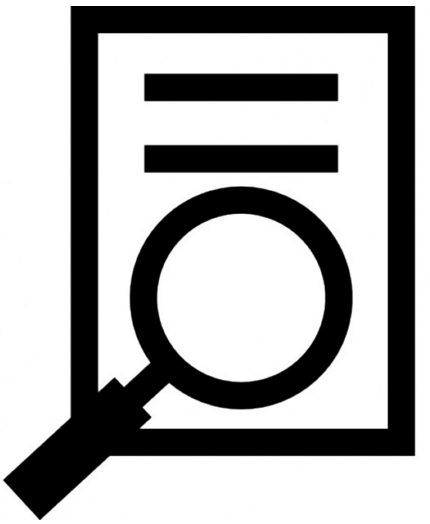
COMUNICACIÓN

MYRIAM REDONDO

VERIFICACIÓN DIGITAL PARA PERIODISTAS

MANUAL CONTRA BULOS Y DESINFORMACIÓN INTERNACIONAL



EDITORIAL UOC

12 h

Verificación digital para periodistas

Manual contra bulos y desinformación internacional

Myriam Redondo

EDITORIAL UOC

Director de la colección Manuales (Comunicación): Lluís Pastor

Diseño de la colección: Editorial UOC
Diseño de la cubierta: Natàlia Serrano

Primera edición en lengua castellana: marzo 2018
Primera edición digital: mayo 2018

Rambla del Poblenou, 156
08018 Barcelona
http://www.editorialuoc.com

Realización editorial: El Taller del Llibre, SL

ISBN: 978-84-9180-130-6

Autora

Myriam Redondo

(@globograma) periodista y profesora universitaria. Ha dedicado su carrera al territorio que vincula la comunicación digital y las relaciones internacionales. Mantiene el blog globograma.com y la iniciativa de debate tertuliainfinita.com.

Su especialidad es la gestión de noticias globales que emergen en la red, con atención a la práctica virtual en las corresponsalías, los contenidos generados por usuarios, la propaganda automatizada y la desinformación en Internet. Ofrece talleres sobre verificación digital desde 2012 en centros educativos y asociaciones periodísticas.

Es doctora en Relaciones Internacionales, máster en Política Europea y técnica avanzada en Obtención de Información con Fuentes Abiertas (OSINT). Actualmente imparte docencia en las universidades Complutense (Relaciones Internacionales) y Francisco de Vitoria (Tratamiento de la Información en Redes Sociales). Ha colaborado con medios como Periodistas-FAPE, Agenda Pública o Revista 5W.

A Macu, Julia y Mateo.

A los científicos que trabajan para evitar la ausencia o desaparición de la memoria.

Agradecimientos

Una alumna y ahora amiga insistió hasta lograr que empezara con el libro. Dice bastante de lo que me aporta la docencia.

Por impulsar esta obra, leerla, mejorarla y/o alegrar la vida mientras la escribía, gracias a muchas personas, entre ellas: Vanesa García, Alicia Rodríguez, Mariluz Congosto, Pilar San Pablo, Remedios Méndez, Rosa Mate, Dalida Cid, Mari Ángeles Martín, Jon Bradburn, María Escudero, Arancha Montejo, Gorka Pérez, Endika Pérez, Virginia Rodríguez, Bernardo Díaz y Juanjo Villalonga.

Índice

Capítulo I
Sobre verificación digital

- Este manual propone técnicas y recursos digitales para la comprobación de contenidos e individuos. Está pensado para periodistas, estudiantes de periodismo, interesados en inteligencia de fuentes abiertas (OSINT) y ciudadanos concienciados sobre los peligros de la desinformación.
- La verificación digital no es una moda (*fake news, posverdad*), sino que remite al buen periodismo de siempre. En esencia trata de responder digitalmente a las preguntas clásicas qué, quién, cuándo, dónde y por qué.
- No llegue a un dictamen utilizando una sola herramienta. Combínelas, realice comprobaciones complementarias. No hay bala de plata, no hay *killer application*.
- Los protocolos o técnicas aquí explicados son más importantes que las herramientas. Los primeros permanecen, las segundas no. Para sustituir un recurso desaparecido busque en Alternativeto (https://alternativeto.net).
- Sea escéptico. «Si tu madre te dice que te quiere, verifícalo» es un mantra habitual en este ámbito.
- Sea transparente. Informe sobre el estado y los pasos tras sus investigaciones.
- Si se equivoca reconózcalo sin dilación. Esta autora ha errado y confesado más de una vez. En verificación lo único imperdonable es tratar de ocultar el fallo.
- Comparta conocimientos en las redes, pida ayuda y agradézcala. La colaboración beneficia. Un tuitero «insignificante» puede aportarle la pista que necesita.

- Observará que muchos procesos de verificación son incompatibles con las prisas de una redacción. Al menos sabrá qué pasos dar prioritariamente, y después es el medio el que deberá decidir si quiere ser rápido o riguroso.
- Tome conciencia de sus posibilidades. Hay recursos muy potentes, pero son de pago y/o están en manos de gobiernos, servicios de inteligencia, partidos políticos o grandes entidades. Aquí se intenta llegar lo más lejos posible con herramientas gratuitas, aunque sean imperfectas y puedan ofrecer resultados erráticos en algún caso.
- Muchos de los recursos apuntados funcionan en inglés y el manual pone énfasis en ejemplos de desinformación internacional. El motivo es que es la más difícil de detectar/gestionar por encontrar al usuario carente de referentes.
- Este texto estará desfasado cuando caiga en sus manos. Trata un ámbito en continua evolución. No deje de formarse. Practique la verificación. Siga a expertos que le actualicen (por ejemplo, los incluidos en la lista @Globograma/Verification).
- La variedad de recursos que menciona el libro puede llegar a abrumar. Léalo sin prisa. Tómese el tiempo necesario para explorar los caminos que abre.
- Si lee algo como esto «v=xfsKeEJ41vg» significa que se recomienda el visionado de un vídeo en YouTube. Entre en esta red social e introduzca en su caja de búsqueda los caracteres que siguen al símbolo =, pero sin el =.
- Si lee una expresión entre corchetes, se le está indicando que introduzca lo que hay dentro de ellos (sin ellos) en un motor de búsqueda.
- Si está leyendo esto es que dispone de la primera cualidad necesaria para ser un buen verificador: la curiosidad. Otras de

importancia son atención al detalle, organización, persistencia, creatividad.

- Disfrute. Está ante un campo fascinante para la profesión. En el futuro el buen periodismo será con verificación y con verificación digital o no será.

Capítulo II
Breve historia de la verificación digital

El 11 de septiembre de 2011, los atentados contra las Torres Gemelas congregan a la sociedad internacional en torno a las pantallas. La gente quiere saber y en la web los grandes medios no pueden ofrecer todo lo que se busca. Los blogs van dejando caer testimonios impactantes, condolencias... Suele señalarse este como uno de los momentos de evolución clara del llamado **periodismo ciudadano**, en el que quienes captan y difunden material de interés no son profesionales de la comunicación. Su aparición enriqueció el circuito informativo, haciéndolo más democrático y espontáneo, pero también fue muy discutida. Para bastantes trabajadores de los medios suponía una usurpación de sus funciones y una pérdida de calidad en los contenidos.

26 de diciembre de 2004. Navidad. Un terremoto en Indonesia provoca un tsunami en el sudeste asiático. Es de tal magnitud que se siente desde Tailandia hasta el este de África. A las grandes redacciones empiezan a llegar imágenes amateur. En la BBC un grupo se organiza para recopilarlas y entiende que la circunstancia volverá a repetirse con cada noticia de alcance global. La cadena crea la UGC Hub (User Generated Contents Hub) o Unidad de Contenidos Generados por el Usuario (CGU). Cumplió diez años en 2015 convertida en referente de un modo de ver la actualidad: asume que ya siempre estará llena de aportaciones no profesionales de valor.

La expresión CGU fue mejor aceptada porque indicaba cierta participación de las redacciones: una persona generaba la infor-

mación; los periodistas la procesaban. Los ciudadanos veían reconocida su relevancia; los profesionales sentían que se salvaguardaba la suya. Con el avance de la tecnología y la miniaturización de los teléfonos esas aportaciones adquirirían calidad formal y relevancia. Actualmente, pueden convertirse en portada de un informativo de televisión prácticamente sin edición.

Los CGU fueron creciendo en paralelo a la expansión de la llamada Web 2.0 (concepto acuñado por Tim O'Reilly en 2004): Internet evolucionaba permitiendo a las personas interactuar con protagonismo real. Ya no solo consultaban contenidos, también los podían transmitir. Gestores de contenido como Wordpress (https://wordpress.com) simplificaban la creación de blogs de apariencia profesional. Con el tiempo la Web 2.0 ya no solo facilitaría la difusión de textos, sino también la de elementos multimedia: hoy grabamos desde el móvil pero también editamos y emitimos desde él. El culmen de esta progresión lo constituyen precisamente las redes sociales, en las que la publicación de contenidos es sencilla y ágil.

1. Materiales testimoniales

Dentro de los CGU han ganado importancia los *eyewitness media*, expresión que podría traducirse como **materiales testimoniales**. Son fotografías o audios pero sobre todo vídeos que testigos de un acontecimiento excepcional graban y envían, normalmente desde su teléfono inteligente. Interesan sobre todo los que revelan alguna realidad oculta o suponen pruebas de crímenes, atentados o ataques contra los derechos humanos. Son publicados por cualquier usuario en una red social o sistema de mensajería instantá-

nea. A partir de ahí se expanden por el universo digital y se convierten en una pieza codiciada para la prensa. Un ejemplo sería el vídeo que mostró el linchamiento y la muerte del líder libio Muamar el Gadafi (v=Lx12hHhugj8). Otro sería el que captó el asesinato de un policía tras el ataque a la revista *Charlie Hebdo* en enero de 2015 (v=GX8KN6zlJYI). Tras hacerse viral, el autor se arrepintió de su divulgación.

Los materiales testimoniales han provocado un debate similar al que se produjo con el periodismo ciudadano. Para algunos expertos se pierde calidad y los medios abusan de ellos, pero muchos aspectos positivos los imponen en el mercado. Primero, es probable que en el futuro las primeras grabaciones de cualquier suceso las aporten testigos, no profesionales. Segundo, el periodismo gana en autenticidad. ¿Quién se resiste a las imágenes de una montañista ante una avalancha (v=p0t3Q2NNmq0)? Tercero, tras la obtención de ese material puede haber habido un buen trabajo. Antes los periodistas tenían que conseguir los mejores testimonios en el lugar del suceso, ahora además han de investigar si existen imágenes del mismo. Suele citarse como buen ejemplo de ello el artículo de Alissa J. Rubin sobre Farkhunda Malikzada, una afgana a la que una turba asesinó tras una acusación sin fundamento. Acceder a la grabación permitió dar a conocer el caso e iniciar un juicio.[1] Cuarto y último, la realidad económica se impone: estos contenidos son baratos, captan la atención del usuario y atraen publicidad, así que además de emplearse

1. La obtención del vídeo y su tratamiento periodístico tuvieron peso a la hora de concederle a la corresponsal el Premio Pulitzer en 2015. Rubin, Alissa J.: «Flawed justice after a mob killed an Afghan woman», *The New York Times*, 26-12-2015 [https://www.nytimes.com/2015/12/27/world/asia/flawed-justice-after-a-mob-killed-an-afghan-woman.html; consultado el 2-1-2018].

cuando no se dispone aún de imágenes profesionales también se convierten en recursos de apoyo con gancho.

Las agencias apuestan crecientemente por el uso de CGU. Associated Press los ofrece verificados a sus clientes desde mayo de 2017. Un estudio de la iniciativa académica Eyewitness Media Hub (https://www.eyewitnessmediahub.com) reveló en 2015 cómo estas aportaciones ya formaban parte natural del menú de los medios. Durante tres semanas los enlaces incluidos en las portadas web de ocho grandes cabeceras dirigieron a una media conjunta diaria de 171 piezas con tales contenidos.[2] Los utilizan medios grandes y pequeños, de calidad y sensacionalistas. Abundan más en estos últimos pero pueden configurar **propuestas periodísticas ejemplares** en las grandes marcas. Según el estudio, en *The New York Times* estos productos se integraban en «vídeos de alta calidad que añadían profundidad y color a crónicas internacionales, revelando las posibilidades que ofrecen los materiales testimoniales a la hora de informar a las audiencias de un modo que simplemente no sería posible sin ellos».

Un 24% de todos los contenidos hallados sobre ISIS/DAESH incluían CGU. Gracias a estos materiales se han podido cubrir escenarios como las primaveras árabes o la guerra en Siria, procesos que les dieron gran popularidad. Cuando la prensa es expulsada de territorios hostiles son ciudadanos los que corren el riesgo de grabar para poder denunciar ante el mundo. Y los medios recogen esas contribuciones.[3]

2. Las cabeceras analizadas fueron *The New York Times, Clarín, Daily Mail, The Guardian, The Cairo Post, The Times of India, People's Daily y The Sydney Morning Herald.* Brown, Pete: *A global study of eyewitness media in online newspaper sites*, Eyewitnessmediahub.com, 12-2-2015 [http://eyewitnessmediahub.com/research/user-generated-content; consultado el 2-1-2018].

3. Sobre la Primavera Árabe y su seguimiento a través de las redes sociales se recomienda: Carvin, Andy: *Distant witness. Social media, the Arab Spring and a journalism revolution*,

Precisamente por esa posible peligrosidad se recomienda extremar el cuidado a la hora de comunicarse con estos testigos. Fergus Bell publicó una imagen ante una noticia internacional ocurrida en julio de 2016. Mostraba que ningún periodista hacía nada malo al solicitar material a un mismo ciudadano vía Twitter, pero todos juntos constituían una situación agobiante para él.[4] Son muy criticados los reporteros que no solo apremian a los usuarios para conseguir derechos sobre sus imágenes, sino que les proponen grabar más cosas mientras aún hay peligro. Algunas entidades han emitido recomendaciones básicas para proteger a testigos en conversaciones sobre noticias de última hora.[5] Lo primero es evitar poner en riesgo a las personas involucradas, sobre todo si están todavía en situación comprometida. Tampoco debe olvidarse nunca pedir permiso ni atribuir el material a su verdadero autor más allá de un «visto en Twitter». La atribución debe ser para el autor de la grabación, no para quien la publica. Hay que averiguar quién es esa persona.

Amazon.com, enero de 2013 [https://www.amazon.com/Distant-Witness-Andy-Carvin/dp/1939293022; consultado el 2-1-2018]. Este periodista se convirtió en «DJ de la información mundial» en aquellos acontecimientos, demostrando gran pericia para seleccionar las contribuciones ciudadanas de calidad.

4. Bell, Fergus: https://pbs.twimg.com/media/Cm2RdNBWEAEXepl.jpg:large [@fergb; consultado el 2-1-2018].

5. Estos artículos aportan consejos para comunicarse con testigos en caso de noticia de alcance, aunque este es un ámbito todavía sometido a muchos debates legales y éticos. Reid, Alastair: «How can journalist better protect eyewitness on social media during breaking news», Firstdraftnews.com, 14-4-2016 [https://firstdraftnews.com/how-can-journalists-better-protect-eyewitnesses-on-social-media-during-breaking-news/; consultado el 2-1-2018]. Reid, Alastair: «5 lessons from eyewitness conversations in breaking news», Firstdraftnews.com, 22-7-2016 [https://firstdraftnews.com/lessons-from-eyewitness-conversations-in-breaking-news-journalism/; consultado el 2-1-2018]. Wardle, Claire: «A journalist guide to working with social sources», Firsdraftnews.com, septiembre 2016 [https://firstdraftnews.com/wp-content/uploads/2016/09/First-Draft-A-Journalists-Guide-To-Approaching-Social-Sources.pdf?x29719; consultado el 2-1-2018].

2. Verificación digital

Es difícil mencionar nombres y fechas en un proceso que tiene mucho de construcción común, y especialmente de ciudadanos anónimos.

En las líneas que siguen son todos los que están pero con seguridad no están todos los que son. Disculpas por ello.

