IUS ET SCIENTIA
2023 • Vol. 9 • Nº 2 • ISSN 2444-8478
https://editorial.us.es/es/revistas/ius-et-scientia
https://dx.doi.org/10.12795/IETSCIENTIA • © Editorial Universidad de Sevilla 2023

BUENO DE MATA, Federico: *Investigación y prueba de delitos de odio en redes sociales: técnicas OSINT e inteligencia policial*. Tirant lo Blanch, Valencia, 2023, 328 páginas, ISBN: 9788411696197

Celia Carrasco Pérez
Contratada Predoctoral (FPI). Universidad de Burgos
ccperez@ubu.es 0000-0003-0540-3477

Recibido: 24 de noviembre de 2023 | Aceptado: 06 de diciembre de 2023

En una época en la que el derecho requiere de un pensamiento jurídico comprometido con la respuesta a las nuevas necesidades y exigencias que plantea la era digital, se reclama de los juristas una actitud reflexiva, crítica y responsable ante los nuevos problemas que suscita la tecnología. Una especie de consciencia tecnológica que sea capaz de calar en las diferentes generaciones de operadores jurídicos y permita sentar las bases de la apertura del derecho a la tecnología.

En este nuevo marco interdisciplinar que se reclama, destaca la labor del Catedrático de Derecho Procesal de la Universidad de Salamanca, el profesor Federico Bueno de Mata. Cuya andadura en el marco de la investigación y enjuiciamiento procesal, a la vanguardia en la implementación tecnológica al proceso penal, se consagra en este año 2023 a partir de la publicación de su última monografía *Investigación y Prueba de Delitos de Odio en Redes Sociales: técnicas OSINT e inteligencia policial* en la editorial Tirant lo Blanch.

La obra que en estas páginas se presenta, parte de una problemática real: nuestro estilo de vida fomenta un ambiente propicio para las manifestaciones basadas en el odio y la intolerancia. Una actitud que se ha visto favorecida por la expansión de las redes sociales, donde fácilmente se puede difundir contenido violento, ofensivo y discriminatorio, dificultando a su vez el control, investigación y enjuiciamiento de estas conductas que sobrepasan la libertad de expresión.

El papel que juegan las nuevas tecnologías en la comisión de este tipo de comportamientos hace que la respuesta frente a los mismos requiera de instituciones procesales adecuadas que puedan ofrecer una respuesta completa, desde la investigación tecnológica de la comisión de estos hechos en redes abiertas o cerradas, hasta el posterior tratamiento de las pruebas obtenidas.

A lo largo de tres capítulos, se afronta el desafío que debe asumir el Derecho Procesal como un derecho de garantías, necesario para proteger los derechos y libertades fundamentales de

los ciudadanos en el espacio cibernético. Se proporciona un completo y riguroso estudio interdisciplinar, bajo un marcado carácter tecnológico a partir de tres premisas que sirven de introducción a la obra: la actividad delictiva relacionada con el odio va en claro aumento; los casos que mayor incidencia presentan, son justamente los cometidos a través de redes sociales; y la existencia de una clara percepción de que es necesaria una mejora en el tratamiento procesal de los delitos de odio en redes sociales desde una triple perspectiva: victimológica, investigativa y probatoria.

La presente monografía, aborda de manera práctica y precisa un auténtico desafío para la ciencia procesal, como es la incorporación de las técnicas de inteligencia en la búsqueda y obtención de fuentes de datos a través de fuentes y canales abiertos. Un reto para el autor, que consideramos superado dada la ausencia de doctrina específica en la materia.

El estudio se divide en tres capítulos interrelacionados entre sí, en el que la técnica OSINT, se presenta como una herramienta fundamental en la localización de discurso de odio en las redes sociales.

De esta forma, trataremos de exponer las principales ideas que desarrolla el autor a lo largo de más de 300 páginas de estudio, que convierten esta obra en una valiosa fuente bibliográfica para la ciencia procesal.

