ĐLESPAÑOL
REVISTA DE LENGUA

Los aportes de la lingüística forense contra el cibercrimen

The Contributions of Forensic Linguistics against Cybercrime

Sheila Queralt
Laboratorio SQ-Lingüistas Forenses
sheila.queralt@cllicenciats.cat
https://orcid.org/0000-0002-0641-0727

Resumen: Este artículo presenta distintas tareas del análisis lingüístico que pueden contribuir a la persecución del ciberdelincuente durante la investigación o a asesorar a los agentes judiciales en la toma de decisiones a través del informe pericial. Este artículo muestra la aplicación de distintos ámbitos de la lingüística forense como pueden ser la construcción de perfiles lingüísticos, el análisis de autoría, el análisis del significado o del lenguaje criminal, en distintos casos relacionados con el cibercrimen. Entre los ciberdelitos analizados se incluyen el ciberacoso, los ataques mediante código malicioso, el discurso de odio o las ciberestafas, destacando de este modo el potencial de la lingüística forense en la lucha contra el cibercrimen.

Palabras clave: Cibercrimen, análisis de autoría, análisis del significado, ciberacoso, discurso de odio, ciberestafas

Abstract: This article presents different tasks of linguistic analysis that can contribute to the prosecution of cybercriminals during an investigation or to aid legal experts to reach decisions through an expert report. This article shows the application of different areas of forensic linguistics, such as linguistic profiling, authorship analysis, the analysis of meaning or criminal language, to different cases related to cybercrime. The cybercrimes analyzed include cyberbullying, cyberattacks through malware, hate speech or cyberfraud. Thus, this contribution highlights the potential of forensic linguistics in the fight against cybercrime.

Keywords: Cybercrime, authorship analysis, meaning analysis, cyberbullying, hate speech, cyberfraud

Del Español: Revista de Lengua, 1, 2023, pp. 259-271
ISSN: 3020-2434 (en línea), 3045-543X (impresa). https://doi.org/10.33776/dlesp.v1.7923

Recibido: 11/10/2022
Aceptado: 12/12/2022

1. Introducción

El número de ciberdelitos a nivel mundial incrementa a una velocidad imparable. Según el Observatorio Español de Delitos Informáticos (OEDI, 2022), hay cuatro factores que facilitan este aumento: la instantaneidad a la que se transmite la información, la afectación global de los incidentes tecnológicos, la falta de medidas legislativas y la multiplicidad de jurisdicciones causante de vacíos legales y, finalmente, la ausencia de medidas de protección que permitan evitar los incidentes. España no es una excepción y los datos reflejan este crecimiento exponencial de los ciberdelitos, entre los cuales destacan el fraude informático, las amenazas y coacciones, la falsificación, el acceso o la interceptación ilícita de información, los delitos contra el honor y los delitos sexuales.

En un gran número de ciberdelitos, la comunicación por parte del delincuente se produce a través de mensajes escritos (Perkins, 2021); de hecho, como señala Williams (2011: 164) la mayoría de las formas de abuso en línea ocurren por el canal escrito. Este artículo tiene como objetivo ilustrar los distintos casos en los que la lingüística forense puede contribuir a la persecución policial y judicial del ciberdelito (Queralt, 2020).

En el caso de la ciberinvestigación, la rama de la lingüística forense más destacada es la del lenguaje como evidencia, ya sea durante el proceso de investigación o en la presentación de pruebas de un proceso judicial. El material que analizan los lingüistas forenses en este tipo de casos evoluciona al ritmo de la tecnología y abarca desde llamadas telefónicas o mensajes de texto y de mensajería instantánea hasta chats de la *dark web* o incluso códigos maliciosos. Las tareas que se llevan a cabo con este tipo de material dependen de cada caso, pero suelen estar relacionadas con el análisis de autoría y el análisis del significado.