En 2004 el periodista canadiense Craig Silverman inicia un blog llamado «Regret the error» (Lamenta el error), dedicado a informaciones que han sido objeto de rectificación y, progresivamente, a sus procesos de expansión en redes. El Instituto Poynter (http://www.poynter.org) decide albergarlo algunos años después, cuando ya goza de gran prestigio. Silverman es hoy responsable de información sobre medios en Buzzfeed. Su nombramiento fue un hito, ya que solían encabezar esta sección periodistas del ámbito de la prensa tradicional. «Consumimos información de un modo al que todavía no estamos acostumbrados como humanos», ha dicho.

El 2010 Mark Little crea en Dublín una pequeña empresa llamada Storyful (http://www.storyful.com). Detecta tales posibilidades en el campo de los UGC que decide apostar por su verificación. Pronto se hace con clientes como *The New York Times*, Reuters, BBC o *The Wall Street Journal*. Avanzando como «la agencia del siglo XXI», la empresa es adquirida en 2013 por News Corp (Ruper Murdoch), una compra que sanciona la importancia de los CGU en el circuito mediático. Storyful reconocía la importancia de la gente a la hora de investigar noticias relevantes. Más que crear su propio contenido, detectaba aportes ajenos de interés e iba relatando paso a paso cómo los verificaba hasta encajar la información disponible con los hechos. Preguntaba por los datos que aún no tenía,

pedía que le ayudaran a contrastar. Entre todos se iba haciendo crecer la historia.[6]

En 2012 un británico de alias «Brown Moses» comienza a analizar vídeos sobre la guerra de Siria desde casa. Visiona exhaustivamente todas las fuentes disponibles para entender mejor el conflicto. Pronto se ha convertido en un experto, especialmente en lo relativo a armamento. No solo encuentra buen material, sino que además explica hallazgos complejos de modo didáctico. Al final esta tarea se convierte en trabajo a tiempo completo y ya convertido en estrella Eliot Higgins (su nombre verdadero) crea una campaña de financiación distribuida o *crowdfunding* que le permite crear el colectivo de verificación digital avanzada Bellingcat (https://www.bellingcat.com).

Higgins colabora además con DFRLab (https://twitter.com/dfrlab), un laboratorio del centro de análisis The Atlantic Council centrado en investigación digital forense (*digital forensics*). El hecho de que esta entidad sea estadounidense y la dimensión política que han adquirido los descubrimientos del británico le han hecho receptor de mayores críticas que en sus comienzos independientes. Hay voces muy hostiles que proceden de Rusia, pero Bellingcat es actualmente referente indiscutible. Aplica con gran pericia al periodismo e Internet técnicas propias de la inteligencia de fuentes abiertas (Open Source Intelligence, OSINT). Este campo, habitualmente reservado al mundo de la seguridad militar o corporativa, se basa en el recurso a fuentes de información no clasificadas, es decir, accesibles de forma pública ya sea de modo gratuito o previo pago.

6. Mac Suibhne, Eoghan: «Syrian slaughter: investigating alleged war crimes via social media», Storyful.com, 5-11-2012 [https://web.archive.org/web/20121111050306/; http:/storyful.com:80/stories/45612; consultado el 2-1-2018].

Los hallazgos OSINT complementan e incluso pueden superar los que se consiguen con otras vías tradicionalmente más cerradas, exclusivas, de la inteligencia (espías, diplomáticos y otras fuentes humanas o HUMINT, interceptación de señales o SIGINT, etc.).[7]

Las ONG han sido igualmente activas en el impulso a la verificación digital por la importancia que tiene para los derechos humanos. Destacan Human Rights Watch y sobre todo Amnistía Internacional, así como el colectivo Syrian Archive (https://www.syrianarchive.org). Formado por activistas locales y apoyado por periodistas, abogados, expertos técnicos y organizaciones humanitarias internacionales, se dedica a detectar, verificar y archivar materiales procedentes de la guerra de Siria. El objetivo es que permitan algún día denunciar crímenes sumarios y detener a los culpables.

Con la expansión de la verificación digital fueron surgiendo gestores de contenido pensados para su desarrollo en redacciones, como Check (https://meedan.com/en/check/) o SAM (https://www.samdesk.io/). Check y su compañía de origen Meedan, con el periodista muy activo en redes sociales Tom Trewinard (@Tom_el_Rumi), destacan por su enfoque internacional y orientado a la traducción, un campo con futuro en verificación digital.

Impulsado por el European Journalism Centre (http://www.ejc.net) aparece en 2014 el primer Verification Handbook o Manual de Verificación, al que se van sumando versiones en

7. Para una inmersión de calidad en esta disciplina se recomienda el curso «Técnico avanzado en obtención de información en fuentes abiertas», impartido por el profesor Carlos Alfonso Rodríguez en CISDE, Campus Internacional para la Seguridad y la Defensa. Es sobre todo de utilidad para los interesados en la conexión OSINT – información internacional y de defensa.

otros idiomas como el español, en cuya traducción participó esta autora, así como manuales de seguimiento.[8] Cuando se publica dicho manual, la actividad ha pasado de ser una rareza a algo más reconocido. En 2015 surge la coalición sin ánimo de lucro First Draft News (https://firstdraftnews.com y es.firstdraftnews.com), con la participación de ocho firmas entre las que hay muchas de las mencionadas, además de Google News Lab. First Draft News es actualmente alma máter de la práctica de la verificación digital en todo el mundo. Analiza, guía y ofrece material de utilidad para periodistas, educadores y ciudadanos. Su responsable, Claire Wardle, es una gran investigadora y pionera en este campo, en el que lleva más de diez años combinando un triángulo casi imposible: ejercicio profesional (Storyful), investigación (Tow Center) y formación a redacciones (BBC).

3. Verificación digital en España

Las redacciones españolas mostraban en 2015 un uso extendido de los CGU pero vacilaciones en los procesos de verificación.[9] Y ello cuando ya había habido fallos notables por valoración errónea de materiales. *El País* publicó en 2013 una supuesta fotografía de Hugo Chávez en una mesa de operaciones (2013). En

8. Silverman, Craig (ed.): *Manual de Verificación. Una guía definitiva para verificar contenido digital al cubrir emergencias*, EJC, febrero 2015 [http://verificationhandbook.com/book_es/; consultado el 2-1-2018]. Silverman, Craig y Tsubaki, Rina (eds.): *Verification handbook for investigative reporting*, EJC, marzo 2014 [http://verificationhandbook.com/book2/chapter1.php; consultado el 2-1-2018].

9. Redondo, Myriam: «¿Qué hacemos con la cantidad masiva de imágenes ciudadanas?» Periodistas, junio 2015 [http://www.globograma.es/wp-content/uploads/2015/07/MyriamRedondo-UGC-FAPE-periodistas38-julio15.pdf; consultado el 2-1-2018].

realidad la imagen mostraba a otra persona, procedía de un vídeo que se pudo ver en Internet y el diario tuvo que retirar los ejemplares de los kioscos y pedir disculpas. Es uno de los fallos más recordados de la prensa española, aunque hoy prácticamente no queda medio de referencia que se haya librado de errar, ni siquiera la BBC con su unidad especializada. Errare humanum est, sobre todo en noticias de última hora.

La verificación digital sistemática en España comenzó con VOST Spain (@VOSTspain), cuya portavoz es la periodista María Luisa Moreo (@marialuisamoreo). Es la rama nacional de VOST, organización de voluntarios digitales nacida en 2011 en Estados Unidos para ayudar a los equipos de emergencia que se activan en las catástrofes. Sus miembros llevaban tiempo en redes y se agruparon a raíz de rumores que entorpecieron la gestión de varios incendios en el verano de 2012, como solicitudes falsas de donación de sangre. Popularizaron la etiqueta #STOPBULOS y lanzaron un buscador de los mismos (http://www.vost.es), impulsando enormemente la verificación digital junto a expertos en comunicación de crisis y emergencias como Luis Serrano (@LuisSerranoR).

Además de estos esfuerzos hubo iniciativas formativas. Esta autora impartió en 2012 varias sesiones vinculadas a la verificación en la Universidad Complutense de Madrid; en 2013, un curso *online* de Periodismo de Investigación Digital muy apoyado en la misma materia y auspiciado por la Federación Española de Asociaciones de Prensa (FAPE); en octubre de 2016, el primer curso presencial sobre Verificación Internacional de Contenidos en Redes Sociales, ofrecido por la Asociación de la Prensa de Madrid. La periodista Julia Rivera Flores (@j_riveraflores) impulsó asimismo iniciativas formativas en 2012 y 2013, aunque en aquella época era casi imposible conseguir atención institucional

y de los medios para este ámbito. Y es necesario destacar a Pau Llop (@paullop). En otoño de 2012 lanzó Fixmedia.org para corregir y mejorar las noticias con la colaboración de los internautas, una idea muy innovadora para la época.

Tras la victoria de Donald Trump en las elecciones de Estados Unidos (noviembre de 2016) la atención hacia la desinformación en red se disparó en todo el mundo. En España, un equipo liderado por Clara Jiménez y Julio Montes (@cjimenezcruz y @MontesJulio), que gestionaban @mhemeroteca, creó @malditobulo, cuenta especializada en desmontar engaños en la red (con información ahora también accesible desde Maldita.es). Pronto se convirtió en referencia internacional, sobre todo tras el atento desmentido de bulos durante el conflicto independentista de Cataluña (otoño de 2017). Otros medios españoles empezaron a atender la verificación digital como línea transversal en sus contenidos o lanzaron secciones específicas. Pueden consultarse en el capítulo «Recursos y lecturas».

Pero la verificación no ha nacido con Internet. Ya describieron su importancia en 2003 Bill Kovach y Tom Rosenstiel en su libro Los elementos del periodismo: «A fin de cuentas, el periodismo se diferencia del entretenimiento, la propaganda, las obras de ficción o el arte por su disciplina de verificación».[10] Es una tarea esencial para la profesión y que debió trasladarse de manera natural a las redes, aunque durante un tiempo pareció relegada. Internet y la crisis económica imponían otras prioridades. Eran tiempos de dura reconversión profesional y se trataba de innovar mientras se cerraban medios y se recurría a los despidos masivos. Casi una cuadratura del círculo.

10. Kovach, Bill y Rosenstiel, Tom (2012). *Los elementos del periodismo*. Madrid: Ediciones El País.

Una muestra de que la necesidad de verificación sigue un continuum y trasciende la división papel/digital es el precursor blog Malaprensa (http://www.malaprensa.com) del profesor Josu Mezo (@malaprensa). Nació en 2004 enfocado a los errores en medios de comunicación tradicionales, pero tiene también gran valor para los actuales, sobre todo en lo referente a manipulación de titulares, estadísticas y gráficos. Su artículo «Mal periodismo por una buena causa» destapó el caso Nadia, una noticia plagada de mentiras que se hizo viral en 2017 a partir de un artículo publicado en *El Mundo*.[11]

4. Verificación y *fact-checking* político

El *fact-checking* (comprobación de datos o hechos) ha acompañado a la profesión desde sus tiempos analógicos, aunque con enfoques algo distintos al actual. En las redacciones, los primeros *fact-checkers* tenían un perfil corrector y se encargaban de leer textos para detectar errores o contradicciones antes de la publicación, completando la labor de los editores. Era una comprobación «antes de» y centrada en los propios periodistas.

En el siglo XX los principales periódicos disponían de *fact-checkers*. Han sido seña de identidad especialmente en *The New Yorker*, por su elevado número y sus investigaciones exhaustivas. También ha llegado a haber 70 *fact-checkers* en el alemán *Der Spiegel*. Pero ni los medios que disponen de *fact-checking* escapan al riesgo de fallo o engaño. La periodista de *The Washington Post* Janet Cook

11. Bernardo, Ángela: «El cuento chino de Nadia Nerea, una niña enferma estafada en busca de una cura», Hipertextual.com, [https://hipertextual.com/especiales/nadia-nerea-tricotiodistrofia; consultado el 2-1-2018].

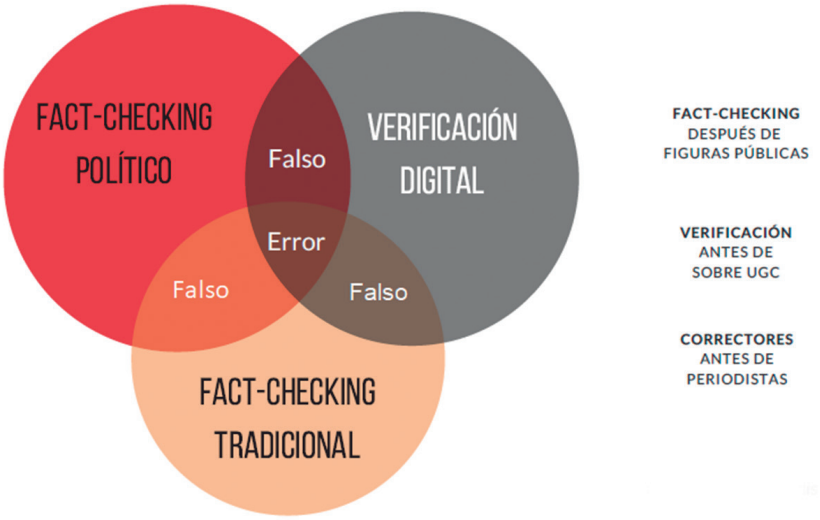
ganó un Pulitzer en 1981 con una historia de un niño drogadicto que no existía; el reportero Jayson Blair publicó durante años viajes y situaciones falsas en *The New York Times*. Sin embargo, cuando una de esas grandes mentiras se destapa, todos comprenden que cuanto más comprobación y comprobadores mejor. Esta realidad no impidió que se prescindiera de muchas de estas figuras durante la crisis.

En el año 2000 aparecen en Estados Unidos versiones de un novedoso tipo de *fact-checking* centrado en el análisis de las declaraciones de políticos. Iría ganando relevancia e interés social hasta experimentar un verdadero auge a partir de 2010, y sobre todo a partir del inicio de la carrera política de Trump. Este candidato ha sido probablemente el más escrutado de la historia, en un esfuerzo periodístico ingente. El corresponsal del periódico canadiense *The Star* en Washington, Daniel Dale (@ddale8), adquirió gran prestigio por resumir cada día las falsedades del aspirante a presidente.[12] El *fact-checking* político se produce «después de», sobre afirmaciones ya realizadas, y se orienta a las declaraciones de figuras o instituciones públicas.

Las tres organizaciones de *fact-checking* político más reconocidas son Politifact (http://www.politifact.com), que pertenece a Tampa Bay Times / Poynter Institute; Factcheck (https://www.factcheck.org/), de la Annenberg Foundation; y el servicio de *fact-checking* de *The Washington Post* (https://www.washingtonpost.com/news/fact-checker). En España ha popularizado este formato y trabajado por un discurso público más riguroso el programa *El Objetivo* (http://www.lasexta.com/programas/el-objetivo/), emitido desde 2013.

12. Para saber más sobre Donald Trump como fenómeno comunicativo: *La comunicación en la era Trump*, Miquel Pellicer (2017), Barcelona: UOC.

Figura 1. Diferencias entre *fact-checking* y verificación digital



Fuente: Elaboración propia a partir de @mantzarlis.

Fact-checking tradicional, *fact-checking* político y verificación digital van en el mismo barco, el de evitar la mentira y el error. Así debe de ser para lograr los mejores resultados, aunque a veces puedan seguir técnicas diferentes.

5. El futuro

Tras la victoria de Trump se analizan nuevas técnicas y formatos para explicar mejor la mentira digital, de modo que el ciudadano comprenda su trascendencia. Si fueron nueve las entidades que configuraron First Draft News en sus orígenes, después de aquellas elecciones se asociaron decenas a la iniciativa, muchas de *fact-checking* político.

Expertos de todas las disciplinas relacionadas colaboran ahora con Facebook, Google y Twitter para evitar la difusión de falsedades en Internet. Aunque la relación no ha resultado fácil y hay críticas hacia las grandes tecnológicas, al menos se detecta movimiento. A finales de 2017 Facebook canceló su iniciativa de advertir de «noticias disputadas» a partir de la indicación de expertos externos, diciendo que lo sustituiría por otros mecanismos más efectivos. Después anunció que fijaría la credibilidad de cada medio a partir de encuestas realizadas a sus usuarios, no a especialistas. Por su parte, Google introdujo avisos que contextualizaban algunos resultados polémicos de búsquedas y revisó sus algoritmos, aunque siguen siendo imperfectos. Se explora un mayor coto a la publicidad programática (compra automática de espacios publicitarios en Internet), que es la que lleva anuncios y por tanto ingresos a los sitios que mienten para hacer negocio. Se investiga también cómo el diseño puede ayudar a distinguir mejor lo verdadero y lo falso y cómo evitar que los desmentidos popularicen los bulos que tratan de desmontar.

