pueda sostener que la naturaleza del dato puede ser problematizada y corregida y que los intereses de las empresas que intervienen en la programación y el procesamiento de información podrían ser auditados (Castelvecchi, 2016; LeCun, Bengio y Hinton, 2015), la naturaleza del *proxy* es algo que no se podrá modificar, y por ello merece nuestra atención.

El concepto de proxy, si bien suele ser asociado con los sistemas informáticos y más allá de su denominación, es algo conocido y empleado por todos nosotros. Cada vez que realizamos una caracterización de otra persona basándonos en aspectos tan dispares como su lenguaje corporal, su vestimenta, la forma en la que nos mira, la zona en la que vive, los comentarios que realiza o la música que escucha estamos reduciendo algo imposible de aprehender —la persona en su compleja totalidad— a un conjunto de características que clasificamos y ponderamos para contar con una evaluación que nos permita saber cómo proceder y dirigirnos a ella. El procedimiento parece simple debido a que, como animales políticos, hemos desarrollado el hábito que nos permite resolver parte de la ansiedad y los temores que nos despiertan las personas, haciendo en parte posible la vida en sociedad. Sin embargo, el hecho de que unos segundos resulten suficientes para tener una impresión sobre si una persona

que cruzamos en la calle es confiable o representa una amenaza solo es posible debido a la enorme cantidad de agrupamientos de datos (*clustering*) y las posteriores codificaciones y relaciones que realizamos sobre lo que vemos de esa persona y que se resumen en un impulso o una sensación que determina la forma en la que nos relacionamos con ella. La noción de *proxy*, entonces, es la representación que nos hacemos de una persona a partir de un número reducido de características. Por supuesto, las características que permiten definir a otro ser humano y su ponderación variarán de una persona a otra y así un hombre puede ser ignorado o menospreciado por algunas personas debido a su etnia, religión, nivel socioeconómico o preferencias culturales, mientras que en otras despierta estima y empatía. El *proxy* funciona de manera análoga en el mundo de las ciencias computacionales y es lo que permite a los algoritmos operacionalizar grandes cantidades de datos para clasificar a las personas en décimas de segundos y agruparlas en determinados segmentos poblacionales, permitiéndoles tratarlas o clasificarlas de determinada manera.

Al igual de lo que ocurre con las personas, el diseño de los *proxies* y la programación de los algoritmos que los procesan no son objetivos, están cargados de los sesgos ideológicos de las empresas o los organismos que encargan la tarea a los científicos de datos, que son quienes diseñan el proceso. La cuestión es que los *proxies* son fácilmente manipulables (como la propia subjetividad humana), pero el agravante en este caso es que los resultados a los que arriban los algoritmos son utilizados para definir una realidad que se justifica a partir de los propios resultados que genera (O'Neil, 2016), mientras que el imperio del "dataísta"[6] (Mager, 2012; van Dijck, 2014) refuerza el hecho de que dichos resultados se encuentren envueltos en una suerte de halo sacral que los vuelve incuestionables. En términos de O'Neil, entendemos que:

> "Las aplicaciones matemáticas que potencian la economía de datos está basada en elecciones hechas por seres humanos falibles. Algunas de estas elecciones se hicieron, sin duda, con las mejores intenciones. Sin embargo, muchos de estos modelos codifican los prejuicios, las incomprensiones y las parcialidades humanas en los sistemas informáticos que manejan cada vez más nuestras vidas. Como los dioses, estos modelos matemáticos son opacos y su funcionamiento es invisible para todos, excepto para los más altos sacerdotes: los matemáticos e informáticos. Sus veredictos, incluso cuando son erróneos o dañinos, son incuestionables y no pueden ser apelados" (O'Neil, 2016, p. 3).