2. Análisis de autoría

Hoy en día nos comunicamos a diario y de forma constante a través de los distintos medios electrónicos. En estas comunicaciones digitales dejamos evidencia de nuestras informaciones personales, entre las que destaca, para el propósito de este artículo, el rastro de nuestra forma de hablar y de escribir. De forma inconsciente y automática, cedemos nuestro rastro digital a distintas bases de datos, como pueden ser Facebook, Instagram, Twitter,

ISSN: 3020-2434 (en línea), 3045-543X (impresa). https://doi.org/10.33776/dlesp.v1.7923

comentarios en foros o vídeos, etc. La mayor parte de los usuarios de estas plataformas no son conscientes de la cantidad de información que dejan en acceso abierto y que puede ser utilizada por las autoridades judiciales y policiales (Fortin, Delle Donne y Knop, 2021; Falik, Deuchar, Crichlow y Hodges, 2020), pero también, con fines maliciosos, por los ciberdelincuentes. Algunas de las finalidades delictivas para las que se puede emplear información obtenida en línea son la creación y el uso indebido de identidades falsas y la comisión de estafas (Queralt, 2022b).

Son muchos ciberdelincuentes los que se valen de la comunicación a través de la red para cometer sus crímenes, puesto que el mundo digital les otorga cierta sensación de anonimato mediante plataformas como Tor o Telegram. En efecto, el uso de la tecnología ha magnificado el anonimato percibido, pero también el real y es por este motivo que los investigadores se han focalizado en su lucha (Hughes, Rayson, Walkerdine, Lee, Greenwood, Rashid, May-Chahal y Brennan, 2008). La lingüística forense es una de las disciplinas utilizadas para luchar contra el anonimato en la red y desvelar quién se encuentra detrás de la pantalla desde la que se está cometiendo un delito. En encargos donde el ciberdelincuente se vale del anonimato, desde la lingüística forense se pueden desarrollar dos tareas. Por un lado, la construcción de un perfil lingüístico cuando todavía no existen sospechosos y, por otro lado, el análisis de autoría en el caso contrario o cuando se sospecha que puede haber más de una persona al teclado.

La elaboración de un perfil lingüístico es una tarea que permite asesorar a los investigadores sobre las características sociolingüísticas o el estilo del hablante (Nini, 2019). Algunas de las características lingüísticas individuales que se pueden extraer del análisis de muestras lingüísticas son la edad, el sexo, la ocupación, el nivel educativo, las creencias religiosas y la ideología política de los hablantes. En cuanto a características sociales, se pueden sacar conclusiones acerca del origen geográfico, la etnia o el posible conocimiento o contacto con más de un idioma (Turell, 2010). Aun así, debe subrayarse que la información que se puede proporcionar en un perfil lingüístico depende en gran medida de la muestra de la que se dispone (Queralt, 2014).

Este tipo de análisis puede ser utilizado tanto para trazar nuevas líneas de investigación cuando no se ha identificado a ningún sospechoso como para reducir el número de posibles autores del delito investigado (Picornell, 2012). Por ejemplo, a través del análisis de conversaciones interceptadas, se puede determinar la procedencia geográfica de los miembros de una red de tráfico de personas o asesorar a unidades policiales especializadas para me-

ISSN: 3020-2434 (en línea), 3045-543X (impresa). https://doi.org/10.33776/dlesp.v1.7923

jorar la detección de pedófilos que se hacen pasar por menores de edad en la red (Coulthard, Grant y Kredens, 2011: 5). Así, se ha documentado un número considerable de casos judiciales a cuya resolución ha contribuido la construcción de perfiles lingüísticos basada en muestras digitales (Kniffka, 1996; Leonard, 2005; Schilling y Marsters, 2015; Queralt, 2020).

En cuanto al análisis de autoría, solicitado en casos en que se dispone de uno o varios sospechosos, como se ha dicho anteriormente, consiste en la comparación de los conjuntos de textos disponibles, es decir, los textos anónimos (o dubitados) y los generados por uno o más autores conocidos (textos indubitados). El objetivo de esta comparación es examinar similitudes y diferencias entre los textos que puedan determinar la probabilidad de que hayan sido escritos o no por la misma persona. Este análisis lingüístico implica el estudio de los distintos niveles de la lengua: léxico, sintaxis, ortotipografía, pragmática, etc. A continuación, se proporcionan ejemplos de análisis de autoría en relación con casos de ciberacoso y de ciberataques mediante código malicioso.