I. El primer capítulo titulado *Inteligencia, proceso penal y delitos de odio en redes sociales: especial referencia a la investigación en fuentes abiertas,* le sirve al autor para contextualizar el fenómeno de la sociedad en red ligada a la tecnología, origen de los delitos de odio en Internet. Claro ejemplo de cómo la constante generación de información en Internet puede tener efectos negativos en la sociedad. Y es que la ubicuidad intrínseca a las conductas que constituyen los delitos de odio requiere de acciones de investigación concretas que permitan determinar al autor y proceder a enjuiciar los hechos. Para el autor, dicho cometido parte de un contenido generado en redes sociales, que se podría denominar información electrónica. Es en este momento, en el que se plantea el tratamiento más adecuado que se debe otorgar a esta información, de cara a su aplicabilidad como prueba en un plano jurídico.

En este sentido, el análisis de la información facilitaría la identificación de patrones con importantes implicaciones de cara a un proceso penal. Sin embargo, muy acertadamente, considera necesario diferenciar en el proceso de conformación de pruebas a partir de información contenida en medios tecnológicos, entre información e inteligencia. Una diferencia conceptual clave que apoya toda la argumentación que prosigue la monografía. La inteligencia como generador de conocimiento, el cual, alimentado de información, sirva al proceso como una valiosa fuente de prueba. Esta premisa, le sirve al autor para abordar la aplicación de técnicas de inteligencia en la investigación de delitos de odio en la era de la sociedad en red. Lo que le lleva a situar el ciclo de la inteligencia en el centro del proceso penal cuya finalidad sea la de lograr una prueba que, generada a través de la aplicación de técnicas de inteligencia sirva para enervar la presunción de inocencia.

De esta forma diferencia de un lado la inteligencia criminal, y de otro, la inteligencia de fuentes abiertas. Dentro de esta última se inserta OSINT como modelo de inteligencia idóneo para investigar delitos de odio en redes sociales.

La inteligencia criminal se caracterizaría, por tener un carácter preventivo que poco encajaría en la investigación de los delitos de odio por cuanto la línea que sigue conforma una finalidad preventiva. La inteligencia de fuentes es el tipo de inteligencia que para el autor se presenta como idónea para el proceso penal por delitos de odio. La metodología electrónica de este tipo de tecnología lleva al autor a asentar el concreto estudio de la técnica de inteligencia OSINT, que, pese a sus limitaciones legales, facilita la investigación en las redes sociales abiertas del investigado.

El planteamiento que se propone en este primer capítulo de la técnica OSINT, se basa en abordar su origen y fundamentos, así como su componente principal: los datos, recopilados en espacios virtuales abiertos. OSINT ejemplifica un modelo de inteligencia adaptado a la realidad tecnológica, en el que los datos abiertos marcan una nueva línea para investigar hechos delictivos por odio. El estudio de los datos es fundamental para el autor, quien centra su enfoque en las redes sociales. Un espacio en el que contar con técnicas especificas se vuelve fundamental. Es por ello por lo que se ofrece el análisis de SOCMINT como variante de OSINT, en tanto analiza el método por el cual, mediante esta técnica, es posible la recopilación de datos en redes sociales, en calidad de fuentes accesibles, cuyo análisis conformarían un factor de polarización radical de la comisión de delitos de odio. Armonizando así una herramienta fundamental en la localización del discurso de odio en las redes sociales.

II. Las redes sociales se convierten en el medio ideal de comisión de delitos de odio, lo que inevitablemente lleva al debate de las técnicas de investigación más adecuadas para afrontar el desafío del odio en línea en fase de instrucción. El segundo capítulo, titulado *Las técnicas OSINT como diligencias para la investigación de delitos de odio en redes sociales*, parte de una idea que consideramos fundamental: la expectativa de privacidad. La presente monografía, se presenta como una propuesta innovadora y clave en el reto investigativo del delito de odio cometido por redes sociales de una manera concreta, pero también respecto de las diligencias de investigación tecnológica. La recopilación de información en el marco de la investigación del delito de odio es fundamental, sobre todo desde el momento en el que estos datos pueden obtenerse de las redes sociales. Como acertadamente señala el autor a lo largo de la obra, apenas se conocen estudios doctrinales en la materia, de ahí la importancia del estudio que ofrece el profesor Bueno de Mata.