Un rasgo actual del *fact-checking político* y de la verificación es el riesgo que corren de verse inscritos en la batalla partidista. Cuando se piensa que la comprobación está politizada, ¿quién comprueba al comprobador?, ¿y por qué fiarse de él? Por su sistematicidad en la denuncia de mentiras de Trump, algunos centros especializados han sido acusados de impulsar una agenda liberal.

La verificación se practica y se demanda y por eso algunos medios se han especializado en la redacción de artículos que recopilan bulos en episodios concretos (narrativa de lista). Otros prefieren ofrecer largas piezas informativas sobre la comprobación que condujo a un desmentido particular (narrativa de verificación).

Buzzfeed es ejemplo de lo primero; Bellingcat de lo segundo.[13] La formación también se valora más. Mark Frankel, responsable de UGC Hub, afirma que los de su equipo son puestos codiciados en la BBC. Explica: «Si estás empezando a formarte como periodista y no aprecias la importancia del CGU, de la verificación, de los modos en que la gente consume y distribuye información en los medios sociales... francamente, no vas a ser un buen periodista».[14]

13. Sobre los nuevos modos de narrativas digitales: Noguera, José Manuel (2015): *Todos, todo. Manual de periodismo, participación y tecnología*. Barcelona: UOC, págs. 83-113.
14. Redondo, Myriam: *op. cit.*, pág. 14.

Capítulo III
Privacidad y ciberseguridad

Se recomienda comenzar a aprender sobre verificación digital analizando las propias huellas digitales. Así se observan dos cosas: qué fugas de contenido ajeno buscar cuando se investiga a alguien y cómo reducir el rastro digital personal cuando se realiza una verificación en línea.

Primero, *googlee* su nombre. Después, compruebe cómo ven su perfil de Facebook personas con quienes no está conectado. En el menú horizontal superior de esta red, pulsar «Ver como» (*View as*), como indica esta imagen: http://www.globograma.es/facebook-privacidad/. Casi nadie se asegura de dejar en modo privado sus fotos y listas de amigos, algo recomendable para evitar problemas. A estos datos inadvertidamente filtrados acuden los verificadores digitales en sus rastreos.

El trabajo de ProPublica «What Facebook knows about you» advierte de la sensible información que extrae Facebook de sus usuarios mediante la **segmentación de perfiles**. Absorbe grandes cantidades de datos derivados de la navegación de cada persona y los completa con compras de datos a terceros. Ello le permite adquirir un conocimiento muy avanzado de los rasgos y preferencias de cada uno, y en consecuencia ofrecer servicios y publicidad altamente personalizada.[1] Algunos partidos políticos

1. Angwin, Julia; Parris, Terry y Mattu, Surya: «What Facebook knows about you», Propublica.org, 28-9-2016 [https://www.propublica.org/article/breaking-the-black-box-what-facebook-knows-about-you; consultado el 2-1-2018].

lo saben y lo utilizan. Para muchos expertos el uso inteligente de los anuncios segmentados por parte de la empresa Cambrigde Analytica estuvo tras el éxito de dos campañas con las que colaboró en 2016: la de Trump y la del Brexit.

La **privacidad** es un reto constante. Todo lo que hacemos en Internet queda registrado y se puede recuperar, aunque se borre. Esta posibilidad, que a menudo es destacada por sus ventajas en materia de seguridad (detección de redes terroristas o de pederastia) entraña también enormes riesgos.

Al periodista holandés Anthony van der Meer le robaron el teléfono móvil. Decidió instalar un programa de vigilancia en el recién adquirido y provocar un segundo robo para comprobar qué extraña vida podía tener el aparato tras el hurto. El mini documental resultante muestra la importancia de los datos personales que se dejan en el teléfono y en las redes (Find my phone; v=NpN9NzO4Mo8).

Muchos ciudadanos siguen esgrimiendo el argumento de «No tengo nada que ocultar» para evitar tomar medidas que protejan su intimidad. Esta convicción ya ha sido desmontada por reporteros que se metieron en problemas solo por entrar en contacto con individuos que sí que los tenían.

Asumiendo esta realidad el profesional de la información debería hacer lo máximo posible por proteger su identidad y la de sus fuentes. Si trata de averiguar cosas sobre un individuo lo hará mejor si no es detectado por este usuario (en adelante, el «investigado» o el «objetivo»). En operaciones digitales de relevancia se recomienda incluso abrir perfiles anónimos en las redes sociales que se vayan a emplear.

La **ciberseguridad** es otro aspecto importante. El robo de determinados datos puede perjudicar mucho al usuario. Solo publicar en Internet la foto de una tarjeta de embarque que nos

hace felices ya puede ocasionar problemas al difundir códigos delicados de la aerolínea. La situación no mejorará con la aparición del «Internet de las cosas». Cada vez más aparatos de la vida cotidiana estarán conectados: el frigorífico, la televisión, el coche. Será más difícil controlar y proteger los datos.

Hasta la aplicación más inocente debe hacer pensar sobre lo que se da a cambio de ella. Conviene recordar una máxima: si el servicio es gratuito el producto eres tú. Así, se ofrecen filtros divertidos para embellecer los autorretratos o selfis, pero en algún caso se ha descubierto que extraían códigos sensibles del consumidor, como hacía la china Meitu. Hay que ser cuidadoso con los permisos de acceso que se otorgan a los programas que se instalan, sobre todo si no son de empresas de confianza.[2]

1. Navegadores

Las cuestiones de privacidad y ciberseguridad ya están presentes en la elección del navegador, por sus extensiones. El de Google, Chrome, tiene muchas relacionadas con la búsqueda avanzada. Por eso eso se toma como referencia en este manual. Sin embargo, Firefox, Safari e incluso Ópera también son utilizados por los expertos, en particular por aquellos que rechazan la omnipresencia del buscador de Mountain View.

Las extensiones son pequeñas aplicaciones que se añaden como botones a la barra de navegación. Si son muchas y no caben

2. Hay pistas prácticas de ciberseguridad en esta conferencia del periodista español Stepháne M. Grueso (2017). «Seguridad digital para periodistas». En: Pilar San Pablo y Aurelio Martín (coords.). *X Jornadas Periodismo en lo Global: Seguridad y Verificación en Internet*. Universidad de Valladolid. [https://www.youtube.com/watch?v=Y7jfaveZ3gc; visto 3-1-2018].

todas, aparecerá a la derecha de las visibles un signo de tres puntos que es un desplegable con las restantes (imagen: http://www.globograma.es/botones/). Una vez instaladas, normalmente hay que pulsar su botón para que realicen la función predefinida, pero a veces se activan a través del botón derecho del ratón (o equivalente en Mac). Otras veces, la aplicación puede actuar automáticamente mientras se navega.

Chrome y otros navegadores permiten abrir pestañas en «modo incógnito» (v=ISyT1NmyPpA), con el que se consigue que las páginas visitadas no queden marcadas en el historial. Sin embargo, el proveedor de Internet sigue detectándolas y registrando el número IP**,** una suerte de DNI o etiqueta digital que distingue a cada ordenador (o a toda una red de ordenadores si estos comparten tal identificador, como sucede en muchas empresas).

La Electronic Frontier Foundation (https://eff.org) ofrece varias extensiones que salvaguardan la privacidad digital más allá de ese modo incógnito. También evalúa servicios de mensajería instantánea para conocer su desempeño en esta materia (Telegram, Signal, WhatsApp). El periodista puede estar atento a esos análisis de EFF para saber qué recurso gana enteros o es más seguro para una tarea determinada. Hay algunas extensiones lanzadas por la propia entidad que son muy recomendables. Panopticlick (https://panopticlick.eff.org) realiza un test rápido que revela si el navegador utilizado rastrea al usuario; propone vías para solucionarlo. Privacy Badger (https://www.eff.org/es/privacybadger) bloquea el seguimiento por parte de muchas webs, que suele tener fines publicitarios. HTTPS Everywhere (https://www.eff.org/https-everywhere) traduce cada url introducida en la barra de navegación a una más segura para entrar en esa web. La dirección pasa automáticamente de http a https y aparece un candado junto a ella. Es importante comprobar que ciertos sitios cuentan con

esa opción de acceso protegido, por ejemplo las páginas donde se realizan transacciones financieras.

Otra extensión recomendable es Click&Clean**.** Para instalarla, escriba «Click&Clean» en el repositorio de extensiones de Chrome (https://chrome.google.com/webstore/category/extensions). Asegura que el cierre de ventanas se efectúa correctamente, sin dejar abierto ningún servicio en el que se haya introducido contraseña. También elimina el historial de navegación y el de descargas, detecta código maligno y ayuda a generar contraseñas seguras, algo muy útil cuando se utilizan numerosos servicios con autenticación. Para Firefox es recomendable el complemento NoScripts, que bloquea algunas acciones de riesgo por parte de sitios que no considera seguros (https://addons.mozilla.org/es/firefox/addon/noscript/).

Las extensiones y complementos mencionados ralentizan la navegación y en ocasiones pueden llegar a impedir la consulta de un sitio, pero protegen. El periodista puede instalarlas en su navegador habitual y mantener otro sin ellas. Lo mejor es probarlas y elegir las que más se ajusten a las necesidades propias, regulando los distintos niveles de vigilancia que ofrecen.

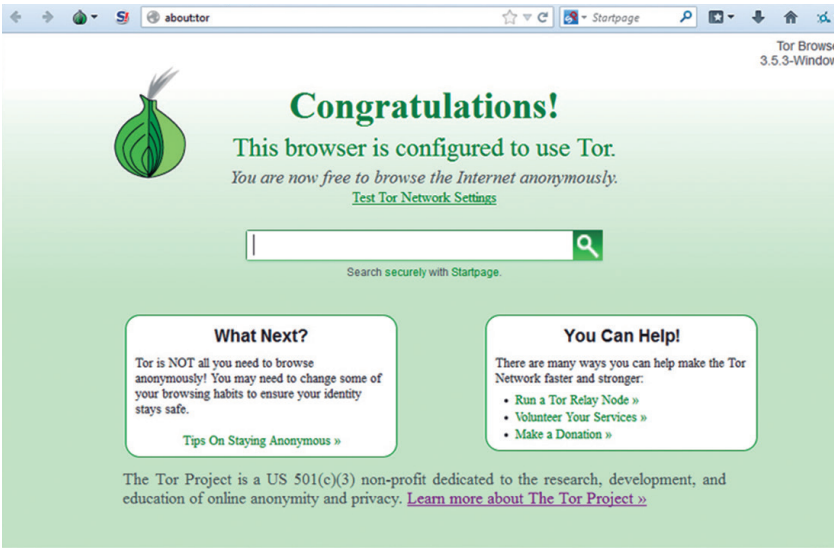
2. Anonimato

Si se quiere investigar aún más oculto se deberá recurrir a un navegador que preste servicio de anonimización o enmascaramiento. El más conocido es Tor (https://www.torproject.org). Este vídeo explica cómo descargarlo: v=tWdjPeuRvgo.

Tor desvía al usuario por túneles aleatorios, y esos túneles atraviesan puntos en los que cambia la IP. Al final del circuito la página receptora no sabe de dónde procede el visitante en realidad.

El navegador se ha hecho popular por permitir el acceso a la *deep web* o Internet profunda y por ser utilizado por muchos activistas. Inicialmente generó cierta sensación de invulnerabilidad, hasta que algunos episodios mostraron que no era infalible. El proveedor de Internet sabe que ha existido una conexión con Tor, aunque no la ruta seguida dentro de él. Una forma de rastrear la actividad de un pirata informático es comprobar la correlación de sus conexiones y desconexiones con las anomalías digitales que sucedieron entre ellas, fórmula que se ha utilizado en ocasiones en el seguimiento de miembros de Anonymous.

Figura 2. Navegador Tor



Fuente: Torproject.org

Dependiendo del grado de seguridad que se le adjudique –alto, medio o bajo– Tor puede llegar a complicar mucho la navegación e incluso impedir el acceso a algunas webs. El reportero –o el

lector– pueden examinar y calibrar su configuración. El nivel bajo es el que proporciona la mejor experiencia de usabilidad, con todas las funcionalidades del navegador habilitadas.

Un paso más avanzado para garantizar la privacidad y el acceso libre a Internet lo constituyen las VPN (Red Privada Virtual). Son muy utilizadas por los corresponsales en países como China, donde la llamada «cibermuralla» bloquea conexiones a páginas relevantes como Facebook, Google o *The New York Times*. La VPN es una red que provee Internet seguro a partir de la conexión con un servidor extranjero, esquivando esa censura. Oculta la navegación ante un posible gobierno autoritario, aunque el proveedor extranjero sí que puede conocer en algunos casos la IP.

Últimamente ha proliferado la oferta de VPN gratuitas o incluso incorporadas en algún navegador, pero hay que tener cuidado con algunas, pues irónicamente captan datos del usuario. Las mejores siguen siendo de pago. Hay rankings y comparativas en sitios como ThatOnePrivacySite (https://thatoneprivacysite.net/) o EFF.

3. Protección del ordenador

Además de vigilar el anonimato (privacidad) pueden añadirse mecanismos para proteger o aislar el ordenador (ciberseguridad). Se mencionan algunos que van creciendo en complejidad, pero también en prestaciones. El periodista puede examinarlos y elegir.

En verificación digital a veces se manejan documentos sensibles. Además de realizar copias de seguridad frecuentes y de dotarse de un buen antivirus actualizado, existen programas de encrip-

tado que protegen directorios completos del ordenador, como VeraCrypt (https://veracrypt.codeplex.org). Su uso en una unidad USB permite resguardar los archivos que contiene y evitar que alguien acceda a ellos en caso de pérdida (v=qdIFEeYgfBI).

Sandboxie (https://www.sandboxie.org), una suerte de cámara de arena o entorno de pruebas, permite ejecutar programas en su interior aislando sus procesos (para instalar: v=1OnFY7fmSiM). Si hay dudas sobre un adjunto que llega por email, abrirlo desde aquí evita un posible ataque de *phising*. Esta modalidad delictiva se da cuando una entidad finge ser otra de confianza del usuario y le convence para que transmita datos personales o descargue un programa maligno. Otra opción algo más compleja en esta misma línea es **crear una máquina virtual**. Además de aislar procesos como Sandboxie permiten emular el comportamiento de todo un ordenador y cargar sistemas operativos distintos (Linux en lugar de Windows, por ejemplo). Las máquinas virtuales ocupan bastante espacio y memoria RAM, reduciendo el rendimiento. Instalarlas tiene una complicación media.[3]

Por último, la opción más segura para garantizar la privacidad y resguardar los archivos es instalar el sistema/distribución Tails (The Amnesys Incognito Linux System, https://tails.boum.org). Puede decirse que combina muchos de los servicios anteriores. Arranca con el mismo encendido del ordenador y supone entrar en una suerte de «universo paralelo» desde el que no se tiene acceso a los documentos o aplicaciones del PC, mientras desde el PC no se tiene acceso a los creados en Tails. Al salir hay dos opciones: o se borran todos los documentos o se crea una carpeta específica donde perdurarán encriptados. El

3. Ramírez, Iván: «Máquinas virtuales. Qué son, cómo funcionan y cómo utilizarlas», Xataca, 4-8-2016 [https://www.xataka.com/especiales/maquinas-virtuales-que-son-como-funcionan-y-como-utilizarlas; consultado el 2-1-2018].

sistema garantiza el mayor anonimato posible, esquiva la cibercensura y no deja trazas en el ordenador. La instalación es extremadamente compleja, incluso puede durar varios días, pero no es imposible y se recomienda a periodistas que realicen investigaciones digitales de riesgo que la intenten (v=3DiE5fmAtYg). Tails no se utiliza con VPN.

Si no se tiene tiempo, si el lector no se atreve con estas instalaciones, la recomendación básica es realizar al menos las búsquedas más comprometedoras con Tor.