2.1 Ciberacoso

El ciberacoso es un acoso agresivo e intencionado a través de medios electrónicos, que se produce de forma repetida por parte de un individuo o un grupo y que se mantiene en el tiempo hacia una víctima que no puede defenderse fácilmente (Ovejero, Yuero, Larrañaga y Moral, 2015: 5). El anonimato que permite el mundo cibernético, como se ha adelantado, dificulta determinar la identidad de la persona que está detrás de una cuenta. Esta situación puede percibirse como una ventaja para atreverse a criticar a otras personas en línea y, en casos extremos, llegar al ciberacoso (Supriadi, Gunawan y Muniroh, 2020).

En investigaciones sobre ciberacoso, la perfilación lingüística puede tener varios objetivos. Entre otros, puede tratar de determinar si el autor de los textos dubitados tiene la misma edad que la víctima, si se trata de un único agresor o, por el contrario, de un grupo de individuos. Cuando el ciberacoso se produce en un contexto escolar, características como la edad, el sexo o la lengua inicial de los autores pueden ser claves para su identificación (Giménez García, 2022). En cambio, cuando la víctima es una persona famosa, el análisis lingüístico suele centrarse en la construcción de la identidad sociolingüística del acosador para estrechar el círculo de sospechosos y algunas

ISSN: 3020-2434 (en línea), 3045-543X (impresa). https://doi.org/10.33776/dlesp.v1.7923

de las características que suelen resultar de más relevancia son el origen geográfico, el sexo, la edad y la profesión.

Además de la elaboración de un perfil lingüístico propiamente dicho, durante la investigación es posible que al lingüista forense se le solicite analizar amenazas, preparar una lista de palabras clave para que otros investigadores puedan crear filtros y bloquear cuentas o mensajes de forma automática e incluso asesorar en las comunicaciones con el agresor para obtener información relevante para la investigación. Una vez se ha localizado el sospechoso, el lingüista forense suele ser requerido para realizar un análisis comparativo de autoría entre los mensajes anónimos y los del posible sospechoso con el fin de determinar la probabilidad de que se trate de la misma persona.

2.2. Código malicioso

El código malicioso es, según González, López y Martínez (2012: 6), «un tipo de programa el cual es diseñado por su creador, con la finalidad de ingresar de forma ilegal en algún equipo informático o bien provocarle algún tipo de daño».

En casos de ataque mediante código malicioso, el lingüista forense puede ser contratado para analizar el lenguaje natural pero también el lenguaje de programación. Esto se debe a que el autor deja, tanto en sus comunicaciones como en el conjunto de comandos que forman el código malicioso, un rastro lingüístico que puede relacionarse, como en los casos comentados anteriormente, con sus características individuales y sociales. Por lo que concierne al código malicioso, el autor puede escoger, en ocasiones, escribir comandos en líneas independientes o agruparlos en bloques mediante el uso de llaves (esto último podría compararse con la estructuración de un texto en párrafos). Por ejemplo, si un autor deseara escribir la función «mostrar la frase A es mayor que 10 y B menor que 8», podría utilizar el siguiente código (**Figura 1**).

```
if (A>10 && B<8) {
    printf(«A es mayor que 10 y B menor que 8\n»);
    }
```

Figura 1

ISSN: 3020-2434 (en línea), 3045-543X (impresa). https://doi.org/10.33776/dlesp.v1.7923

Sin embargo, podría también utilizar otra formulación, reproducida a continuación (**Figura 2**), con igual resultado. Ambas opciones son igualmente válidas y reflejan preferencias lingüísticas del autor.

```
if (A>10 && B<8) printf(«A es mayor que 10 y B menor que 8\n»)
```