La opacidad del proceso y el devenir de un discurso que promueve el imperio de la soberanía digital (Sadin, 2018a) transforman los resultados en algo de naturaleza casi divina a la que los profesionales no especializados en matemáticas o informática deben responder obedientemente, mientras que nadie puede explicarles a las personas implicadas las razones por las que un seguro médico, un empleo o una reserva en un restaurante les fueron denegadas (O'Neil, 2016). A esa opacidad y a

6. Nos referimos por dataísmo a "la transformación de las acciones sociales en información cuantificada *online* posibilitando el seguimiento en tiempo real (*real-time tracking*) y el análisis predictivo" (van Dijck, 2014, p. 198).

los vicios que puede acarrear la conformación de los proxies debemos agregar que las tecnologías informacionales requieren de la alimentación permanente de datos para funcionar adecuadamente, lo cual fuerza muchas veces a las compañías o a los gobiernos a obtener datos de manera no siempre ética ni legal. Un ejemplo claro de esto puede ser que en los últimos años se ha considerado al teléfono móvil como un proxy de nosotros mismos. Es decir, la localización del teléfono en un momento y lugar específicos es, en principio, considerada como la ubicación del dueño del dispositivo mientras que bajo el mismo supuesto se analiza su perfil como usuario al traducirse y combinarse paramétricamente suposición geolocalizada y el movimiento de sus dedos en la pantalla con los tiempos de consulta, la hora del día y la música que está reproduciendo al tiempo que todo esto se combina, a su vez, con los datos biométricos registrados en su reloj inteligente o sus patrones de consumo a través de las compras realizadas y todo el conjunto de metadatos generados a través de las diversas aplicaciones utilizadas para navegar y comunicarse (Greenfield, 2018; Srnicek, 2018). La aceptación —tácita o no— de que vivimos en la era de la economía del dato —en la que se "aspira a hacer de todo gesto, hálito o relación una ocasión de beneficio", razón por la que se registra, analiza, clasifica y explota la vida integral de una persona (Sadin, 2018b, p. 28)— debe ser entendido no solo como parte del oscurantismo del que se alimenta el Arcano de las tecnologías digitales, sino como un elemento más que se suma a la violación flagrante de las bases jurídicas del debido proceso.

Si consideramos el debido proceso como el conjunto de derechos y garantías que surgen de los tratados y concordatos internacionales, no hay dudas de que, a pesar de que se insista en la potencia y la capacidad de las nuevas tecnologías informáticas, existe en la propia lógica del proceso que anima a dichas tecnologías suficientes motivos para interponer escrúpulos fundados en razones tanto humanitarias como jurídicas (Beresñak, 2020). A los aspectos señalados por los especialistas en matemáticas e informática, que permiten concebir a los algoritmos como "armas de destrucción matemática" (O'Neil, 2016), debemos agregar las particularidades que se dan en el contexto de la lucha contra el terrorismo y al análisis jurídico de datos. Como ya hemos precisado, las características del terrorista de cosecha propia son las que suelen servir de justificativo para implementar medidas de vigilancia y monitoreo sobre poblaciones completas vulnerando sistemáticamente derechos y garantías elementales como la inviolabilidad de la privacidad, sin que existan razones debidamente fundadas (art. V CADDH; art. 12 DUDH; art. 11 inc. 2 CADH) o la presunción de inocencia (art. XXVI DADDH; art.11 DUDH; art. 8 inc. 2 CADH). A su vez, si consideramos su opacidad, no hay dudas de que también se vulnera el principio de sana crítica[7] (Couture, 1979), dado que a los integrantes del Poder Judicial les sería imposible explicar cómo se

7. Nos referimos al sistema de valoración de la prueba denominado de la libre convicción o sana crítica racional, mediante el cual el juez debe llegar a sus conclusiones apoyándose en el razonamiento motivado de las pruebas. Ello significa que el juez "debe proporcionar las razones de su convencimiento, demostrando el nexo racional entre las afirmaciones o negaciones a que llegó y los elementos de prueba utilizados para alcanzarlas" (Cafferata Nores, 1988, p. 47) mediante la descripción del elemento probatorio y su valoración crítica. Al respecto, también nos remitimos al trabajo realizado por Couture (1979).6. Nos referimos por dataísmo a "la transformación de las acciones sociales en información cuantificada *online* posibilitando el seguimiento en tiempo real (*real-time tracking*) y el análisis predictivo" (van Dijck, 2014, p. 198).