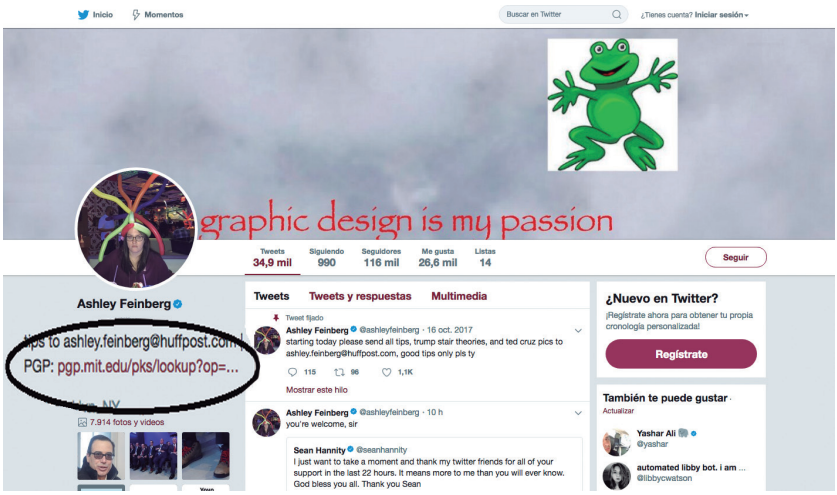
4. Comunicación privada

Otra necesidad del periodista es la de proteger sus comunicaciones con las fuentes. Para empezar, en intercambios relevantes se desaconseja utilizar conexión inalámbrica (wifi) y se prohíbe utilizar wifi sin contraseña (como la que ofrecen gratuitamente muchas cafeterías). Otro de los principios esenciales es utilizar una contraseña segura en el correo electrónico y en cualquier otro servicio que exija autenticación. En este videotutorial se ofrecen pautas para elegirlas combinando letras, números y símbolos (v=COU5T-Wafa4).

Los periodistas que manejan filtraciones e información sensible suelen recurrir al *software* Pretty Good Privacy o PGP, llamado «de dos claves» o de «clave pública». Se basa en una primera clave que se ofrece abiertamente para que otros usuarios envíen la información (es como la dirección de un buzón) y en una segunda clave que es privada para cada usuario del servicio y será la que permita cifrar y descifrar los mensajes. La extensión Mailvelope (https://www.mailvelope.com) permite crear

claves PGP que se pueden utilizar en diversas cuentas de correo (videotutorial: v=oEMfkIBM2zc).

Figura 3. La periodista Ashley Feinberg enlaza a su clave pública desde Twitter



Fuente: http://www.twitter.com/ahsleyfeinberg

A algunos estudiantes de periodismo les resulta complejo el sistema PGP. En ese caso otra opción es el correo Protonmail (http://protonmail.com), donde abrir una cuenta es tan sencillo como en Gmail. Proporciona la posibilidad de intercambiar mensajes solo inteligibles si emisor y receptor comparten una clave privada. Si el lector persiste en utilizar su habitual cuenta de dominio general incluso al realizar investigaciones delicadas, puede introducirla previamente en Have I been pwned? (https://haveibeenpwned.com) para comprobar si ha sido pirateada. En tal caso deberá cambiar la contraseña.

En algún momento puede ser conveniente generar una identidad falsa temporal vinculada a una cuenta de correo también temporal y falsa. Esto es útil por ejemplo cuando se prueban muchas

plataformas que exigen identificarse con correo. El lector puede facilitar a las plataformas esa dirección temporal, recibir de ella la información de acceso y no volver a utilizarla. Así evitará comunicar su correo personal. Secure Fake Name Creator (https://fakena.me) y Temporary email (https://temp-mail.org) son recursos habituales.

Lo importante es que el lector sea consciente de cómo algunas nociones de privacidad y ciberseguridad pueden ayudarle en su tarea de verificación. Y siempre es necesario recordarlo, aunque parezca obvio: las pistas apuntadas en este manual se ofrecen con fines educativos, periodísticos y de investigación ética. Cualquier uso vinculado a actos delictivos será responsabilidad única del lector.

Capítulo IV
Un escritorio para la última hora

Cuando se habla de un «escritorio para la verificación digital» se hace referencia a un lugar adaptado al máximo para realizar esta tarea. Lo primero es disponer de equipos adecuados. El ordenador ha de tener memoria suficiente para procesar muchas pestañas abiertas. Si la verificación es profesional, dos pantallas de visualización son prácticamente imprescindibles, y en las redacciones se suele incorporar un tercer monitor de pared para el seguimiento de servicios como Crowdtangle, que se explica más adelante. Preparar el escritorio también implica tener bien ubicados en el ordenador y el navegador los recursos más frecuentemente utilizados.[1]

La necesidad de agilidad se extrema cuando surgen noticias de última hora («noticias de alcance», «noticias de emergencia» o «urgentes», como se les llama en algunos medios). Hay que actuar con aplomo y rapidez para decidir si se tuitea o no una imagen o un contenido que pueden ser la noticia de la semana o el gran bulo. Ahí es cuando el reportero agradece haber personalizado su escritorio, tenerlo preparado de antemano y conocer las aplicaciones que lo componen para recurrir a ellas sin dudas.

1. Mac Suibhne, Eoghan: «Pro tips for set up an efficient verification Workstation», FirstDraftNews.com, 4-1-2018 [https://firstdraftnews.com/verification-workstation; consultado el 5-1-2018].

1. Noticias de última hora

Las noticias de última hora son episodios habitualmente confusos y la desinformación aumenta cuanto mayor es su relevancia. Twitter suele ser el hilo conductor de rumores que surgen en zonas más a la sombra como las redes de mensajería instantánea o foros del tipo 4Chan (https://boards.4chan.org/) y Reddit (https://www.reddit.com/). A estos últimos se les compara en ocasiones con el español Forocoches (https://www.forocoches.com/).

Hay algunos tipos de bulos que se repiten cada vez que se producen episodios violentos o catástrofes. Conocerlos permite estar alerta. El principal es la difusión de imágenes pertenecientes a acontecimientos anteriores. Un ejemplo fue la información difundida sobre el conato de referéndum proindependencia celebrado en Cataluña el 1 de octubre de 2017 (1-O). La votación fue considerada ilegal por las autoridades judiciales españolas, lo que dio lugar a una intervención muy polémica por parte de la policía. Se vivieron escenas de violencia y las redes se llenaron de imágenes reales pero también de imágenes de heridos correspondientes a sucesos previos. @MalditoBulo desenmascaró numerosas falsedades. Este es un listado de ese y otros errores/bulos frecuentes en noticias de alcance:

- Imágenes y vídeos de fechas anteriores.
- Imágenes, vídeos y gifs animados trucados.
- Fenómenos climatológicos extraños.
- Animales fuera de lugar (especialmente tiburones).
- Segundos ataques / atacantes en episodios terroristas.
- Número equivocado de víctimas.

- Señalamiento prematuro de culpables.
- Errores iconográficos con logos y banderas.
- Escenas violentas descontextualizadas.
- Contenidos aterradores y divisivos que fomentan la confusión y la polarización.

En globograma.com se ofrecen varios ejemplos reales de este tipo (http://bit.ly/2HjRoOY). Algunas imágenes falsas se convierten en clásicos. Es el caso de la fotografía del Huracán Sandy (2012) que publicó Jason Otts combinando una tormenta anterior y la Estatua de la Libertad en Nueva York (http://bit.ly/2opdNmV), y la del joven cuya foto trucaron sus amigos para que le tomaran por uno de los terroristas que atentó en París en 2015 (http://bit.ly/2HIhwUz). Los tiburones fotografiados en su hábitat natural por Thomas Peschak también son invitados frecuentes en las catástrofes. Han aparecido en carreteras y andenes inundados de todo el mundo (http://bit.ly/2ooxQlq).

El programa de radio estadounidense *On the media* elaboró en 2013 una de las primeras hojas de ruta para noticias de última hora y la va actualizando. Está pensada para ser recortada y colocada cerca del ordenador. Incluye advertencias como las siguientes: en los primeros momentos los medios se equivocarán; no te fíes de las fuentes anónimas; presta atención al lenguaje («Estamos obteniendo información» podría no significar nada). A continuación se ofrece una guía propia:

Guía para la verificación digital en noticias urgentes

– Cuanto más espectacular es una imagen o noticia, mayor riesgo de bulo. Cuanto más irritante, también.
– Piense antes de redifundir. Si se equivoca pida disculpas, no borre sin más.
– **QUIÉN.** Hay tres niveles: A) ¿Qué medio lo cuenta? ¿Lo conozco? B) ¿Hay firma? ¿La conozco? Y C) ¿Ese autor cita fuentes propias? ¿Anónimas o explícitas? ¿Una o varias? ¿Son oficiales o especialistas en ese tema? Autoridades y expertos también pueden mentir o equivocarse; las fuentes más fiables suelen ser las vinculadas a servicios de emergencia.
– **QUÉ.** No quedarse con el título o el tuit. Pulsar en el enlace que contiene para comprobar si el contenido confirma ese adelanto. Comprobar la url de destino, puede indicar sátira o poca calidad o imitar la dirección de un sitio respetable.
– **CUÁNDO.** Tres niveles: A) ¿La información está fechada? B) ¿La fecha está expresada en mi zona horaria? C) ¿He comprobado si es una publicación antigua?
– **DÓNDE.** ¿Conozco ese lugar? ¿Tengo referencias/contexto del mismo? Hay que acudir a los medios locales, pero en escenarios de tensión política también interesan fuentes sin intereses en la zona (como los corresponsales).
– **POR QUÉ**. ¿Puede haber motivos ocultos tras la difusión de esta información? ¿Es una crítica contra alguien?
– **CÓMO.** ¿Es una información o una opinión? ¿Es una difusión masiva y repentina? ¿De cuentas recién abiertas o con escasa actividad previa?

2. Extensiones para la verificación

Algunas extensiones están especialmente indicadas para agilizar el trabajo de verificación digital. En Chrome, si se crea una cuenta tales extensiones se pueden recuperar desde cualquier equipo a través de la nube. Para instalar las siguientes propuestas, hay que buscarlas por su nombre en el repositorio de extensiones de Chrome: https://chrome.google.com/webstore/category/extensions.

2.1. Almacenamiento

El periodista va a recopilar mucha información mientras investiga y probablemente tendrá que volver a ella una y otra vez, siendo capaz de reproducir los pasos dados si se le solicita. Diigo y Zotero son recursos documentales gratuitos para almacenar y gestionar esa información consultada, aunque hay muchas otras herramientas disponibles en este campo (como Pocket, bastante popular). Permiten marcar las lecturas volviendo a ellas cuando se desee.

Diigo guarda lecturas en la nube en modo público o privado y destaca por la facilidad para aplicar etiquetas y recuperar lecturas. Incorpora una opción para que cada vez que se realice una búsqueda en Google los resultados ofrezcan también –si así lo desea el usuario– las informaciones que ha almacenado con relación a ese tema/etiqueta.

En investigaciones críticas de verificación digital no se recomienda guardar documentación en la nube. En ese caso Zotero puede ser una buena alternativa. Requiere instalación en el ordenador precisamente para generar una carpeta local que pueda almacenar los archivos. En Zotero las opciones de clasificación

y recuperación de la información son muy superiores a las de Diigo. A cambio, el sistema de guardado es más complejo.

El periodista que no concede importancia al almacenamiento ordenado de la información no es un buen verificador. Es como un científico que ofrece un gran descubrimiento sin garantizar el rigor en la metodología que ha conducido a él.

La extensión Session Buddy almacena en una sola pestaña todos los enlaces abiertos, para poder volver a ellos. The Great Suspender y Tabs Onliner evitan que el alto número de pestañas abiertas cuando se verifica lleve al bloqueo del ordenador.

2.2. Búsqueda

Storyful Multisearch se instala en Chrome y su símbolo es una lupa. Como muestra este videotutorial (v=CKP3Hey1Azo), cuando se pulsa en ella despliega una pequeña ventaja que permite buscar términos en siete direcciones activas a la vez: Twitter, Twitter Imágenes, Twitter Vídeos, YouTube, Tumblr, Instagram y Spokeo (un directorio de personas). También busca en la ya desaparecida Vine, que todavía no han retirado de las opciones. En cada caso el resultado se muestra en una pestaña diferente. Storyful ofrece otra extensión de pago, solo para socios, Verify, que marca los vídeos amateur con un signo verde si están verificados, amarillo si ofrecen dudas y rojo si son bulos.

2.3. Búsqueda inversa de imágenes

Quizá la operación más elemental de verificación digital es la búsqueda inversa de una imagen con el objetivo de comprobar si

pertenece a un momento anterior. El servicio más destacado es Google Images, con una extensión específica para Chrome, porque cuenta con el mayor número de imágenes indexadas y suele encontrar más material. Entre los resultados es posible filtrar por tamaños y buscar imágenes similares. El principal inconveniente de Google es que no permite identificar la imagen más antigua, aunque se puede buscar por fechas anteriores al episodio que interesa (en el menú Herramientas>Fecha>Intervalo personalizado) para ver si aparece ese material antes (imagen: http://www.globograma.es/inverso/).

TinEye es otro recurso relevante. Fue de los primeros buscadores inversos y se basa en una tecnología de análisis distinta a la de Google. Es además la única extensión que ordena los resultados cronológicamente permitiendo detectar cuál fue la primera fotografía publicada. La mayor desventaja es que ofrece menos resultados que otros buscadores.

RevEye es la extensión de búsqueda inversa más completa. Se coloca el cursor sobre la imagen, se pulsa el botón derecho del ratón o equivalente en Mac y se comprueba al momento si ha aparecido en Google Imágenes pero también en Yandex (principal buscador y portal ruso), Baidu (buscador chino), la mencionada TinEye (que es propiedad de Idée, empresa canadiense) o Bing, el buscador de Microsoft (https://www.bing.com).

Interesa utilizar todos estos motores porque cada uno ofrece ventajas, incluido Bing, aunque sea habitualmente relegado ante el predominio de Google.[2] Sus algoritmos son diferentes y las preocupaciones que conforman el imaginario colectivo de los internautas (estadounidenses, rusos, chinos...) pueden ser distin-

2. González, Gabriela: «Cómo usar la búsqueda inversa de imágenes en Bing», Hipertextual.com, 18-3-14 [https://hipertextual.com/archivo/2014/03/busqueda-inversa-imagen].

tas y haber impulsado uno u otro contenido entre los resultados. Cada vez más los bulos comienzan a mostrar una expansión global, con origen en un país y traslado a otro, y es esencial comprobar si una imagen sospechosa ya ha hecho la ronda de engaño más allá de las propias fronteras.

Ninguna de estas extensiones tiene una fiabilidad total. Si una fotografía no aparece utilizando los recursos anteriores puede tratarse solo de un falso negativo. El periodista hará bien en tenerlo en cuenta a la hora de realizar afirmaciones categóricas. «El buscador inverso TinEye no encuentra» o «Una búsqueda inversa no arroja resultados» son expresiones más precisas que «Esta imagen nunca se ha publicado antes».

Por último, en este apartado de búsqueda inversa es también recomendable instalar FistDraftNews Check y el complemento InVid, que se verán con más detenimiento en el capítulo «Imágenes y vídeos».

2.4. Guardado

Muchos contenidos con los que trabaja el periodista pueden desaparecer. Es necesario guardarlos a través de servicios como Wayback Machine (https://archive.org/web) o Archive.today (https://archive.is). El primero guarda la página que se esté visitando, deja consultar versiones anteriores de la misma, indica su relevancia en el ranking Alexa, y ofrece un registro antiguo que funciona cuando encuentra un enlace con error 404. Archive.is es más recomendable para guardar páginas web.

Guardar la página entera en html es mejor que realizar captura de pantalla, que guarda en formato imagen, pero si se necesita lo segundo se recomienda la extensión Nimbus (también puede hacer-

se con atajos de teclado en Mac y PC). En Nimbus se decide si se guarda: la parte visible de una página, toda la página o un área seleccionada, pudiendo después editarse la imagen; también es posible grabar vídeos de pantalla (de una pestaña o de todo el escritorio).

Como las destinadas a privacidad y seguridad digital que se explicaron anteriormente, las extensiones vistas en este capítulo suelen ralentizar la navegación. Además, debe revisarse detenidamente su configuración para comprobar los permisos de acceso que requieren, ya que algunas pueden ser bastante invasivas. Lentitud y cierta relajación de las pautas de privacidad habitualmente respetadas son a veces los peajes que hay que pagar por emplear estos servicios gratuitos muy útiles.