Figura 2

3. Análisis del significado

Los lingüistas forenses son requeridos para analizar documentos en los que se disputa el significado de una palabra o un fragmento. Por ejemplo, pueden ser requeridos para determinar el significado más probable de una cláusula de un documento legal que resulta ambigua para una de las partes. No obstante, los casos de ambigüedad no son los únicos en lo que se refiere al análisis del significado. También se analizan los delitos lingüísticos, habitualmente conocidos en inglés como *language crimes* (Shuy, 1993; 1996). Los delitos lingüísticos son aquellos actos ilegales (Gibbons, 2003; Tiersma y Solan, 2012) que se realizan a través del lenguaje (oral o escrito), por ejemplo, amenazar, sobornar, coaccionar, acosar o estafar. A continuación, se exponen dos ciberdelitos para cuya persecución se solicitan actualmente peritajes lingüísticos de análisis del significado, el discurso de odio y las ciberestafas.

3.1 Discurso de odio

El borrado de contenido abusivo en redes es una de las grandes preocupaciones de las redes sociales actualmente, y es que el incremento de mensajes de odio con contenido agresivo en redes no cesa. Estos mensajes pueden resultar ofensivos para sus víctimas, dañar su dignidad y honor o incluso incitar a la violencia en el plano físico. Por estos motivos, son muchos los trabajos que se han centrado en el estudio de este delito y cómo puede combatirse. Desde el punto de vista lingüístico, el análisis y la categorización de este tipo de lenguaje es clave para mejorar su detección. La mayoría de los delitos lingüísticos son susceptibles de cometerse de forma directa e indirecta

ISSN: 3020-2434 (en línea), 3045-543X (impresa). https://doi.org/10.33776/dlesp.v1.7923

(Tiersma y Solan, 2012: 22). El discurso de odio no es una excepción, ya que el lenguaje puede ser abusivo de forma explícita o implícita.

El lenguaje abusivo explícito «siempre tiene una evidencia superficial de abuso con respecto a un objetivo por medio de blasfemias, construcciones performativas, imperativos, modismos, adjetivos o sustantivos con una clara connotación negativa» (Caselli, Basile, Miltrović, Kartoziya y Granitzer, 2020: 5). De este modo, es un tipo de lenguaje que no suele mostrar ambigüedad respecto a su connotación ni a «su potencial para ser abusivo, por ejemplo, lenguaje que contiene insultos raciales u homofóbicos» (Waseem, Davidson, Warmsley y Weber, 2017: 2).

En el caso del lenguaje implícito sucede lo contrario, no suele mostrarse de forma superficial a través de palabras malsonantes, sino que el abuso se sugiere y debe ser inferido por el receptor (Caselli, Basile, Miltrović, Kartoziy Granitzer, 2020, p. 5). Esta falta de superficialidad dificulta su detección, sobre todo, en el caso de detectores automáticos del discurso del odio. Los autores de este tipo de discurso de odio suelen ocultarlo a través de distintos recursos lingüísticos como pueden ser el sarcasmo, la metonimia, la ironía, las lítotes, los eufemismos o la broma.

En este tipo de casos, el lingüista forense es requerido para indicar si en los mensajes se observa lenguaje abusivo constitutivo de un posible delito de odio según nuestro Código Penal. Generalmente, su participación suele ser más frecuente en el caso del lenguaje implícito en el que se debe demostrar que los recursos lingüísticos utilizados camuflan el discurso de odio y la toxicidad del lenguaje resulta menos evidente que cuando se emplea el lenguaje abusivo explícito.

3.2 Ciberestafas

En España, más de la mitad de las denuncias por ciberdelitos están relacionadas con las estafas. Entre las estafas más comunes se encuentran las estafas amorosas. Este tipo de ciberestafas son cometidas, generalmente, por organizaciones criminales internacionales a través de páginas web de citas y redes sociales (Whitty y Buchanan, 2012) o por lobos solitarios (Queralt, 2022a). En estos casos los delincuentes seleccionan, contactan, seducen y engañan para establecer una relación romántica y explotar a su víctima para su propio beneficio económico de manera parasitaria (Burns, 2019).