conformaron y dispusieron los distintos elementos probatorios que permitieron arribar a una determinada conclusión más allá de que aún resta dirimir la legalidad misma del proceso. La suma de estas cuestiones parece dar suficientes bases para apelar a la doctrina del fruto del árbol envenenado (Cafferata Nores, 1988; Carrió, 1994; Anselmino, 2012), invalidando así todo el proceso posterior, debido a que:

> "… siendo el procedimiento inicial violatorio de garantías constitucionales (...) tal ilegalidad se proyecta a todos aquellos actos que son su consecuencia y que se ven así alcanzados o teñidos por la misma ilegalidad. De tal manera, no solo resultan inadmisibles en contra de los titulares de aquellas garantías las pruebas directamente obtenidas del procedimiento inicial (...) sino además todas aquellas otras evidencias que son 'fruto' de la ilegalidad originaria" (Carrió, 1994, p. 164).

Todo esto pone en cuestión la base tanto lógica como jurídica en la que se sustentan las nuevas tecnologías informáticas, lo cual también viene a resaltar las graves omisiones que cometen quienes asumen que el único desafío que tenemos ante nosotros para liberarnos de la pesada carga de tener que decidir sobre nosotros mismos es el de programar "la inteligencia artificial para que pueda incluir un enfoque jurídico y ético" (Corvalán, 2017, p. 1). Esta suerte de entusiasmo por la tecnología aplicada al campo de las cuestiones humanas no se debe exclusivamente a que se presupone —contrariamente a lo que afirman los especialistas informáticos— que la tecnología es capaz de tratar de manera eficiente el "monstruoso volumen de datos e información" que minuto a minuto se vuelca en las redes, sino que también supone que se pueden superar sin inconvenientes el procesamiento de información mediante lenguaje natural, debido a que "asistimos a la progresiva eliminación de las barreras de comprensión de otras lenguas casi instantáneamente, a partir del desarrollo exponencial del sistema de inteligencia artificial" (Corvalán, 2017, p. 2). La cuestión central aquí no es si al día de hoy la tecnología es capaz de procesar la información de manera eficiente y segura, sino si el origen y la naturaleza de los elementos que intervienen en la elaboración de diagnósticos que impliquen consecuencias directas o indirectas para la vida de las personas son lícitos tanto ética como jurídicamente. El problema del terrorismo representa aquí no solo uno de los problemas más graves y angustiantes de nuestra época, sino que, precisamente por sus características e implicancias para la humanidad, sirve para poner en evidencia que la solución que se nos brinda no puede ser a costa de la dignidad y los derechos humanos. A las dudas razonables que pueden anteponerse en materia ética y jurídica sobre la forma en la que se obtienen datos e información sobre nosotros, y lo abstruso de su procesamiento, debemos agregar que en casos de seguridad pública y, particularmente de terrorismo todo se vuelve mucho más complejo e inaccesible para personas o instituciones ajenas a las fuerzas de seguridad. Si comúnmente resultan inaccesibles las líneas de los códigos de programación por pleitos o denuncias comerciales en casos como el que hemos propuesto aquí, es donde resulta más evidente que "la necesidad de mantener los algoritmos en secreto es ciertamente mayor de lo habitual (mientras que) este interés por el secreto puede extenderse también a algunos de los datos subyacentes, a fin de proteger las fuentes de inteligencia" (Steinbock, 2005, p. 64).