2.5. Contexto e idiomas

Varias extensiones advierten al usuario cuando se topa con una url poco fiable. No pueden detectar todas las falsedades que circulan, pero sí los sitios sospechosos más habituales. En español existe la extensión Malditobulo, que indica si se ha entrado en un sitio web con contenidos que se han tenido que desmentir. Un funcionamiento parecido pero aplicado a Twitter tiene Real Donald Context (de *The Washington Post*), para Firefox. Alerta cuando se consultan tuits inexactos del presidente de Estados Unidos (https://addons.mozilla.org/en-US/firefox/addon/real-donald-context/).

En su sección de configuración, se puede indicar al navegador Chrome que traduzca automáticamente los sitios en idioma extranjero que se visiten. Pero a veces no se desea hacerlo pues, por ejemplo, el usuario puede leer en varios idiomas. En este caso se puede instalar la extensión Google Translate. Se

selecciona el fragmento de texto en lengua extranjera y se pulsa el botón derecho del ratón en Windows (equivalente en Mac). Aparecerá su traducción.

2.6. Tráfico / influencia

Las redacciones tienen que estar cada vez más pendientes no solo del contenido propio sino de las noticias ajenas que están atrayendo visitas. Conviene desmontar bulos que están ganando tracción social, y no otros de escaso efecto pues se les estaría dando a conocer. Buzzsumo y Crowdtangle son dos webs de referencia para la detección de contenido viral. Revelan qué asuntos se están convirtiendo en tendencia (*trending topic*), así como qué impacto está teniendo una url concreta.

Al principio se podían utilizar gratuita o semigratuitamente pero su oferta ha ido modificándose. Buzzsumo facilita algunos servicios que se recomienda probar al periodista (demo) pero básicamente ha quedado convertido en un servicio de pago (http://buzzsumo.com/). Crowdtangle fue comprado por Facebook y ahora se ofrece para redacciones asociadas a esta red social (hay que solicitarlo en http://www.crowdtangle.com/). Una muestra de su utilidad: el servicio Live Displays de Crowdtangle ofrece una visión multicolumna y multiplataforma que permite contemplar simultáneamente las tendencias en Google, Facebook, Twitter y otras redes sociales. El usuario lo configura como quiere y algunas redacciones optan por una versión televisión para colocarlo en grandes pantallas.[3]

3. Vídeo demostrativo de Crowdtangle Live Display: http://bit.ly/2sOQA2c. Facebook cuenta con otro servicio de utilidad para periodistas y redacciones, Signal, pero sólo está disponible en EEUU.

Con lo que sí cuentan ambos servicios (Crowdtangle, Buzzsumo) es con extensiones gratuitas para Chrome. Una vez instaladas y generada una cuenta, cuando el periodista entra en una url y pulsa el botón característico de la extensión se abre una pequeña ventana que ofrece un repaso básico del impacto y número de interacciones que ha generado ese contenido. Constatar que un conjunto de falsedades sobre un fenómeno concreto se está expandiendo puede servir de base para un artículo con «narrativa de verificación».[4]

3. Tweetdeck y otros recursos

Tweetdeck se ha convertido en el servicio imprescindible para la verificación digital. Es gratuito y permite un seguimiento multicolumna de la red social Twitter. Hay distintos tipos de columna (de búsqueda, de lista, de usuario...) y cada una se puede personalizar: para que muestre solo los tuits de un usuario, de una lista, de una tendencia, con una etiqueta o una palabra... También es posible elegir la franja temporal que interesa y pueden establecerse notificaciones sonoras (cada vez que tuitee un usuario muy relevante, por ejemplo). Caso práctico de su valor: si un reportero sigue la actualidad de Nueva Zelanda, imposible no considerar útil una columna que avise de tuits que se publiquen conteniendo la palabra Ardern y superando un número considerable de retuits. Algo habrá pasado con la primera ministra de este país (Jacinta Ardern).

4. Un ejemplo: Llaneras, Kiko y Colomé, Jordi: «España también tiene noticias falsas», *El País*, 28-1-2017 [https://politica.elpais.com/politica/2017/01/27/actualidad/1485523499_326784.html; consultado el 2-1-2018].

Se recomienda explorar las opciones de geolocalización, que permiten ver solo los tuits procedentes del lugar de la noticia. Aunque la localización totalmente precisa es difícil en Internet, este filtro evita mucho ruido en los resultados.

Para un periodista pendiente de un lugar remoto donde ha ocurrido una catástrofe, Tweetdeck es de mucho valor en el hallazgo de testimonios, imágenes y vídeos. Este vídeotutorial de Javier Cossío explica con bastante claridad sus opciones (v=oSKpor2bCLs).

No hay que esperar a que se produzca la noticia para crear las columnas. Las esenciales deberían estar previamente configuradas a partir de listas de Twitter alimentadas con esmero por el periodista. Aquí ofrecen un videotutorial para crear tales listas: v=_n5MaYnAiU8. Es conveniente que se centren en el ámbito propio de interés (deportes, moda, relaciones internacionales...) pero también y con un carácter más general en perfiles que ayuden a actualizar las habilidades en verificación. Ejemplo: lista @Globograma-Corresponsales sobre periodismo internacional (https://twitter.com/globograma/lists/corresponsales) y lista @Globograma-Verificación sobre expertos en verificación digital (https://twitter.com/globograma/lists/verification).[5]

Esta es una **propuesta de columnas** en Tweetdeck. Está pensada para la noticia imaginaria de un crimen que se acaba de producir en Galicia y es adaptable a cada caso:

5. En las listas de Twitter puede añadirse a cualquier usuario. En Facebook también hay listas aunque para incluir a alguien en ellas hace falta estar conectado con él o seguirle (si es que ha activado su perfil público). El proceso de creación es muy intuitivo: en el menú vertical izquierdo, opción «Friends lists» o «Lista de amigos». Tweetdeck no permite el seguimiento de listas de Facebook.

- Columna de usuarios imprescindibles (familiares de la víctima con perfil en Twitter), con aviso sonoro.
- Básicos (fuentes oficiales, @policía, @guardiacivil, @VOSTSpain...). En este caso ampliadas al ámbito gallego y con aviso sonoro dependiendo del ritmo de información. Este aviso se elimina si resulta demasiado frecuente.
- Medios de comunicación (lista general del país) con filtros por palabra clave (la propia del suceso).
- Medios de comunicación (lista de medios locales, debe hacerse en ese momento)
- Usuarios ubicados en la zona específica y con cuenta verificada.
- Tuits geolocalizados con un número determinado de retuits.
- Seguimiento de las etiquetas principales con que se narra el episodio; si son muy activas deberá imponerse un filtro (que se ofrezcan solo los tuits con un volumen importante de retuits).
- Corresponsales en el país. En un suceso local esta columna es prescindible, pero se recomienda mantenerla por ejemplo en caso de atentado; la información de servicios de inteligencia extranjeros que puedan filtrar es interesante.

Hay servicios más avanzados que Tweetdeck en el ámbito de monitorización de redes pero son de pago. En las grandes redacciones es muy apreciado Newswhip Spike (https://www.newswhip.com/newswhip-spike/). También se recurre a menudo a Dataminr (https://www.dataminr.com) o Audiense (https://audiense.com/).

Para finalizar este capítulo se realizan **algunas recomendaciones**:

- Probar todos los recursos disponibles también en el teléfono móvil. Se aconseja: a) instalar alguna aplicación de medios de comunicación con alertas de última hora en función de los intereses propios (las más conocidas en periodismo internacional son las de AP, BBC y *The New York Times);* y b) instalar aplicaciones de seguimiento de usuarios favoritos como Nuzzel (http://www.nuzzle.com), que se basa en listas de Twitter.[6]
- Suscribirse a boletines de verificación digital. Destacan Checklist Meedan, Craig Silverman, First Draft News y Disinformation Review.[7]
- Generar alertas de correo sobre temas muy específicos de interés. Se apunta Google Alerts (https://www.google.es/alerts), pues es el servicio que permite avisos más frecuentes.
- Seguir medios concretos a través de programas RSS, como RSS Feedreader (http://feedreader.com, v=FkSV0Nhn4pc), con opción *online* y de descarga. Pero la «sindicación de contenidos» o RSS solo es útil si el periodista de verdad la va a utilizar. De otro modo es mejor prescindir de ella pues conduce a un conjunto de lecturas acumuladas sin leer. Deben seguirse pocos hilos y específicos, acotándolos por expresiones de búsqueda.

6. Pistas de utilidad en periodismo móvil: Ríos, Carmela (2015). *Cómo el #15M cambió la información. Una guía de periodismo móvil,* Barcelona: UOC, y Bernal, Ana I. (2015). *Herramientas digitales para periodistas*, Barcelona: UOC.

7. Checklist Meedan: https://meedan.com/en/check/ (la caja de suscripción se encuentra en la parte inferior de la página); Craig Silverman: http://eepurl.com/cxDkyX; FirstDraftNews: https://firstdraftnews.org/newsletter/ y DisinformationReview: http://eepurl.com/bN1ub5.

Capítulo V
Búsquedas avanzadas

Muchas veces verificar pasa por encontrar otros materiales que contextualicen el que se está comprobando. Algunas pistas básicas para una búsqueda rigurosa son:

- Conocer a fondo las opciones de Google, el principal buscador.
- Google no es el único buscador; combinarlo con otros.
- Buscar desautenticado y del modo más anónimo posible, para que el motor no capte preferencias de otras navegaciones anteriores.
- Averiguar si existe –y utilizar– la sección «búsqueda avanzada».
- Buscar preferentemente en el idioma local de la zona en que se ha dado la noticia, en inglés y en el idioma propio, por ese orden.
- Probar los llamados operadores avanzados en toda caja de búsqueda. Son los que relacionan de manera lógica los términos que interesan al usuario que investiga y se explicarán más adelante. ¿Cuáles funcionan?
- Elegir bien la pregunta, la cadena de búsqueda. Hay que pensar cómo puede expresarse el autor y con qué nombre derivado de su mentalidad puede haber publicado el material, especialmente si se trata de un archivo no profesional. ¿Qué es más probable, que un terrorista publique el vídeo de uno de sus ataques con el nombre de archivo «drama» o con el de «victoria»?

Mauricio Jaramillo ya hablaba del **periodista Google** en 2010.[1] Años más tarde se sigue acudiendo masivamente a este buscador, pero muy pocos recurren a su sección avanzada (https://google.es/advanced_image_search). Esta reduce el trabajo al ofrecer una interfaz sencilla con atajos basados en los principales operadores de búsqueda. El usuario puede ir directo a localizar un tipo de archivo u otro, en este idioma o en aquel. Es recomendable buscar y conocer las opciones avanzadas de todos los buscadores.

1. Operadores básicos

Este videotutorial de First Draft News explica algunos trucos para buscar en Google: v=tJWDKg1fjj0, y en Globograma.com se ofrecen algunos operadores útiles (http://globograma.es/operadores-de-busqueda-para-periodistas/#operadoresutiles). Aquí va un listado de los principales:

- «...». Una expresión específica que aparezca sin alteración: [«Embajador de Perú en España»].
- ***.** Una expresión de la que se desconoce una parte que se sustituye por asterisco, por ejemplo un nombre: [«El actor * Darín»].
- **- o NOT**. Una expresión concreta excluyendo un término que introduce ruido en los resultados: [Argo –película] o [Argo NOT película].
- **OR**. Un término u otro. [Daesh Siria OR Irak or Africa].

1. Jaramillo, Mauricio: *Guía de herramientas Google para periodistas*, Mauriciojaramillo.com.com, 2010 [https://es.scribd.com/document/36980256/Herramientas-Google-para-periodistas]

- **Related**. Sitios con información similar/relacionada a la de otro sitio que interesa: [related:revista5W.com].
- **Intitle.** Que el título de la página incluya un término concreto, lo que indicaría que es relevante dentro de la información: [intitle:Congo]
- **Allintitle.** Una cadena de texto en el título de una web: [allintitle:«refugiados en Hungría»]
- **Inurl**. Que la dirección url incluya un término concreto: [inurl:inmigrantes]
- **Site**. Busca solo en dominios elegidos: [«Theresa May» site:bbc.com]

Ejemplos avanzados del operador «site», uno de los más prácticos:

- Para encontrar un tema dentro de un sitio web o varios: [«casos de corrupción» site:elconfidencial.com site:elpais.com]
- Uso con subcarpetas, como para hallar «libros sobre extremismo en Amazon»: [extremismo site:amazon.com/books]
- Buscar una cosa o la otra: [site:amazon.com/books Daesh OR ISIS]
- Dentro de un sitio y con palabra clave en la url: [site:amazon.com inurl:Murcia]
- Cuando interesa una palabra y otras vinculadas: [site:amazon.com ~Daesh]
- Cuando interesa una palabra y otras que se le relacionen pero no una que introduce ruido: [Islam -terrorismo -terrorism site:amazon.com]
- Más que un dominio, interesa un conjunto de dominios (militares, educativos, etc.): [site:mil refugiados]

- Para obtener información en las redes sociales o monitorizar lo que se dice de una persona en ellas: [site:twitter.com OR site:Facebook.com OR site:Instagram.com «Gerda Taro»]
- Buscar hilos en un sitio para seguirlos: [rss site:foreignaffairs.com]

Las búsquedas anteriores funcionan en Google y el lector hará bien en explorar las particularidades de otros buscadores. Por ejemplo, en Bing funciona el operador «author». Apunta hacia materiales que haya escrito una persona, relegando los que giran en torno a ella: [author:«Bru Rovira»].

2. Búsquedas personalizadas

Los mejores resultados se obtienen **combinando operadores**. Las expresiones no dejan de perfeccionarse y muchas veces lo hacen a partir de aficionados a la informática y *hackers* que experimentan con cadenas de búsqueda por curiosidad. Contra el uso extendido no debería llamarse hackers a quienes vulneran sistemas informáticos, sino *crackers*, que son los *hackers* que cometen actos ilícitos.

Las **alertas de Google** pueden precisarse mucho si se usan operadores. Un ejemplo: [«coyuntura económica europea» «nuevo estudio» OR «nuevo informe»] avisará al periodista que cubra estos asuntos en Bruselas cada vez que aparezca un nuevo análisis. También es posible crear alertas de libros en Google Académico (https://scholar.google.es/). Hay apuntes para diseñar esas alertas avanzadas en Papelesdeinteligencia.com (http://papelesdeinteligencia.com/12-formas-de-exprimir-

google-alerts/) y Globograma.com, «Operadores de búsqueda avanzada para periodistas» (http://bit.ly/2DgQZdw). Todo esto ayuda a estar actualizado en el ámbito de dedicación cuando surge una noticia de última hora y hace falta recurrir a expertos o comprobar datos.

Otra opción recomendable es diseñar un buscador personalizado en el servicio Custom Search Engine de Google (CSE, https://cse.google.es). Es muy sencillo y evitará tener que usar el operador «site» todo el rato, ya que permite generar una lista de sitios que interesan, y solo buscará en ellos.[2] Las url elegidas pueden ser de medios, centros de análisis, cuentas de Twitter, webs o secciones dentro de una web (por ejemplo, http://www.globograma.es/tag/periodismo-internacional). El lector puede insertar ese buscador personalizado en su sitio web, guardar la url que se genera para volver a ella cuando quiera o compartirla públicamente para que otros la usen. En todo momento podrá modificar o completar sus elecciones desde cse.google.es.

En CSE también es posible añadir «tipos» de Schema.org: son un conjunto de etiquetas html acordadas por Google, Bing y Yahoo para distinguir mejor ciertos datos estructurados. Por ejemplo, si al periodista solo le interesan películas, puede añadir el tipo [Movie] a su buscador. Si lo ha configurado con el objetivo de encontrar personas, puede añadir el tipo [Person]. Para reporteros gráficos: si solo se buscan imágenes o videos se pueden añadir los tipos [ImageObject] y [VideoObject]. Schemes.org es complejo para quien no esté familiarizado con codificación pero

2. Rubio, Yaiza y Brezo, Félix: «Estrategias de búsqueda para el analista (con buscadores personalizados)», Elevenpahts.com, 18-9-2017 [http://blog.elevenpaths.com/2017/09/estrategias-de-busqueda-para-el.html; consultado el 8-1-2018]

el buscador CSE puede crearse sin estos tipos y ya estaría prestando gran ayuda.[3]

Aunque se ponga énfasis en dominar Google, conviene conocer más opciones (en Diigo-Globograma hay una lista de otros buscadores: de medios, científicos, musicales, académicos... (https://www.diigo.com/profile/globograma/search-engines). Inteltechniques, un imprescindible recurso de OSINT que será muy mencionado en este manual, ofrece una lista de buscadores propia y la posibilidad de realizar una investigación en todos a la vez (https://inteltechniques.com/osint/menu.search.html).