ISSN: 3020-2434 (en línea), 3045-543X (impresa). https://doi.org/10.33776/dlesp.v1.7923

Las tareas que desempeña el lingüista forense en estos casos pueden ser múltiples, desde determinar el perfil sociolingüístico del estafador, esclarecer si se trata de un lobo solitario o de una organización criminal y/o analizar las estrategias lingüísticas de que se sirven los estafadores para conseguir engañar a la víctima y demostrar si se trata de un *modus operandi* típico de este tipo de estafadores del amor.

El primer paso en este tipo de engaños consiste en seleccionar a la víctima. Para hacerlo, los estafadores utilizan la técnica conocida como pesca del gato o *catfishing* en inglés (Hartney, 2018). Mediante esta técnica el estafador consigue fabricar una identidad digital falsa que sea atractiva para la víctima, ya sea desde el punto de vista físico (a través de la fotografía), de las características del usuario (por ejemplo, edad, profesión, gustos, etc.) o de una combinación de ambas. En muchos casos, los estafadores incluso crearán un círculo de confianza a través de la adhesión de contactos de la futura víctima, para que crea que tienen contactos en común. Este círculo de confianza hace que la víctima baje el nivel de sospecha. Una vez establecido el contacto, el estafador suele declarar su supuesto amor de forma rápida y profunda. El hecho de que conozca los gustos de la víctima favorece que, de nuevo, la víctima baje la guardia. Una vez iniciada la relación, suelen abandonar la plataforma de citas y continuar la comunicación a través de correos electrónicos o WhatsApp. En este punto el delincuente ya ha *preparado* a la víctima para la estafa (Whitty, 2013; Whitty, 2015).

Los estafadores utilizan el lenguaje como un arma para seducir y engañar a sus víctimas (Carter, 2021; Queralt, 2022a). El análisis lingüístico permite observar las estrategias lingüísticas que utiliza el estafador para crear su identidad, manifestar la autenticidad de esta, consolidar la relación e involucrar a la víctima en el fraude.

La construcción de identidades en comunicaciones digitales fraudulentas es un caso inusual porque los estafadores únicamente disponen de sus primeras comunicaciones con las víctimas para establecer confianza (Hiß, 2015). Es decir, no existen otros contextos dados entre el emisor y el receptor que puedan serles útiles para establecer un vínculo con ellas. Por este motivo, el primer objetivo comunicativo del estafador es persuadir a la posible víctima, entablar un vínculo de forma inmediata y establecer una relación «de tú a tú» basada en la confianza mutua. Para establecer ese vínculo ambos interlocutores deben conocerse. Es por ello que el estafador se presenta desde el inicio a la víctima explicando quién es (género, edad, profesión, origen, ideología) e incluso declarando sus expectativas (Queralt, 2022b).

ISSN: 3020-2434 (en línea), 3045-543X (impresa). https://doi.org/10.33776/dlesp.v1.7923

En esas primeras comunicaciones, destaca la repetición de ciertas ideas que ayudan a construir el vínculo de confianza mutua. Entre las palabras que utiliza para describirse destacan «soy una persona confiable», «soy digno de confianza», y también suele insistir en que eso es lo que busca mediante expresiones como «busco a alguien en quien confiar» o «puedes confiar en mí».

Otro de los objetivos que tiene es conocer a la víctima, para poder ir adaptando su perfil. Una de las cosas que más destacan las víctimas es que el estafador las escuchaba atentamente (Queralt, 2022a). Lamentablemente, las víctimas desconocían que esa escucha era interesada y pretendía sacarles el máximo de información para utilizarla en su beneficio y perfeccionar la estafa. En ocasiones incluso se interesan por los secretos de sus víctimas con el fin de poder utilizarlos para extorsionarlas en caso de que se descubra el fraude (Queralt, 2022b).

Estas estrategias lingüísticas propias del inicio de la relación y las que utilizan para la sustracción del dinero pueden ser detectadas por el lingüista forense para probar que las comunicaciones analizadas presentan un patrón comúnmente utilizado por estafadores. Además, el análisis lingüístico de las comunicaciones también puede ser clave para iniciar un proceso judicial contra el delincuente por violencia de género, ya que muchas de estas estrategias son propias de la violencia psicológica sobre la víctima. La víctima ha entablado una relación honesta con el interlocutor y desconoce que se le está manipulando, presionando y engañando para conseguir su dinero (Queralt, 2022a).