Los diferentes aspectos que hemos abordado deberían ser suficientes para llamar la atención y calmar los bríos de quienes proclaman que es posible sostener un progresivo avance de estas tecnologías sobre ámbitos determinantes para la vida de las personas resguardando, a su vez, los derechos humanos. Finalmente, y como parte de un conjunto de trabajos que exceden el marco del presente escrito, creemos necesario enfatizar la importancia de la figura del terrorista de cosecha para disciplinas como la ciencia política, la sociología y el derecho, debido a que consideramos que representa el paradigma *par excellence* que signará el marco en el que se desarrollarán tanto las relaciones interpersonales como algunas de las disputas más sensibles para el futuro de la humanidad y la vida democrática. Una muestra de esto ha surgido recientemente con el confinamiento de buena parte de la población mundial a raíz de la pandemia de Covid–19 y la rápida respuesta que Google y Apple han brindado en pos de hacer posible el rastreo en tiempo real de las personas para prevenir la propagación del virus. Como hemos afirmado en otra oportunidad, creemos que "el rápido gesto que recientemente han realizado dos de los más poderosos gigantes tecnológicos al ofrecer unir sus recursos con el fin de rastrear los movimientos que cada usuario realiza para permitir detectar y prevenir posibles contagios no responde al diseño de una nueva tecnología sino a la readecuación de los protocolos utilizados para la detección y la prevención del terrorismo" (Acerbi, 2020, p. 1). Es decir, la rápida adaptación de esta tecnología evidencia que los patrones de parametrización ya están dispuestos de manera tal que, sin importar si se trata de un virus o de un terrorista, somos cada uno de nosotros los que representamos una potencial amenaza para otros y, en definitiva, para el bienestar general. Nuestros derechos, así como la identidad, la seguridad, la gubernamentalidad y la soberanía estatal, ya han comenzado a redefinirse y continuarán haciéndolo por lo que resulta imperioso, si no es posible formar parte de los círculos que definen esos nuevos contornos, intentar al menos poner una palabra sobre lo que está aconteciendo a nuestro alrededor.

Conclusiones

Hemos iniciado el artículo abordando la figura de un tipo particular de terrorista debido a los desafíos e implicancias que ella plantea tanto a los profesionales de las ciencias sociales y jurídicas como a los organismos encargados de garantizar la seguridad pública. El análisis de dicha figura nos permitió comprender las razones por las que se suele recurrir a la tecnología en pos de preservar la seguridad jurídica de las personas, pero también como el único medio capaz de analizar la gran cantidad de datos e información que segundo a segundo genera buena parte de la población mundial. Sin embargo, como hemos visto, la supuesta eficiencia con la que se suele caracterizar al uso de la *big data* y el *machine learning* no se constata cuando dicha tecnología es aplicada a gran escala en Internet o en las redes sociales que, como Facebook y Twitter, funcionan como el principal medio de reclutamiento y de difusión de material propagandístico vinculado al terrorismo. De hecho, observamos que, si bien esta tecnología permite mejorar los tiempos en los que la inteligencia policial responde a un hecho delictivo, lo hace de manera relativa y sobre hechos que son públicos debido a que operan sobre la información proporcionada por los usuarios de las redes sociales. En casos de delitos más complejos, es de esperar que el rendimiento de los sistemas informáticos disminuya significativamente, más aún tratándose de lobos solitarios,

que aumentan sus probabilidades de éxito actuando de manera individual y siendo extremadamente precavidos al momento de planificar el atentado y, particularmente, al utilizar Internet. En este sentido, los casos como el de Breivick en Noruega o el de Tarrant en Nueva Zelanda evidencian la brecha entre la publicidad de la que goza el procesamiento algoritmico de datos y sus capacidades actuales.

En una segunda parte, hemos analizado los aspectos técnicos que operan detrás del análisis inteligente de datos. Allí hemos podido comprobar que la supuesta objetividad con la que los algoritmos procesan la información es por lo menos cuestionable debido a la opacidad que recubre el proceso de conformación de perfiles, así como la conformación de los *clustering* y el delineamiento de los *proxies*. Como hemos señalado, dicha opacidad suele ser aceptada como si se tratase de una parte natural del proceso, el cual continúa, de manera recursiva, cuando esos primeros resultados son utilizados como insumos de nuevos procesos, los cuales contribuyen a opacar aún más los resultados dificultando su cuestionamiento por parte de los profesionales que son ajenos a las ciencias de datos. De esta manera, las conclusiones a las que suelen arribar los sistemas de procesamientos algorítmicos de datos se vuelven incuestionables, tanto por la imposibilidad de comprender el proceso en sí como por el hecho de que se ha instalado en nuestras sociedades un dataísmo que tiende a reforzar el paradigma que sitúa el Arcano de la soberanía ya no en el ámbito de las decisiones humanas, sino en la constelación del universo digital.