3. Búsquedas avanzadas en Twitter y Tweetdeck

Se puede buscar en Twitter desde Google [verificación site:twitter.com]. En caso de noticias de última hora, se propone empezar localizando rápidamente listas de calidad:

- Buscar una lista llamada de determinada manera. Aquí «Bruselas» (se obtendrán más resultados con el nombre en inglés, Brussels): [site:twitter.com/*/lists/Brussels]
- Buscar cualquier lista sobre un asunto concreto y de la que se desconoce el nombre. Aquí «Siria» (Syria): [site: twitter.com inurl:lists inurl:syria]

3. Merino, Marcos: «¿Qué es Schema.org?», TicBeat, 3-5-2015 [http://www.ticbeat.com/tecnologias/que-es-schemaorg; consultado el 3-5-2018]

También se puede buscar en Twitter desde Inteltechniques.com (https://inteltechniques.com/osint/twitter.html). Si no funciona este enlace directo, ir a la sección «Tools» en el menú horizontal superior de Inteltechniques.com y, dentro de ella, elegir en el menú vertical de la izquierda la subsección «Twitter».

Otra opción es buscar en esta red social desde Tweetdeck. Es aconsejable experimentar con la cadena de búsqueda en la propia caja de Twitter (es decir, desde https://twitter.com/search-home) y si funciona pasarla a Tweetdeck. Pueden usarse operadores y cadenas avanzadas como [Madrid –Real] y [Cataluña OR Catalunya], y también términos dentro de perfiles específicos [Catalonia from:BBCWorld], palabras dentro de listas [Mosul list:globograma/corresponsales], tuits que estén teniendo mucho eco [Macron min_retweets:45 OR min_replies:15], solo tuits que contengan material multimedia [Iran filter:media] o solo tuits con imágenes [Mexico filter:images] o procedentes de medios [filter:news]. Hay alguna opción más en Globograma.com, «Operadores de búsqueda avanzada para periodistas» (http://www.globograma.es/operadores-de-busqueda-para-periodistas/#twitter).

Se recuerda la importancia de buscar **poniéndose en la mente del emisor**. En Twitter, donde abundan las valoraciones personales, probablemente el testigo de un suceso extraordinario recurra a los pronombres «me» o «a mí» para contar su experiencia personal.[4]

4. Victor, Daniel: «The one word journalists should add to Twitter searches that you probably haven`t considered», Medium.com, 27-4-2015 [https://medium.com/@bydanielvictor/the-one-word-reporters-should-add-to-twitter-searches-that-you-probably-haven-t-considered-fadab1bc34e8; consultado el 2-1-2018]

4. Búsquedas externas en Facebook

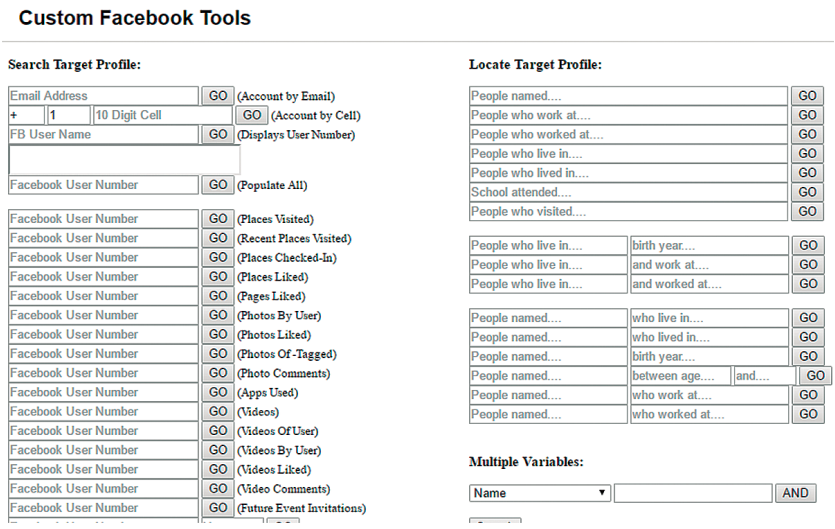
Los periodistas suelen tener dificultad para encontrar información en Facebook. En parte se debe a los frecuentes cambios en su sistema, que provocan incertidumbre. Sin embargo, es necesario manejarse con soltura en este caladero: aunque Twitter es el ágora de los reporteros Facebook es en muchos países la red donde se expresa la gente. Para los mejores resultados de búsqueda, ha de configurarse en inglés (*English-US*).

Lo más sencillo es buscar desde fuera de la plataforma. En Google basta con utilizar «site» solo o en combinación con otros operadores. Con [«resultado electoral» intitle:honduras site:facebook.com] aparecerán todos los post públicos de usuarios de Facebook sobre el resultado electoral en Honduras.

Hay otros recursos externos que buscan información derivada de la actividad de sujetos concretos en Facebook. Para funcionar, requieren conocer el identificador o ID único que recibe todo usuario en esta red social. Tal ID puede obtenerse en FindMyFBID (https://findmyfbid.com). Situado en este servicio, se introduce la url del objetivo en Facebook (por ejemplo, http://www.facebook.com/pepitina.gomez). Aparecerá el número ID que corresponda a ese perfil.. Los países y las grandes ciudades también tienen su propio ID. Se obtiene buscando su página en Facebook dentro de la pestaña «Places» (lugares). Al abrirla, la url mostrará el ID (https://www.facebook.com/places/Things-to-do-in-Madrid-Spain/106504859386230). Para mayor seguridad esa url puede llevarse a FindmyFBID, que detectará el identificador. Hay que evitar confundir las páginas oficiales de lugares con otras que presentan nombres similares pero son de corte publicitario o asociativo. Las que verdaderamente representan un emplazamiento aparecen entre los resultados de búsqueda acompañadas del símbolo de geolocalización ( ).

Una vez se disponga del ID del objetivo, y autenticado en Facebook, se pueden usar los servicios externos Stalkscan.com (https://stalkscan.com), Inteltechniques Facebook (https://inteltechniques.com/osint/facebook.html) o Graph Tips (http://graph.tips/beta/). Se recomienda mantener Facebook abierto en una pestaña y estas herramientas de búsqueda en otra. Si hay algo que el objetivo haya publicado o realizado en abierto (dar «me gusta» en un comentario público, por ejemplo), estos tres recursos lo van a detectar. No violentan ninguna cuenta personal ni acceden a publicaciones privadas pero, como si se tratara de una aspiradora, extraen todas aquellas huellas que se hayan dejado en abierto inadvertidamente. Se sugiere al lector que pruebe Inteltechniques, el servicio que más suele impresionar, examinando la información que arroja su propio ID.

Figura 4. Inteltechniques Facebook



Fuente: Inteltechniques.com.

La única forma de evitar la labor de estas herramientas es solicitar que buscadores externos no enlacen a nuestro perfil en Facebook. Esto puede hacerse desde el menú superior de esta red social, en la flecha que abre un desplegable donde se encuentra la opción «Configuración» (*Settings*). Dentro de ella está «Privacidad» (*Privacy*).

El consejo que se ofrece para obtener mejor información en servicios como Inteltechniques es buscar en acciones del objetivo realizadas en perfiles ajenos, donde no solemos detenernos a comprobar si la configuración es pública o privada. Por ejemplo: si se rastrean fotografías publicadas por X y apenas se obtiene material, podrían buscarse comentarios de ese usuario en fotografías ajenas donde quizá aparezca él mismo o sus amistades, aunque no esté etiquetado.

Las posibilidades son numerosas: indagar qué ha dicho una persona, a qué eventos ha asistido, en qué hoteles se ha alojado. Es posible comparar fotos, lugares o grupos en común con otro sujeto investigado y también comprobar en qué lugares han coincidido ambos. Otra posibilidad son las búsquedas indirectas, en las que no se rastrea a alguien, sino que se buscan perfiles determinados: personas a las que guste una foto, lugar o grupo. Todo ello es de un valor incalculable a la hora de verificar datos sobre el protagonista repentino de una última hora (un premiado, un criminal).

5. Búsquedas desde el propio Facebook

Además de estos recursos externos, para buscar desde Facebook se puede recurrir a su **caja de búsqueda,** los **menús superior e izquierdo y** la propia **barra de navegación**. Se recuerda una vez más que la plataforma debe estar configurada en inglés.

5.1. Menú y caja de búsqueda

Es accesible desde la portada (*Home*). Si se introducen en ella una o varias palabras clave ([protestas en Irán], por ejemplo), antes aún de darle a «buscar» o «Enter», se muestra un desplegable que abajo da la opción «Ver todos los resultados». Pulsando ahí el usuario queda situado ante lo que será su cuadro de mando para búsquedas con el menú. Aparece uno horizontal en la parte superior para centrarse en entradas (*posts*), personas o páginas. Otro menú vertical a la izquierda deja establecer filtros por ubicación, fecha, autor de la información (gobiernos, servicios de emergencia...), etc. Para obtener solo entradas de un usuario concreto, seleccione su nombre en «Elija una fuente» (*Choose a source*).

Las siguientes propuestas funcionarían en la caja de búsqueda y estarían dirigidas a obtener imágenes y vídeos procedentes de lugares concretos. Elegir «vídeos» o «fotos» según convenga, así como la ubicación.

- Vídeos tomados recientemente en X: [recent videos taken in X]. Ejemplo: Vídeos tomados recientemente en Bruselas: [recent videos taken in Brussels]
- Vídeos tomados en el lugar X desde la fecha Y: [videos taken in X from date Y]. Ejemplo: Vídeos tomados en Bruselas desde enero de 2017: [videos taken in Brussels from January 2017]
- Vídeos tomados en X por personas de Y: [Videos taken in X by people from Y]. Ejemplo: Vídeos tomados en Madrid por personas de Chile: [videos taken in Madrid by people from Chile]

Facebook ofrece resultados que combinan lo objetivamente interesante con lo publicado por personas conectadas al usuario.

También da prioridad al material multimedia sobre los textos. Ocasionalmente pueden aparecer informaciones no relacionadas con lo solicitado, al menos de manera obvia. **La búsqueda no es perfecta**. Tampoco es preciso el filtro «ubicación». Si se solicitan entradas escritas desde París pueden aparecer emisores que afirmen estar emplazados habitualmente en ese lugar, aunque en ese momento no lo estén, o que mencionen esa ciudad en sus entradas públicas. No obstante, los filtros ayudan al menos a reducir el ruido informativo.

5.2. Barra de navegación

Localizar a testigos, contrastar testimonios, comprobar la opinión de ciertas comunidades o localizar material amateur de valor. Las siguientes cadenas de búsqueda pueden ayudar a todo esto. Requieren números identificadores (ID) y por su complejidad y longitud se introducen directamente en la barra de navegación. Parten de las enseñanzas de Henk van Ess (@henkvaness), uno de los mayores expertos internacionales en búsquedas junto a Paul Myers (@paulmyersBBC). No hace falta «redactarlas» cada vez, pueden copiarse y pegarse desde este manual o desde un documento que las contenga. Solo será necesario cambiar cada vez los términos clave. Para que funcionen hay que estar autenticado en Facebook.

Es recomendable jugar con estas expresiones avanzadas para entender su **lógica de redacción** y poderla reproducir si herramientas más sencillas como Inteltechniques desaparecen o se hacen de pago.

- Residentes en el lugar A que han visitado el lugar B [https://www.facebook.com/search/IDlugarB/visitors/IDlugarA/home-residents/intersect/]
  Ejemplo: Personas de Francia que han visitado Siria: [https://www.facebook.com/search/112708625409031/visitors/105604449474183/home-residents/intersect/]

- Fotos de residentes en A que han visitado B [https://www.facebook.com/search/IDlugarB/visitors/IDlugarA/home-residents/intersect/photos-of]
  Ejemplo: Fotos de residentes en Francia que han visitado Siria: [https://www.facebook.com/search/112708625409031/visitors/105604449474183/home-residents/intersect/]

- Fotos que gustan a gente de A que ha visitado B: [https://www.facebook.com/search/IDlugarB/visitors/IDlugarA/home-residents/intersect/photos-liked]
  Ejemplo: Fotos que gustan a la gente de Francia que ha visitado Siria. [https://www.facebook.com/search/112708625409031/visitors/105604449474183/home-residents/intersect/photos-liked]

- Un clásico: fotos donde una persona esté etiquetada: [https://www.facebook.com/search/IDusuario/photos-tagged]
  Ejemplo: Fotos que etiquetan al político holandés Geert Wilders: [https://www.facebook.com/search/202064936858448/photos-tagged]

- Imágenes relacionadas con una palabra clave (sustituya «photos» por «videos» si le interesa esto segundo)

[https://www.facebook.com/search/str/palabraclave/photos-keyword]
Ejemplo: Imágenes relacionadas con la palabra refugiados
[https://www.facebook.com/search/str/refugees/photos-keyword]

- Vídeos sobre el tema X publicados en el lugar Y
[https://www.facebook.com/search/str/palabraclave/videos-keyword/IDlugar/videos-in/intersect]
Ejemplo: Vídeos de toros en Francia
[https://www.facebook.com/search/str/toros/videos-keyword/105604449474183/videos-in/intersect]

- Personas que hayan nacido en un lugar, vivan en otro y trabajen en una entidad/sector específico:
https://www.facebook.com/search/str/IDlugarnacimiento/pages-named/users-birth-place/IDlugarresidencia/residents/str/IDempresa/pages-named/employees/intersect]
Ejemplo: Personas nacidas en India que residen en Londres y que trabajan en el Ejército
[https://www.facebook.com/search/str/india/pages-named/users-birth-place/106078429431815/residents/str/army/pages-named/employees/intersect].

Hay más cadenas en Globograma.com (http://www.globograma.es/verificacion-digital-en-facebook/), siendo especialmente útiles las que indagan en pertenencia a grupos.

6. Búsquedas en otras redes

Las estrategias para Twitter y Facebook pueden intentar desarrollarse en otras redes sociales. Pruebe en sus cajas de búsqueda con el operador «site», por ejemplo. Utilice también recursos externos como Inteltechniques, que ofrece desde su sección Tools atajos avanzados para Instagram, YouTube y Linkedin (https://inteltechniques.com). Otra opción es personalizar el buscador CSE de Google para que indague en una o en varias redes sociales.

Los periodistas están acostumbrados a buscar contenidos, pero también se pueden localizar equipos conectados a la red. En el Internet de las cosas que se está expandiendo hay ya motores que, con las expresiones adecuadas, conducen a **máquinas indexadas** (cámaras web, impresoras, PCs...). El más conocido es Shodan (https://shodan.io), enfocado a *pentesting* o pruebas de intrusión en equipos informáticos. Si se busca [«default passwords»] en este motor se puede acceder a aparatos conectados cuyos dueños no cambiaron la contraseña de fábrica, una invitación a amigos no deseados. Aunque la explicación de Shodan queda fuera de este manual, el usuario puede probarlo creando una cuenta, paso necesario para acceder a sus opciones de búsqueda más sofisticadas.

Si el lector ha llegado hasta aquí, ya domina la configuración del escritorio y las búsquedas avanzadas. Ahora la sugerencia es recordar las preguntas básicas de la profesión periodística, las llamadas 5W: **quién, qué, cuándo, dónde y por qué** (*who*, *what*, *when*, *where*, *why*), además de cómo. Los próximos capítulos tratan de aportar recursos digitales que permitan responder en cada caso.

Con todo ello, no debe olvidarse que sigue siendo necesario realizar gestiones en el mundo real, documentarse y sobre

todo acudir al lugar de los hechos para observar y hablar con fuentes y testigos. La red no es una excusa para evitar esos pasos, que hay que seguir dando siempre que sea posible, pero es un complemento excepcional en cada uno de ellos.[5]

5. Para una aproximación breve a la verificación digital desde las 5W de la profesión: Redondo, Myriam: «Cómo verificar en un mundo digital lleno de trampas», Revista5w.com, 4-5-2017 [https://www.revista5w.com/newsroom/como-verificar-un-mundo-digital-lleno-trampas]

Capítulo VI
Quién (I). Fuentes / usuarios

Para comprender el contexto de una noticia **siga a la fuente**. El mejor consejo para realizar una lectura crítica es preguntarse **de dónde procede la información**, a tres niveles: qué medio o sitio publica, quién firma y qué fuentes cita.