4. Conclusión

Los avances tecnológicos han contribuido a un aumento de los ciberdelitos gracias, en gran medida, a la sensación de anonimato que ofrece la red a los delincuentes. Ese incremento galopante provoca que los investigadores tengan que adaptarse y actualizarse de forma constante (Choo y Smith, 2008) para hacer frente a este tipo de delitos. Los agentes policiales intentan disponer del mayor número de herramientas posible para combatirlos y eso incluye recurrir a *más disciplinas* que hace unos años. Es por este motivo que campos como la lingüística forense han recibido un mayor énfasis en los últimos años para ayudar a los investigadores (Hughes, Rayson, Walkerdine, Lee, Greenwood, Rashid, May-Chabal y Brennan, 2008). Los avances en los

ISSN: 3020-2434 (en línea), 3045-543X (impresa). https://doi.org/10.33776/dlesp.v1.7923

métodos utilizados por los ciberdelincuentes también afectan al trabajo de los lingüistas forenses. Por este motivo, no es sorprendente que el trabajo de los lingüistas forenses también esté en constante evolución y crecimiento (Perkins, 2021: 9).

Como se ha podido observar a lo largo de este artículo, el análisis lingüístico de las comunicaciones digitales puede resultar especialmente significativo en el marco más amplio de la lucha contra el cibercrimen para encontrar al autor o autores de un delito, para determinar si existe un delito lingüístico o incluso para detectar y describir patrones típicos de ciertos delitos. Además, los análisis lingüísticos no deben entenderse únicamente como pruebas en una investigación o en un juicio, sino también como una herramienta que pueden utilizar los agentes policiales que hayan sido entrenados. Por ejemplo, Grant y MacLeod (2020) explican cómo se puede entrenar desde el punto de vista lingüístico a los agentes policiales para asumir distintas identidades en internet o incluso para detectar a posibles pedófilos que se hacen pasar por menores.

Los ciberdelincuentes utilizan los avances de la tecnología en su propio beneficio y, sin duda, los lingüistas forenses debemos seguir de cerca esos avances para poder combatirlo. Por ejemplo, debemos avanzar en la investigación del lenguaje creado o modificado por Inteligencia Artificial (IA) que ya está siendo usado en distintos tipos de delitos como pueden ser el uso de *bots* para acosar o robar informaciones en las redes sociales o la conocida estafa del CEO, en la que se suplanta la voz de un directivo para engañar a uno de sus trabajadores y ordenarle que realice una transferencia de dinero. Finalmente, se debe destacar el interés por esta disciplina en España y en otros países como Reino Unido o Estados Unidos para combatir el cibercrimen, y cómo la cooperación entre los lingüistas forenses y los cuerpos policiales ha demostrado tener un impacto positivo en aras de la justicia.

ISSN: 3020-2434 (en línea), 3045-543X (impresa). https://doi.org/10.33776/dlesp.v1.7923

Bibliografía

Audelo González, Jesús; Guevara López, Pedro, y Valdez Martínez, Jorge Salvador (2012). «Definiciones Formales de los Conceptos Básicos en los Modelos de Propagación de Gusanos Informáticos», en AA. VV., *Actas del XIII Congreso Nacional de Ingeniería Electromecánica y de Sistemas*, Ciudad de México, pp. 5-9.

Burns, Asia Simone (2019). «Match.com user bought BMW with $80K from woman he promised to marry, police say», *The Atlanta Journal-Constitution (AJC)*, https://www.fox23.com/news/trending-now/matchcom-user-bought-bmw-with-80k-from-woman-he-promised-to-marry-police-say/955986311/.

Carter, Elisabeth (2021). «Distort, extort, deceive and exploit: Exploring the inner workings of a romance fraud», *The British Journal of Criminology*, 61, 2, pp. 283-302, https://doi.org/10.1093/bjc/azaa072.