Resulta insoslayable la necesidad de que los profesionales de las ciencias sociales cuestionen seriamente el lugar al que se los ha relegado frente al avance de las nuevas tecnologías informacionales. Por referirnos solo a los tópicos que hemos tratado aquí —terrorismo, seguridad y tecnología—, el tamaño del desafío ante el que se enfrentan nuestras sociedades y nuestros sistemas políticos resulta evidente y es, por esto mismo, que la humanidad no puede desligarse de la responsabilidad que sobre ella recae. En definitiva, se puede pensar que la tensión entre amenaza (terrorista, bacteriológica, climática o alimentaria) y seguridad continuará marcando el rumbo de la agenda pública en las décadas siguientes y, en este sentido, no debería menoscabarse que en el binomio amenaza–seguridad se asientan las bases del Estado moderno y, en consecuencia, nuestra noción de soberanía.

Bibliografía

Aaronson, T. (2019). Terrorism's double standard: Violent far right extremists are rarely prosecuted as terrorists. The Intercept, 23 de marzo. Recuperado de: https://theintercept.com/2019/03/23/domestic-terrorism-fbi-prosecutions/

Acerbi, J. (2019). Metapolítica. Enemigo público, poder y muerte civil en la tradición republicana. Buenos Aires: Miño y Dávila.

Acerbi, J. (2020). La identidad del virus. Pensar la pandemia. La filosofía interpelada por el COVID-19. Buenos Aires: Miño y Dávila. Recuperado de: https://germyd.wixsite.com/bitacorabfv.

Adorno, T. (2001). Epistemología y Ciencias Sociales. Valencia: Cátedra.

Albrecht, G. (2003). Sociological Approaches to Individual Violence and their Empirical Evaluation. En W. Heitmeyer y J. Hagan (Eds.), International Handbook of Violence Research (611-656). Dordrecht, Boston y Londres: Kluwer Academic Publishers.

Alsaedi, N., Burnap, P. y Rana, O. (2017). Can we predict a riot? Disruptive event prediction using Twitter. Transactions on Internet Technology, 17(2), 1-26.

Alzahrani, A. *et al*. (2018). Countering Terrorism on Social Media Using Big Data. CS&IT, 35-42.

Andrejevic M. (2013). Infoglut. How too Much Information is Changing the Way We Think and Know. Nueva York: Routledge.

Anselmino, V. (2013). Las garantías constitucionales y la regla de exlcusión probatoria en el proceso penal. Anales, 42, 106-119.

Aquaro, V. (2019). Prólogo. En J. G. Corvalán (Ed.), Prometea. Inteligencia Artificial para transformar organizaciones públicas. Buenos Aires: Astrea.

Battersby, J. y Rhys, B. (2019). Christchurch in the context of New Zealand terrorism and right wing extremism. Journal of Policing, Intelligence and Counter Terrorism,1-17.

Becker, H., Mor, N. y Gravano, L. (2011). Beyond trending topics: Real-world event identification on twitter. Proceedings of the 5th International AAAI Conference on Weblogs and Social Media (ICWSM'11), 1-4.

Benigni, M., Kenneth, J. y Carley, K. (2017). Online extremism and the communities that sustain it: Detecting the ISIS supporting community on Twitter. PloS one, diciembre, 1-23.

Beresñak, F. (2020). Comentario crítico sobre un posible nuevo orden jurídico-político: la unidimensionalidad de la norma y el uso de la tecnología. En J. G. González, Á. A. Lozano y G. M. Rodríguez (Dir.), El derecho público y privado ante las nuevas tecnologías (568-574). Madrid: Dykinson.

Berkebile, R. (2015). What Is Domestic Terrorism? A Method for Classifying Events From the Global Terrorism Database. Terrorism and Political Violence, 0, 1-26.