¿Debería tener control judicial la obtención de datos a través de fuentes y canales abiertos? ¿Hay divergencia entre lo que se considera dato abierto y la funcionalidad de este?

El autor, ofrece un riguroso examen procesal de la inteligencia de fuentes abiertas como técnica aplicada a la investigación en un proceso penal, por cuanto el carácter extensivo y abierto de las redes sociales condiciona las herramientas de investigación criminal. En este sentido, las técnicas OSINT vienen a materializar, desde el punto de vista de las fuentes abiertas, la mejor o más adecuada forma de configurar inteligen-

temente el dato para producir una prueba. El autor retoma la inteligencia de fuentes para conformar el tratamiento procesal de las técnicas OSINT, poniendo su énfasis, de manera acertada, en la diferenciación entre fuente abierta y fuente accesible, y el correspondiente dato accesible y dato abierto, planteando la posibilidad del uso de técnicas OSINT sobre fuentes accesibles, esto es sobre aquellas fuentes en las que hay una expectativa de privacidad frente a las fuentes abiertas, en las que no tiene por qué.

Uno de los desafíos principales que aborda el autor respecto de estas técnicas, es la posible vulneración de los derechos fundamentales en la obtención del dato electrónico. Para tal cuestión, se plantea desde el punto de vista del marco regulatorio, si la técnica OSINT es una diligencia de investigación tecnológica que, como tal, requiera de autorización judicial para romper la expectativa de privacidad y obtener así el dato electrónico como prueba valida. El tratamiento procesal de esta tan innovadora técnica de investigación presenta desafíos que son abordados por el autor, pues ciertamente la recopilación de datos electrónicos puede afectar a derechos fundamentales, hecho que dependerá de la capa de Internet en la que se encuentren estos datos.

De tal manera que este segundo capítulo, presenta una metodología que parte de analizar el marco legal aplicable en la obtención de datos electrónicos en redes sociales para la investigación de delitos de odio. Examinando a su vez, los posibles derechos fundamentales que pueden lesionarse según el tipo de dato que se pretenda obtener. De ahí, la importancia que cobra para el autor la diferenciación entre datos electrónicos abiertos y accesibles, vinculados a cuentas en redes sociales abiertas y cerradas del investigado.

Junto a ello se plantean los presupuestos procesales que deberán tenerse en cuenta, así como el cumplimiento de los principios procesales que actuarán como límite a la actuación práctica.

Son analizadas de una manera rigurosa, las diferentes medidas para la obtención de los datos electrónicos en redes sociales por medio de técnicas OSINT. De un lado aquellas medidas, que, sin ser consideradas diligencias de investigación con amparo en la LECrim, podrán ser usadas para canales abiertos en los que no se necesite autorización judicial: el ciberpatrullaje, o las cuentas títere. De otro, aquellas medidas que encajarían en canales virtuales cerrados: interceptación de comunicaciones y el registro de repositorios telemáticos de datos alojados en la nube. A lo que se añade el estudio de figuras concretas, aplicadas a contenido de odio en redes sociales como la herramienta del agente encubierto o el uso de virus espía. Figuras clave sobre las que, de manera posterior, se puedan aplicar técnicas de inteligencia y configurar así una verdadera prueba de delitos vinculados a odio.

III. Finaliza la obra con el tercero de los capítulos titulado *Prueba de inteligencia policial y delitos de odio en redes sociales***.** En este capítulo el autor se desliga de los anteriores, al pasar del ámbito de la investigación, al desafío que supone desde una óptica procesal la construcción probatoria de los delitos de odio en Internet. Abordar los delitos de odio, requiere de una especial atención a la motivación e intencionalidad que hay detrás de la conducta delictiva. En concreto, la particularidad del delito de odio recae en demostrar que el delito fue motivado por el odio o la discriminación contra un

grupo específico o uno de sus miembros. Sin duda requiere de un enfoque subjetivo que debe contar con las herramientas y garantías procesales adecuadas.