«Quién dice» es la primera pregunta de las 5W de la profesión. El peso de las fuentes en las **rutinas periodísticas** es y será siempre muy notable. Estas son algunas consideraciones generales sobre ellas:

- El profesor Guillermo Peris (@waltzing_piglet) destacaba en las redes sociales cómo un diario mencionaba «según varios tuiteros» como fuente de una noticia (http://bit.ly/2ov8Tnx). No se cita a Internet como una fuente en sí. Siempre hay personas detrás de los hechos/datos/declaraciones. «Lo han dicho en Facebook», «Lo dice Twitter» son expresiones que debería ser desterradas del vocabulario mediático.
- Lejos de conformarse con identificar a una fuente, hay que intentar hablar con ella. Skype puede ser una buena opción.
- Cuantas más fuentes se consulten, mejor. Tradicionalmente ha existido la costumbre de «triangular» consultando al menos a tres personas de distintas tendencias, pero la cifra ascenderá todo lo necesario hasta tenerlo claro. Las fuentes utilizadas deben ser relevantes para el tema, esto es, no basta con que muchos tuiteros indiquen que algo está «confirmado».

- Ha de evitarse la «trampa del equilibrio». Es el temido «Él dice, ella dice» (*he says, she says*), propio del periodismo declarativo. Consiste en reproducir dos visiones enfrentadas del mundo casi robóticamente, argumento y contraargumento, dejando al ciudadano perdido en la duda. Es uno de los rasgos más criticados de la información política actual y complica otras coberturas, como la del cambio climático. Dentro de lo posible la verificación digital debe ayudar a evitarlo, destacándole al lector la explicación más certera de acuerdo con los hechos.
- Interesa saber qué usuario fue el primero que publicó un contenido en las redes, pero lo más importante es identificar al usuario que lo captó/fabricó. Muchas veces se olvida que ambos pueden no coincidir y esto conlleva numerosos fallos en verificación (atribución de fechas incorrectas a un acontecimiento). Recuerde siempre: lo que está viendo puede ser una copia del material original.
- La ubicación de esa fuente en un asunto especialmente relevante y hay que tomar todas las precauciones para aclararla, sin fiarse de la ciudad que se indica en la biografía de una red social. Como se verá en el último capítulo, la geolocalización es un campo escurridizo y existen mecanismos para fingir ubicaciones.

Este capítulo se centra en la investigación de individuos en redes sociales, y por sus amplias posibilidades remite especialmente a Twitter.

1. Investigar un nombre

Cuando lo primero que se conoce de un objetivo es su nombre y apellido o apellidos, ¿cómo actuar? Googlearlo es el primer paso al que pueden seguir otros más:

- Buscar ese nombre y apellidos en **otros buscadores** (expresión exacta, con el operador «comillas»: [«Amelio González Paz»].
- Buscar los **apellidos con el nombre tras ellos** para encontrar posibles documentos oficiales ([«González Paz, Amelio»]) y buscar solo los apellidos ([«Gónzalez Paz»]) para conocer la existencia de hermanos. Si se encuentran familiares la investigación puede seguir a partir de ellos (domicilio, fotos compartidas...).
- Recurrir a **directorios de personas**. En países como Estados Unidos los directorios conducen a información muy detallada del objetivo como el número de teléfono, la dirección postal y hasta un mapa señalando su hogar. En Inteltechniques-Real Name (https://inteltechniques.com/osint/menu.name.html) ofrecen un amplio listado de estos recursos, entre los que destaca Spokeo (https://www.spokeo.com/). A veces, tras varios pasos y al borde de obtener la información que se solicita, se avisa de que los registros se ofrecerán solo previo pago. En esos casos hay que valorar si la relevancia de la investigación aconseja abonar esa cantidad. Thatsthem es otro directorio útil para EEUU (https://thatsthem.com). En Europa las leyes de protección de datos son más estrictas y es difícil obtener información personal en este tipo de servicios. Se recomienda Webmii: es gratuito y ofrece información muy genérica, pero a veces desvela puertas interesantes a las redes sociales del objetivo.

- **Averiguar el email**: si se conoce la compañía para la que trabaja el investigado puede tratar de descubrirse su correo electrónico en Email Format (http://www.email-format.com/) o Mailtester (http://mailtester.com/). Si no se conoce se recomienda probar a partir de hipotéticos alias. Por ejemplo, si el objetivo se llama Fernando García, se rastrearían las expresiones fgarcia, fernandogarcia o fergarcia acompañadas de la arroba y los dominios de correo más habituales (Gmail, Hotmail, Yahoo...). Esta búsqueda puede realizarse en un motor genérico pero se recomiendan las cinco últimas cajas de búsqueda de Inteltechniques - User Name (https://inteltechniques.com/osint/username.html): Email search, Leaks-HIBP, Leaks-H-E, Leaks-HIBP API y Leaks-H-E API. La primera asocia esos nombres de usuario a servicios como Gmail, Yahoo o Hotmail. Las demás analizan si tales nombres aparecen vinculados a otros dominios de correo más alternativos o a bases de datos de cuentas pirateadas como HaveIbeenpwned.com. La búsqueda se abre en múltiples pestañas, una por cada base de datos analizada.
- **Verificar cualquier imagen** vinculada al objetivo. ¿La de su perfil es real? ¿Aparece en otros lugares? ¿Ni siquiera tiene imagen? En 2017 Twitter sustituyó su popular «huevo» por una figura gris para representar a los usuarios sin foto de perfil, pero la impresión es la misma con ambos recursos: cuentas poco fiables.

2. Investigar un alias (recursos)

Varias herramientas gratuitas ayudan a investigar a un usuario a partir de su alias en Twitter. Tinfoleak (https://tinfoleak.com/), del español Vicente Aguilera, analiza los doscientos últimos tuits

del objetivo: fotos, sistemas operativos desde los que tuitea, etiquetas y también su ubicación. La información se solicita y se recibe por email. El servicio es gratuito.

Otros recursos ofrecen este tipo de información en línea. Hay que fijarse en cuántos tuits extraen y qué aspectos analizan. Foller.me (https://foller.me), Twopcharts (http://twopcharts.com/), Followthehashtag (http://followthehashtag.com) y Followerwonk (https://moz.com/followerwonk/) son los más prácticos dentro de la gratuidad o semigratuidad (*freemium*, lo que quiere decir que permiten un número escaso de usos o solo dan acceso a las opciones básicas). Aunque en los siguientes párrafos se mencione principalmente Twopcharts porque presenta atajos sencillos a cada función, el lector hará bien en examinar todas las herramientas y ver con cuál se siente más cómodo.

Foller.me es la que permite el análisis más rápido, no exige identificarse ni abrir una cuenta, pero realiza sus dictámenes basándose solo en los cien últimos tuits del objetivo. Son muy pocos y podrían fingirse para alterar el perfil, pero la herramienta es útil ante una última hora. Por ejemplo, en los primeros momentos tras un hipotético terremoto en México, sería difícil que un usuario publicase cien tuits para aparentar conocer asuntos mexicanos. Los informes de Twopcharts, también de acceso libre, se basan en doscientos tuits.

Followthehashtag requiere autorización de acceso a la cuenta de Twitter, pero a cambio aporta un análisis más profundo: mil quinientos tuits o siete días de actividad. Está pensada para investigar etiquetas y palabras clave, pero también ayuda con usuarios. Su búsqueda avanzada y su cuadro de mando (*Dashboard*) son bastante valiosos para ser gratuitos. En cuanto a Followerwonk, que requiere asimismo autorización desde Twitter, se utiliza sobre todo para hallar perfiles con rasgos determinados, compa-

rar usuarios y analizar perfiles de seguidores y seguidos (dónde se encuentran, qué horario de actividad tienen, etc.). Su búsqueda avanzada es igualmente interesante (en la franja horizontal superior de su portada, hay que pulsar en «*More options*»).

Es importante conocer las **limitaciones de estas herramientas** para no generar expectativas infundadas:

- Son gratuitas y en algún caso están en beta. En cualquier momento pueden desaparecer, dejar de actualizarse o comenzar a exigir un pago.
- La mayoría surgen del ámbito del marketing, se diseñaron con propósitos distintos a los de la verificación y no alcanzan una precisión absoluta. Su información es insuficiente cuando el periodista está ante un caso crítico.
- No hay certeza total sobre la localización que ofrecen para un perfil.
- La actividad que un usuario muestra en Internet siempre es parcial y puede estar llena de lagunas. Cuantas más herramientas use y más pesquisas realice el periodista más se acercará al retrato real del objetivo, y así evitará quedarse con una falsa primera impresión.

Si un tuitero dice ser experto en la monarquía y a partir de estas herramientas se comprueba por ejemplo que su primer seguidor es un periodista reconocido por sus vínculos con el Palacio de La Zarzuela podría pensarse que es así. Pero habría que realizar más comprobaciones para asegurarse. Ambos pueden ser compañeros de colegio. En 2016 se hizo famosa una niña que tuiteaba las penurias de la guerra siria desde Alepo, Bana Alabed (@alabedbana). Gestionaba la cuenta con ayuda de su madre. El hecho de que se expresase en inglés y de que los

primeros perfiles que la siguieran fuesen corresponsales contribuyó a las suspicacias. Se pensó que la pequeña no existía y que la suya era una cuenta falsa enfocada a los medios. Una investigación con fuentes abiertas mostró sin embargo que no había nada en el tuiteo de Bana que revelara engaño en la ubicación o los escenarios descritos. Tiempo después la prensa pudo conocerla en carne y hueso.[1]

Teniendo en cuenta todas estas advertencias, hay muchas comprobaciones digitales que el periodista puede realizar. Antes de ponerse con ello, el primer consejo es guardar ese posible tuit que ha llevado a investigar al usuario por si tiene la tentación de borrarlo, por ejemplo con Archive.today (https://archive.is/).

3. Investigar un alias (procedimientos)

Algunas preguntas o pasos recomendables si se investiga un alias de Twitter. Se apuntan junto al recurso que permite darles respuesta.

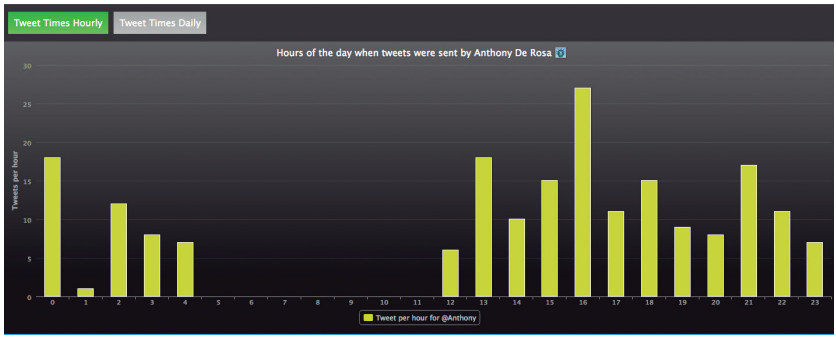
- ¿Hay **otros alias** relacionados con ese en Twitter? Por ejemplo, de @glucamat podría investigarse @gluclamat01, @glucamat02... Twopcharts detecta esos alias secundarios a partir del primero (buscando en «Search Twitter Account»).

1. Al margen del debate sobre si la niña terminó siendo utilizada propagandísticamente por grupos o líderes políticos, su existencia en Alepo durante la guerra fue real, como apuntó Bellingcat. Waters, Nick: «Finding Bana. Proving the existence of a 7-year-old girl in Eastern Aleppo», Bellingcat, 14-12-2016 https://www.bellingcat.com/news/mena/2016/12/14/bana-alabed-verification-using-open-source-information/

- ¿Está ese alias en **otras redes sociales?** Puede investigarse en la mencionada Inteltechniques - Usernames. Hay que investigar la información que ofrezcan esos nuevos perfiles.
- ¿Ofrece pistas de **actividad profesional**? Si el *target* afirma trabajar en la entidad X, ¿le sigue esa entidad en alguna red social o aparece su nombre en la web corporativa? También, ¿se sigue mutuamente con algún especialista de referencia? Quien dice ser un importante cardiólogo debería ser seguido por otro cardiólogo conocido. Twopcharts Relationships: http://twopcharts.com/relationship.
- ¿Quién fue su **primer seguidor**? Puede ser alguien relevante en su vida y dar pistas sobre su entorno más cercano: Social Rank First Follower (https://socialrank.com/firstfollower).
- ¿Cuáles son sus **horarios de actividad**? Si el objetivo dice estar tuiteando desde una ciudad alemana inundada, sus pautas de actividad y sueño coincidirán con las horas de ese país. Cuando se analiza este aspecto hay que comprobar en qué zona horaria se basa el recurso digital. Twopcharts y Foller.me.
- ¿Qué diferencias y similitudes hay entre los **seguidores del objetivo** y los de otros usuarios que traten temas parecidos? FollowerWonk Compare: https://moz.com/followerwonk/compare.
- ¿Acaba de abrir la cuenta o lleva tiempo en la red? Lo segundo es más fiable. Twopcarts - HowlongonTwitter: http://twopcharts.com/howlongontwitter.
- ¿Tuitea con **regularidad**? Una intervención repentinamente intensa es sospechosa. La sección IDcheck de Twopcharts ofrece gráfico histórico: http://twopcharts.com/idcheck.
- ¿Cuáles son sus **inclinaciones**? Tuits en los que el objetivo ha marcado «Me gusta». Twopcharts - IDcheck.

- ¿Ha elaborado **listas**? Son muy reveladoras. Si alguien afirma ser experto en deporte lo normal es que giren sobre este asunto y acierten con los expertos incluidos. Twopcharts - IDcheck.
- ¿De qué **temas** suele hablar? Importan las palabras y etiquetas que utiliza (todos los recursos apuntados las analizan).
- ¿Cuál es el **sentimiento** que destilan los tuits (positivo o negativo)? Foller.me.
- ¿Pueden **geolocalizarse** sus tuits? Followthehashtag y también Geosocialfootprint (http://geosocialfootprint.com/) o Keith Armstrong Tweetmap (https://keitharm.me/projects/tweet) con las habituales cautelas sobre geolocalización.
- ¿Cuáles son sus **tuits con más impacto** (retuiteos, me gusta)? Si el *target* se presenta como un especialista en mediación diplomática pero en su tuit más relevante insulta soezmente... Twopcharts - IDcheck.
- ¿Cuál es la **ratio seguidos/seguidores**? Las cuentas falsas suelen seguir a muchos y tener pocos seguidores, o presentar un número inusualmente alto y muy parecido de seguidores y seguidos. Twopcharts - ID Check.

Figura 5. Ejemplo de horarios de un usuario «humano» con siete horas de sueño



Fuente: Twopcharts.com

- ¿Quién menciona a ese usuario o **quién interactúa** más con él? ¿En qué perfiles influyentes (*influencers*) impacta? Followthehashtag - Dashboard.
- ¿Cómo son los **usuarios que siguen** al objetivo (autoridad, ubicación geográfica, retuits, relación seguidos-seguidores...)? Twopcharts y Followthehashtag.

Conviene profundizar en los **rankings de autoridad** en redes sociales. En Twopcharts - IDcheck se obtiene el Twopscore del objetivo. Se basa en aspectos como la antigüedad de la cuenta o la cercanía en el tiempo de su último tuit. Orienta, pero no ofrece una garantía absoluta. Otros servicios indicadores de influencia son más avanzados, como Klout (http://klout.com), pero tampoco pueden ser considerados determinantes. Hay perfiles falsos que dedican meses a interactuar amablemente con usuarios relevantes ascendiendo posiciones en estos rankings. Hay también cuentas que difunden falsas capturas de pantalla mostrando un nivel más elevado del obtenido realmente en estos rankings; muchos usuarios nunca acuden a la fuente original a comprobarlo.

Además, algunas de las expansiones más dañinas de bulos se deben precisamente a que los hayan creído y difundido de buena fe usuarios con una posición relevante y merecida en las redes. Que un futbolista con autoridad digital y millones de seguidores retuitee la imagen de un accidente de autobús en el extranjero no garantiza que haya estado allí o que haya comprobado la escena.