Bjørgo, T. (1997). Racist and right-wing violence in Scandinavia: Patterns, perpetrators and responses. Oslo: Tano Aschehoug.

Bjørgo, T. (2005). Root Causes of Terrorism. Myths, reality and ways forward. Londres: Routledge.

Bjørgo, T. (2013). Strategies for Preventing Terrorism, Basingstoke. Palgrave: Macmillan.

Bolin, G. y Andersson Schwarz, J. (2015). Heuristics of the algorithm: Big Data, user interpretation and institutional translation. Big Data & Society, julio–diciembre, 1-12.

Boyd, D. y Crawford, K. (2012). Critical Questions for Big Data. Information, Communication & Society, 15(5), 662-679.

Breivik, A. (2011). 2083: A European Declaration of Independence.

Cafferata Nores, J. I. (1988). La prueba obtenida por quebrantamientos constitucionales. Temas de Derecho Procesal Penal. Buenos Aires: Depalma.

Cafferata Nores, J. I. (1998). La prueba en el proceso penal. Buenos Aires: Depalma.

Carrio, A. (1994). Garantías constitucionales en el proceso penal. Buenos Aires: Hammurabi.

Carvalho, C. (2016). The Importance of Web 2.0 for Jihad 3.0. Female Jihadists Coming to Grips with Religious Violence on Facebook. Online. Heidelberg Journal of Religions on the Internet, 11, 46-65.

Castelvecchi, D. (2016). Can we open the black box of AI? Nature News, 538(7623), 20-23.

Chichizola, M. (1983). El debido proceso como garantía constitucional. La Ley, Tomo Nro.1983.

Corvalán, J. G. (2017). La primera inteligencia artificial predictiva al servicio de la Justicia: Prometea. La Ley 2017-E-1.

Couture, E. (1979). Estudios de Derecho Procesal Civil. Tomo II. Buenos Aires: Ediciones Depalma.

Delanda M. (1991). War in the Age of Intelligent Machines. Nueva York: Zone.

Eubank, W. y Weinberg, L. (2001). Terrorism and Democracy: Perpetrators and Victims. Terrorism and Political Violence, 13(1), 155-164.

Facebook News Room (2018). Hard Questions: How Effective Is Technology in Keeping Terrorists off Facebook? Recuperado de: https://about.fb.com/news/2018/04/keeping-terrorists-off-facebook/-.

Falk, A., Kuhn, A. y Zweimüller, J. (2011). Unemployment and right-wing extremist crime. Scandinavian Journal of Economics, 113(2), 260-285.

Farzindar, A. y Khreich W. (2015). A survey of techniques for event detection in twitter. Comput. Intell., 31(1), 132-164.

Freilich, J. *et al.* (2018). Patterns of Fatal Extreme-Right Crime in the United States. Perspectives on Terrorism, 12(6), 38-51.

Greenfield, A. (2018). Radical Technologies: The Design of Every-day Life. Londres: Verso.

Gries, T., Meierrieks, D. y Redlin, M. (2015). Oppressive governments, dependence on the United States and anti-American terrorism. Oxford Economic Papers, 67, 83-103.?

Groh, T. (2019). Proxy War. The Least Bad Option. California: Standford University.

Hamm, M. y Spaaij, R. (2017). The Age of Lone Wolf Terrorism. Columbia: Columbia University Press.

Hainsworth, P. (2018). The Extreme Right in Western Europe. Londres y Nueva York: Routledge.

Hamidreza, A., Soumajyoti, S. y Shakarian, P. (2019). Detection of Violent Extremists in Social Media. ArXiv:1902.01577, 1-5. Ithaca: Cornell University.

Hebberecht, P. y Baillergeau, E. (2012). Social Crime Prevention in Europe. Bruselas: Brussels University Press.

Heitmeyer, W. (1993). Hostility and violence towards foreigners in Germany. En T. Bjørgo y R. Witte (Eds.), Racist violence in Europe (17-28). Basingstoke: Palgrave Macmillan.