Caselli, Tommaso; Basile, Valerio; Miltrović, Jelena; Kartoziya, Inga; y Granitzer, Michael (2020). «I feel offended, don't be abusive! implicit/explicit messages in offensive and abusive language», en Nicoletta Calzolari, Frédéric Béchet, Philippe Blache, Khalid Choukri, Christopher Cieri, Thierry Declerck, Sara Goggi, Hitoshi Isahara, Bente Maegaard, Joseph Mariani, Hélène Mazo, Asuncion Moreno, Jan Odijk y Stelios Piperidis (eds.), *Proceedings of the 12th language resources and evaluation conference*, Marsella, European Language Resources Association, pp. 6193-6202.

Choo, Kim-Kwang Raymond; y Smith, Russell G. (2008). «Criminal exploitation of online systems by organised crime groups», *Asian Journal of Criminology*, 3, 1, pp. 37-59, https://doi.org/10.1007/s11417-007-9035-y.

Coulthard, Malcolm; Grant, Tim; y Kredens, Krzysztof (2011). «Forensic Linguistics», en Ruth Wodak, Barbara Johnstone y Paul Kerswill (eds.), *The SAGE Handbook of Sociolinguistics*, Los Ángeles, Sage, pp. 529-544, https://doi.org/10.4135/9781446200957.

Fallik, Seth Wyatt; Deuchar, Ross; Crichlow, Vaughn J.; y Hodges, Hannah (2020). «Policing through social media: a qualitative exploration», *International Journal of Police Science & Management*, 22, 2, pp. 208-218, https://doi.org/10.1177/1461355720911948.

Fortin, Francis; Delle Donne, Julie; y Knop, Jus-

tine (2021). «The Use of Social Media in Intelligence and Its Impact on Police Work», en *Policing in an Age of Reform. An Agenda for Research and Practice*, Cham, Palgrave Macmillan, pp. 213-231, http://dx.doi.org/10.1007/978-3-030-56765-1_13.

Gibbons, John (2003). *Forensic Linguistics: An Introduction to Language in the Justice System*, John Wiley & Sons.

Giménez García, Roser (2022). *Edat, sexe i llengua inicial en l'elaboració de perfils lingüístics forenses d'adolescents en català*, tesis doctoral, dirigida por Francesc Xavier Vila i Moreno y Sheila Queralt Estévez, tutorizada por Lluís Payrató, Barcelona, Universitat de Barcelona, http://handle.net/10803/675636.

Grant, Tim; y MacLeod, Nicci (2020). *Language and Online Identities: The Undercover Policing of Internet Sexual Crime*, Cambridge, Cambridge University Press.

Hartney, Tyler (2018). «Likeness used as bait in catfishing: How can hidden victims of catfishing reel in relief», *Minnesota Journal of Law, Science and Technology*, 19, 1, pp. 277-303.

Hughes, Danny; Rayson, Paul; Walkerdine, James; Lee, Kevin; Greenwood, Phil; Rashid, Awais; May-Chahal, Corinne; y Brennan, Margaret (2008). «Supporting law enforcement in digital communities through natural language analysis», en Sargur N. Srihari y Katrin Franke (eds.), *International workshop on computational forensics*, Berlín/Heidelberg, Springer, pp. 122-134.

Kniffka, Hannes (1996). «On Forensic Linguistic "Differential Diagnosis"», en Hannes Kniffka, Susan Blackwell y Malcolm Coulthard (eds.), *Recent Developments in Forensic Linguistics*, Fráncfort del Meno, Peter Lang GmbH, pp. 75-122.

Leonard, Robert Andrew (2005): «Forensic Linguistics», *The International Journal of the Humanities*, 3, pp. 65-70.

Nini, Andrea (2019): «Developing forensic authorship profiling», *Language and Law/Linguagem E Direito*, 5, 2, pp. 38-58.