El desarrollo del capítulo se centra concretamente en la prueba de inteligencia policial, para la que el autor propone una teoría general en base a la falta de tratamiento procesal de esta figura. La lectura y estudio de este capítulo termina por corroborar la excelente técnica procesal del profesor Bueno de Mata. Una particular habilidad que ha dejado ver a lo largo de la obra que se presenta, por la que ha dirigido la política jurídica en reglas claras de aplicación tecnológica, ante un derecho penal sustantivo tan complejo como es la concreción de una conducta de odio en un comportamiento típico, antijurídico y culpable en sede procesal.

Hasta el momento, el autor no se había centrado específicamente en determinar la validez probatoria del contenido de los datos recabados, sin embargo, el último de los capítulos resuelve el desafío de la prueba de los delitos de odio en las redes sociales centrado en: la intención y la motivación. El autor parte de los indicadores de polarización radical para probar estas dos facetas detrás del delito de odio, que pese a conformarse como una institución que no cuenta con un reconocimiento legal y jurisprudencial expreso, permite articularse como prueba indiciaria. Se propone un verdadero análisis del tratamiento del delito de odio en Internet, por cuanto la prueba de la motivación e intencionalidad que subyace en los delitos de odio debe revestirse de las garantías propias del Estado de Derecho.

En este sentido, los denominados factores de polarización radical son analizados como parámetros indiciarios que sirvan a la construcción probatoria del odio. La figura de la prueba de inteligencia policial se plantea desde su construcción mediante la prueba de indicios, pero ¿una prueba de inteligencia construida por indicios debe tener el valor de prueba indiciaria? Esta es la pregunta base que da forma al último de los capítulos.

A partir de lo que plantea la Circular 7/2019, de 14 de mayo, de la Fiscalía General del Estado sobre pautas para interpretar los delitos de odio, tipificados en el artículo 510 del Código Penal, se proyecta la utilidad probatoria asociada a la prueba pericial de inteligencia. Manteniéndose crítico respecto de los indicadores de polarización propuestos por la Fiscalía General española, propone otros tantos, concretamente aplicables en el análisis de las redes sociales abiertas del investigado, bajo la denominación de "Decálogo de indicadores de polarización de las redes sociales abiertas", entre los que se incluye el análisis de los algoritmos de recomendación asociados al perfil o en análisis de hashtags.

El autor, Catedrático de Derecho Procesal, apuesta por la prueba de inteligencia policial y la virtualidad probatoria que de la misma se desprende. La metodología de esta debe reunir un proceso de evaluación, de análisis de la información. Para lo que se deberán utilizar técnicas de inteligencia. Aspecto clave por cuanto la diferenciarían de las simples diligencias de investigación; y es que la complejidad de este tipo de delitos junto al contexto tecnológico requiere de herramientas útiles, las cuales deben ser empleadas por especialistas en inteligencia. Un planteamiento que logra relacionar los delitos de odio, con el uso de inteligencia en la investigación y prueba de estos en el marco de un contexto cada vez más tecnológico.

IUS ET SCIENTIA • 2023
Vol. 9 • Nº 2 • pp. 289 -294
ISSN 2444-8478

Nos encontramos ante una obra de máxima actualidad, de carácter crítico y reflexivo, con numerosas indicaciones prácticas, fruto del trabajo del Catedrático de Derecho Procesal Federico Bueno de Mata. La obra *Investigación y prueba de delitos de odio en redes sociales: técnicas OSINT e inteligencia policial* se presenta como lectura obligada para los incipientes y ya aventajados estudiosos de la ciencia procesal, así como para autoridades policiales y judiciales, por cuanto se ofrecen desde una vertiente humanista, líneas clave en la implementación de herramientas tecnológicas de investigación al proceso penal, que permitan en este concreto ámbito, atajar el odio tecnológico.

IUS ET SCIENTIA • 2023
Vol. 9 • N° 2 • pp. 289 -294
ISSN 2444-8478