Heitmeyer, W. (2005). Right-Wing terrorism. En T. Bjørgo (Ed.), Root Causes of Terrorism. Myths, reality and ways forward (141-153), Londres: Routledge.

Hemmingby, C. y Bjørgo, T. (2016). The Dynamics of a Terrorist Targeting Process: Anders B. Breivik and the 22 July Attacks in Norway. Londres: Palgrave Macmillan.

Hemmingby, C. y Bjørgo, T. (2018). Terrorist Target Selection: The Case of Anders Behring Breivik. Perspectives on Terrorism, 12(6), 164-176.

Hilbert, M., Liu, B., Luu, J. y Fishbein, J. (2019). Behavioral Experiments With Social Algorithms: An Information Theoretic Approach to Input–Output Conversions. Communication Methods and Measures, 13, 267-286.

Horgan, J. (2005). The social and psychological characteristics of terrorism and terrorists. En T. Bjørgo (Ed.), Root Causes of Terrorism. Myths, reality and ways forward (44-53). Londres: Routledge.

Jurczak, J., Łachacz, T. y Nitsch, H. (2020). The So-Called 'Lone Wolf' Phenomenon. En B. Akhgar, D. Wells y J. M. Blanco (Eds.), Investigating Radicalization Trends. Case Studies in Europe and Asia. Suiza: Springer.

Kearns, E., Betus, A. y Lemieux, A. (2019). Why do some terrorist attacks receive more media attention than others? Justice Quarterly, 26 [online first], 985-1022.

Koehler, D. (2018). Recent Trends in German Right-Wing Violence and Terrorism: What are the Contextual Factors behind 'Hive Terrorism'? Perspectives on Terrorism, 12(6), 72-88.

Koehler, D. (2017). Right-Wing Terrorism in the 21st Century. The "National Socialist Underground" and the history of terror from the Far-Right in Germany. Londres y Nueva York: Routledge.

Koehler, D. (2019). Violence and Terrorism from the Far-Right: Policy Options to Counter an Elusive Threat. The International Centre for Counter-Terrorism – The Hague, 10.

Latour, B. (2009). Tarde's idea of quantification. En M. Candea (Ed.), The Social after Gabriel Tarde: Debates and Assessments. Londres: Routledge.

Lecun, Y., Bengio, Y. y Hinton, G. (2015). Deep learning. Nature, 521(7553), 436-444.

Levin, J. (2006). Domestic Terrorism. Reno: Chelsea House Publishers.

Levitt, M. (2018). Neither Remaining nor Expanding. The Decline of the Islamic State. Washington: The Washington Institute for Near East Policy.

Mager, A. (2012). Algorithmic Ideology. Information, Communication & Society, 15(5), 769-787.

Manch, T. (2019). Alarming' increase in extreme-right genocide theory came before Christchurch terror attack – report, Stuff News. Recuperado de: https://www.stuff.co.nz/national/christchurch-shooting/114066106/alarming-increase-in-extremeright-genocide-theory-came-before-christchurch-terror-attack--report.

Medhurst, P. (2000). Global terrorism, a course produced by UNITAR. Nueva York: UNITAR.

Mohammad, A. (2005). Roots of terrorism in the Middle East. En T. Bjørgo (Ed.), Root Causes of Terrorism. Myths, reality and ways forward. Londres: Routledge.

Münkler, H. (2002). Die neuen Kriege. Hamburgo: Rowohlt Verlag.

Nesser, P. (2010). Joining jihadi terrorist cells in Europe: Exploring motivational aspects of recruitment and radicalisation. En M. Ranstorp (Ed.), Understanding Violent Radicalisation: Terrorist and Jihadist Movements in Europe (81-114). Londres: Taylor and Francis.

O'Neil, C. (2016). Weapons of Math Destruction. Londres: Penguin.

Pasquale, P. (2015). The black box society: The secret algorithms that control money and information. Cambridge: Harvard University Press.