Ovejero, Anastasio; Yubero, Santiago; Larrañaga, Elisa; y Moral, María de la V. (2015). «Cyberbullying: Definitions and Facts from a Psychosocial Perspective», en Raúl Navarro, Santiago Yubero y Elisa Larrañaga (eds), *Cyberbullying Accros the Globe: Gender, Family and Mental Health*, Nueva York, Springer, pp. 1-31, https://doi.org/10.1007/978-3-319-25552-1_1.

Perkins, Ria C. (2021). «The Application of Forensic Linguistics in Cybercrime Investigations», *Policing. A Journal of Policy and Practice*, 15, 1, pp. 68-78.

Picornell, Isabel (2012). «La aplicación de la atribución de autoría en la investigación e inteligencia: La aplicación práctica (y su problemática)», en Elena Garayzábal, Miriam Jiménez y Mercedes Reigosa (eds.), *Lingüística forense: la lingüística en el ámbito legal y policial*, Madrid, Euphonía Ediciones, pp. 79-96.

Queralt, Sheila (2014). «Acerca de la prueba lingüística en atribución de autoría hoy», *Revista de Llengua i Dret*, 62, pp. 35-48, http://dx.doi.org/10.2436/20.8030.02.77.

— (2020). *Atrapados por la lengua*, Barcelona, Larousse.

— (2022a). *Estafas amorosas: El donjuán seduce, convence y manipula*, Larousse.

— (2022b). «Cuando el amor es una estafa», en M.ª Mar Galindo y M.ª Carmen Méndez (eds.), *La lingüística del amor:*

de la pasión a la palabra, Madrid, Pie de Página (col. Tinta Roja), Madrid, pp. 229-246.

Schilling, Natalie; y Marsters, Alexandria (2015). «Unmasking Identity: Speaker Profiling for Forensic Linguistic Purposes», en Alison Mackey (ed.), *Annual Review of Applied Linguistics*, Cambridge, Cambridge University Press, pp. 195-214, https://doi.org/10.1017/S0267190514000282.

Shuy, Roger (1993). *Language Crimes: the Use and Abuse of Language Evidence in the Courtroom*, Cambridge, MA, Blackwell.

— (1996). *Language Crimes: The Use and Abuse of Language Evidence in the Courtroom*, John Wiley & Sons.

Supriadi, Nabila Putri; Gunawan, Wawan; y Muniroh, R. Dian Dia-an (2020). «Bullies' Attitudes on Twitter: A Forensic Linguistics Analysis of Cyberbullying (Systemic Functional Linguistics Approach)», *Passage*, 8, 2, pp. 111-124.

Tiersma, Peter; y Solan, Lawrence M. (2012): «The language of crime», *Brooklyn Law School Legal Studies Research Papers*, 263, http://ssrn.com/abstract=2017652.

Turell, M. Teresa (2010): «The use of textual, grammatical and sociolinguistic evidence in forensic text comparison», *International Journal of Speech, Language & the Law*, 17, 2, pp. 211-250, https://doi.org/10.1558/ijsll.v17i2.211.

Waseem, Zeerak; Davidson, Thomas; Warmsley, Dana; y Weber, Ingmar (2017). «Understanding abuse: A typology of abusive language detection subtasks», en Zeerak Waseem, Wendy Hui Kyong Chung, Dirk Hovy y Joel Tetreault (eds.), *Proceedings of the First Workshop on Abusive Language Online*, Vancouver, Association for Computational Linguistics pp. 78-84.

Whitty, Monica T.; y Buchanan, Tom (2012). «The Online dating romance scam: a serious crime», *Cyberpsychology, Behavior, and Social Networking*, 15, pp. 181-183, https://doi.org/10.1089/cyber.2011.0352.

Whitty, Monica T. (2013). «The scammers persuasive techniques model: development of a stage model to explain the online dating romance scam», *British Journal of Criminology*, 53, 4, pp. 665-684, https://doi.org/10.1093/bjc/azt009.

— (2015). «Anatomy of the online dating romance scam», *Security Journal*, 28, pp. 443-455, https://doi.org/10.1057/sj.2012.57.

Williams, Matthew (2001). «The Language of Cybercrime», en David Wall (ed.), *Crime and the Internet*, Londres, Routledge, pp. 152-166.