Piazza, J. (2017). The determinants of domestic right-wing terrorism in the USA: Economic grievance, societal change and political resentment. Conflict Management and Peace Science, 34(I), 52-80.

Post, J. (2005). The socio-cultural underpinnings of terrorist psychology. En T. Bjørgo (Ed.), Root Causes of Terrorism. Myths, reality and ways forward (54-69). Londres: Routledge.

Powell, K. (2011). Framing Islam: An analysis of U.S. Media coverage of terrorism since 9/11. Communication Studies, 62(1), 90-112.

Raffaello, P. (2011). What Have We Learned about Lone Wolves from Anders Behring Breivik? Perspectives on Terrorism, 5(5/6), 27-42.

Ravndal, J. (2017). Explaining right-wing terrorism and violence in Western Europe: Grievances, opportunities and polarisation. European Journal of Political Research, 57(4), 845-866.

Sadin, É. (2018a). La humanidad aumentada. La administración digital del mundo. Buenos Aires: Caja Negra.

Sadin, É. (2018b). La silicolonización del mundo. La irresistible expansión del liberalismo digital. Buenos Aires: Caja Negra.

Sandler, T. (2015). Terrorism and Counterterrorism: An Overview. Oxford Economic Papers, 67(1), 1-20.

Savage, M. y Burrows, R. (2007). The coming crisis of empirical sociology. Sociology, 41(5), 885-899.

Schmid, A. *et al.* (1984). Political Terrorism: A Research Guide to Concepts, Theories, Data Bases and Literature. Amsterdam: North-Holland.

Schmid, A. (2001). The Routledge Handbook of Terrorism Research. Londres y Nueva York: Routledge.

Schmid, A. (2005). Preventing of terrorism. Towards a multi-pronged approach. En T. Bjørgo (Ed.), Root Causes of Terrorism. Myths, reality and ways forward. Londres: Routledge.

Seliktar, O. y Rezaei, F. (2020). Iran, Revolution and Proxy Wars. Suiza: Palgrave Macmillan.

Sikkens E., Van San, M., Sieckelinck, S., Boeije, H. y Winter, M. (2016). Participant Recruitment through Social Media: Lessons Learned from a Qualitative Radicalization Study Using Facebook. Sage Journals, 29(2),130-139.

Simon, J. D. (2013). Lone Wolf Terrorism: Understanding the Growing Threat. Amsterdam: Prometheus books.

Small, D. (2011). The uneasy relationship between national security and personal freedom: New Zealand and the 'War on terror'. International Journal of Law in Context, 7(4), 467-486.

Srnicek, N. (2018). Capitalismo de plataformas. Buenos Aires: Caja Negra.

Steinbock, D. (2005). Data Matching, Data Mining, and Due Process. 40 Georgia Law Review, 1, 1-88.

Stohl, M. (2005). Expected utility and state terrorism. En T. Bjørgo (Ed.), Root Causes of Terrorism. Myths, reality and ways forward. Londres: Routledge.

Tarrant, B. (2019). The Great Replacement.

Taylor, H. (2019). Domestic terrorism and hate crimes: legal definitions and media framing of mass shootings in the United States. Journal of Policing, Intelligence and Counter Terrorism, 14(3), 227-244.

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. Surveillance & Society, 12(2), 197-208.

Vieweg, S., Castillo, C. y Imran, M. (2014). Integrating social media communications into the rapid assessment of sudden onset disasters. Proceedings of the 6th International Conference on Social Informatics, 444–461.

Waldmann, P. (2005). Social-revolutionary terrorism in Latin America and Europe. En T. Bjørgo (Ed.), Root Causes of Terrorism. Myths, reality and ways forward. Londres: Routledge.

Fuentes normativas

Declaración Americana de los Derechos y Deberes del Hombre

Declaración Universal de Derechos Humanos

Convención Americana sobre Derechos Humanos

Cómo citar este artículo

Acerbi, J. (2021). Terrorismo, tecnología y sociedad en el siglo XXI. Revista Iberoamericana de Ciencia, Tecnología y Sociedad —CTS, 16(48), 11-33.