Muchas redes sociales tienen un símbolo de verificación común (), en el que es muy recomendable fijarse pero que tampoco es determinante. En octubre de 2017, en plena crisis por el proceso independentista catalán, circuló un tuit muy grosero de quien se presentaba como delegado de Cataluña en Estonia. En aquel momento la cuenta estaba verificada, pero el usuario era un

bromista y no un representante oficial. Twitter explicó que había colocado el símbolo cuando el usuario tenía otro cargo previo y no utilizaba su perfil para engañar. El campo de los rankings de influencia y de la corroboración de identidades tiene mucho espacio de mejora y hay investigaciones prometedoras en esa línea.

4. Buscar usuarios con características concretas

En ocasiones el reportero puede estar interesado en hallar mensajes o perfiles sobre temas concretos más que en investigar a un usuario específico.

- Buscar **mensajes exactos** o que excluyan determinados términos: Followthehashtag (botón «Advanced» en la franja superior de su portada) y Twopcharts (botón «Search Tweets»).
- Buscar usuarios con **características específicas** (policía, periodista, abogado, etc.): Followerwonk («Search Bios») y Twopcharts («Search Twitter Accounts»).
- Averiguar **quiénes impulsan una etiqueta.** Followerhashtag, Hashtagify.me (https://hashtagify.me) y Mentionmapp (http://mentionmapp.com). Esta última ofrece una visualización muy sencilla de comprender, aunque requiere darse de alta y ofrece un número limitado de pruebas.

En realidad, contestar con precisión a esta última pregunta (quién impulsa una etiqueta) requeriría realizar un **análisis de redes**. Para ello se emplean programas que extraen grandes volúmenes de tuits (no cientos, sino decenas de miles o millones), realizan cálculos sobre ese conjunto y presentan los resultados de

modo gráfico y comprensivo (*data visualization*). Su estudio queda fuera de este manual, pero al final del mismo se verá una breve introducción a la disciplina.

El análisis de redes requiere de ciertos conocimientos informáticos, tiempo para descargar el material y tiempo para interpretarlo, algo que no suele estar al alcance de los periodistas. Pese a ello, se anima al lector a avanzar en este campo porque supone un plus de calidad en materia de verificación. Mientras tanto, las herramientas anteriores y otras que se verán pueden considerarse remedios decorosos para investigar a un usuario de manera mínimamente profesional. Son rápidos, revelan muchos aspectos útiles y son mucho mejor que nada.

Capítulo VII

Quién (II). Fuentes en redes sociales. Sitios y empresas

1. Facebook e Instagram

Para verificar a un usuario en Facebook pueden seguirse las indicaciones aportadas sobre esta red social en el capítulo referido a búsquedas. Cabe recordar el papel fundamental de Inteltechniques - Facebook y también se destaca PeoplefindThor (http://www.peoplefindthor.dk). Ambos son servicios externos que funcionan solo estando autenticado en Facebook.

Algunas preguntas ayudan a detectar un perfil falso en Facebook:

- ¿Presenta muchos contactos pero apenas está actualizado?
- ¿Tiene fotografías propias o estas son tomadas de Internet, según una búsqueda inversa? ¿La cuenta está llena de imágenes de figuras famosas, cantantes, modelos o mujeres atractivas?
- ¿Sus imágenes etiquetan a muchas personas?
- ¿El investigado dice estar ubicado en países donde Facebook tiene presencia menor? Puede ayudar el mapa mundial de redes sociales de Vincos (http://vincos.it/world-map-of-social-networks/).
- ¿Qué rasgos muestran sus contactos?

- ¿Dispone de listas o participa en grupos con usuarios vinculados a su supuesta experiencia?

También en Instagram pueden realizarse investigaciones de interés. El recurso Inteltechniques vuelve a ser recomendable. Desde su sección «Instagram» (https://inteltechniques.com/osint/menu.instagram.html) se puede indagar en el objetivo a partir de su nombre real, del nombre de usuario que ha elegido o de su número identificador. Este puede obtenerse en lugares como Bufa (http://www.bufa.es/instagram-obtener-id-usuario/).

En junio de 2017 el servicio Stories de Instagram (publicación de fotos y vídeos que desaparecen tras veinticuatro horas) alcanzó los doscientos cincuenta millones de usuarios al día, según la compañía. Es por tanto un servicio que interesa cada vez más como fuente de información y de testimonios visuales. Ya que la plataforma está enfocada a la imagen, otras de sus opciones se verán más detenidamente en el tema específico que se dedica a los recursos gráficos.

2. YouTube

Cada usuario de YouTube dispone de un apartado llamado «Más información» que ofrece datos básicos sobre la cuenta. En él aparece la fecha de creación de la misma y los autores suelen presentarse y publicar enlaces a sitios afiliados. Son caminos que se abren para verificar desde otros puntos.

Inteltechniques no permite investigar a usuarios en YouTube, solo indagar a partir de vídeos específicos (https://inteltechniques.com/osint/menu.youtube.html). Pero el investigador puede plantearse algunas preguntas para detectar inconsistencias y valorar la

fiabilidad del objetivo o su canal. Los expertos de Storyful proponen realizar indagaciones como las siguientes:

- ¿Cuándo se creó la cuenta? ¿Ha aportado contenido fiable en el pasado?
- ¿Presenta el usuario una actividad constante, estable?
- ¿Hay faltas de ortografía, lenguaje coloquial?
- ¿Qué dice el historial del usuario de sus posibles ubicaciones? ¿Los lugares que ha visitado tienen que ver con la información que facilita ahora?
- ¿Giran los vídeos en torno a asuntos relacionados con el que ocupa al investigador?
- ¿Las descripciones de los vídeos son fieles a los mismos?
- ¿Se copia y pega ilegalmente material de otros usuarios o medios (*scraping*)?
- ¿Cuántas personas hay suscritas al canal?
- ¿A qué canales ajenos se ha suscrito el usuario y qué listas de preferencia ha establecido?

Para rastrear la presencia de un usuario de YouTube en otras redes hay que partir de su alias, que a veces se confunde con el del canal. En la página de un vídeo determinado se pulsa sobre el icono que queda debajo y a la izquierda del mismo. El usuario aparecerá en la url de abajo tras la palabra «user» (https://www.youtube.com/user/WebAPM1). Si se pulsa en el texto que acompaña al icono, lo que aparece debajo es la dirección del canal (https://www.youtube.com/channel/UCCtcteYhxGHxKNNj5QiwrgA). Esta diferencia entre canal y usuario puede entenderse mucho mejor consultando las siguientes imágenes: http://www.globograma.es/youtube-2. El alias del usuario puede rastrearse en otras redes en busca de menciones.

3. Linkedin y Reddit

Otro lugar por donde debería pasarse es Linkedin. Presenta un menor impacto de los bulos y da acceso rápido a información formal que puede ser determinante. Se accede a lugares en los que el objetivo ha trabajado, a cursos realizados, a compañeros de oficina.

Además de la opción externa Inteltechniques - Linkedin, que busca por nombre de usuario (https://inteltechniques.com/osint/menu.linkedin.html), se puede indagar desde el interior de la plataforma. Aunque mejoró su interfaz en 2017, su principal dificultad sigue siendo que suelen aparecer muchos nombres similares cuando se investiga un perfil. Pero existen filtros.

El servicio debe configurarse en inglés. Desde portada, una vez autenticado, pulsar en la pequeña foto circular de perfil y en la opción «Idioma» (*Language*) del desplegable que aparece.

Tras introducir la expresión de interés en la caja de búsqueda, se obtiene una página de resultados con un menú horizontal superior y otro vertical a la derecha.

A través de los dos menús los resultados se pueden limitar a personas, empleos, compañías, grupos o centros educativos, así como a contenidos (equivalentes a las entradas o posts en Facebook). El menú de la derecha permite filtrar por parámetros como palabra clave, conexiones, ubicación, compañías, sector de actividad, intereses solidarios o instituciones educativas que los usuarios mencionen en sus currículos.

Se pueden realizar asimismo búsquedas avanzadas con algunos operadores. Además de AND, OR y NOT:

- firstname: busca a usuarios basándose en su nombre de pila [firstname:antonio]

- lastname: busca a partir de un apellido [lastname:fernández]
- title: busca perfiles poniendo énfasis en su actual puesto profesional [title:actor]
- company: busca basándose en la compañía actual de la persona [company:Actorama]
- school: busca asociando usuarios a una institución educativa por la que hayan pasado [school:RESAD]

En las antípodas de Linkedin y precisamente por los motivos contrarios interesa también investigar en Reddit. Si Linkedin es una red profesional, Reddit es una plataforma popular. Puede definirse como un agregador de noticias en inglés organizado por secciones o *subreddits* donde los usuarios dejan enlaces y los comentan, votando a favor o en contra y haciéndolos ganar o perder visibilidad. Es un sistema que se parece en algunos rasgos al español Menéame (https://www.meneame.net), aunque Reddit, que puede resultar muy útil, suele atraer la atención de los medios sobre todo por la generación de rumores.

Reddit Investigator (http://redditinvestigator.com) es el mejor lugar para analizar a un usuario de esta red. La búsqueda se realiza a partir del alias y permite comprobar cuándo se dio de alta en el servicio ese objetivo, cuál de sus enlaces y comentarios ha tenido más votos, cuál es su karma (percepción de que es alguien agradable o desagradable), horas de actividad y sueño, etc.

4. Investigar un sitio web

Se apuntan técnicas para valorar un sitio web: quién lo ha puesto en marcha, con qué otros sitios se relaciona, etc.:

- Buscar la sección «Quiénes somos» o «Contacto» para detectar nombres, teléfonos, emails o direcciones postales. Si nada de esto aparece hay que dudar.
- Consultar a quién pertenece el dominio, quién lo registró.[1] Además del atajo que ofrece la extensión Wayback Machine, el servicio oficial para dominios .com es Whois ICANN (https://whois.icann.org) pero existen otros como Whois.net (https://www.whois.net) o Domaintools (https://whois.domaintools.com). A veces los nombres que aparecen son los de intermediarios de contratación y no los de los titulares del dominio, que han pagado para permanecer ocultos. En ese caso puede consultarse el mismo nombre con otro tipo de extensión que también registre ICANN, por si la han adquirido los mismos dueños decidiendo no pagar por la ocultación en esta dirección secundaria. Por ejemplo, se busca el mismo nombre con .net. Para dominios .es puede utilizarse Dominios.es (http://dominios.es), aunque la información ofrecida es mucho menor.
- Ver cómo era ese sitio en el pasado: Wayback Machine (https://archive.org/web/).[2]

1. Un dominio de Internet es un nombre único que identifica a un sitio web. Ej.: globograma.com. Evita que el internauta tenga que recordar el número IP que se asocia a ese dominio (los nombres se recuerdan más fácilmente que los números): la ICANN (Internet Corporation for Assigned Names and Numbers) es la entidad estadounidense que gestiona los dominios terminados en .com.
2. Este recurso también permite indagar sobre la dirección de un antiguo sitio que ha desaparecido y de cuya dirección no se está seguro. Por ejemplo, si se recuerda que el

- Averiguar la IP vinculada a un dominio o buscar otros dominios relacionados: Spyonweb (http:// spyonweb.com). Muchas veces esa IP será compartida y de poca utilidad, pero si existe una IP única es probable que revele conexiones de interés. También puede indagarse en webs que que compartan los mismos códigos publicitarios de Google Adsense o Google Analytics (lo que querría decir que los ingresos van al mismo destinatario).[3]
- Saber qué dominios corresponden a una IP, qué otros sitios web pertenecen a la misma persona o compañía a partir de su nombre o email, cuál es la evolución histórica de un dominio, la ubicación geográfica de una IP: ViewdDNS (http:// viewdns.info).
- Indagar en contenido que ese sitio pueda querer ocultar. Suele ser contenido sensible o que al haber conllevado problemas legales se deja a resguardo en un directorio llamado «Nombredelsitio.com/robots.txt»). Solía citarse el ejemplo de CasaReal.es (http://www.casareal.es/robots.txt), ahora no disponible, que contuvo en esa lista las entradas relativas a Iñaki Urdangarín cuando fue procesado legalmente. El lector puede hacer la prueba con otras webs.[4]

Grupo PRISA lanzó hacia el año 2000 un portal llamado algo parecido a «Inicio» pero no se encuentra buscando en Google, al introducir en Wayback Machine la expresión [inicio portal prisa site:es] aparece el resultado pretendido: www.inicia.es, con las versiones antiguas pertinentes.

3. Comprobar si los códigos identificativos y de publicidad Google (Google Analytics y Google Adsense) que se detectan en un sitio web están presentes en otros sitios y por tanto comparten dueño se conoce como «método de Chuiso». Aquí se explica en qué consiste. Bermejo, Jaime: «Dominios que tiene registrados una persona. Cómo saberlos», Jaimebermejo.com, 25-5-2017 [https://www.jaimebermejo.com/saber-los-dominios-que-tiene-registrados-una-persona/; consultado el 2-1-2018]

4. Sobre el uso de «robots.txt» se recomienda: Otto, Carlos: «Indultos a políticos y corrupción. Lo que gobiernos y empresas te ocultan en Google», elconfidencial.com, 9-5-2017. https://www.elconfidencial.com/tecnologia/2017-05-09/desindexar-google-boe-

- Revisar el código fuente del sitio, como permiten todos los navegadores por una u otra vía. En Chrome, situarse en un espacio en blanco (no texto, no imagen) de la portada de ese sitio, pulsar botón derecho del ratón o equivalente en Mac y elegir «Ver el código fuente de la página». Dentro de él se pueden hallar nombres propios o pistas de interés. En 2011 surgió una plataforma llamada «Mucho PSOE por hacer», un manifiesto de algunos líderes de este partido en el que transmitían una visión autocrítica de la organización ante un próximo congreso. Negaron estar impulsando ninguna candidatura concreta, pero el periodista Juan Luis Sánchez observó que una de las expresiones contenidas en el código fuente era «Carmen Chacón», entonces ministra de Defensa. Los programadores borraron la referencia.[5]

5. Investigar una entidad o empresa

Wikipedia, una plataforma denostada tan a menudo, no es buena idea como fuente única en una investigación, pero a veces constituye una de las mejores puertas de entrada para un rastreo digital en profundidad. Cuando se trata de información empresarial suele incluir posibles problemas sociales o legales de las firmas que nunca aparecerían en la web corporativa o en otros sitios más formales. Dispone de mucha más información en inglés que en español.[6]

---

eva-belmonte-samuel-parra_1374332/]. Un ejemplo de directorio robots.txt con humor: http://www.senormunoz.es/robots.txt

5. *El País*: «En el código fuente estaba la clave», El País, 21-12-2011 [https://politica.elpais.com/politica/2011/12/21/actualidad/1324457772_658075.html; consultado el 2-1-2018]

6. Ibáñez, Álvaro: «Wikipedia. Un recurso informativo más fiable y resiliente de lo que parece», *El País*, 18-9-2017 [https://elpais.com/tecnologia/2017/09/13/actualidad/1505313335_934389.html; consultado el 5-1-2018].

Linkedin también es un lugar muy útil para investigar sobre empresas (encontrar empleados, contactar con ellos). Y hay otras direcciones de interés:

- LibreBORME (https://libreborme.net). Es un sitio en español para realizar consultas y recibir notificaciones sobre lo que se publica en el Boletín Oficial del Registro Mercantil (BORME), que está en formato electrónico desde 2016. El BORME recoge los cambios y operaciones que las compañías españolas están obligadas a comunicar oficialmente; LibreBORME permite buscar en ellos por empresa o por persona.
- Open Corporates (https://opencorporates.com). En inglés, se presenta como la mayor base de datos corporativa del mundo (más de cien millones de empresas indexadas). Extrae información de diferentes bases de datos para ofrecérsela al usuario de una forma más comprensible. Se puede buscar por responsable empresarial y compañía. A partir de un directivo, aporta los nombres de otros directivos en su misma firma. A partir de una compañía, ofrece datos como su dirección de registro, sus principales accionistas, sus CEO...
- Investigative dashboard (https://investigativedashboard.org). En inglés, facilita la búsqueda de documentos, personas y compañías a partir de investigaciones periodísticas anteriores o de bases de datos oficiales. Ofrece relaciones entre ellas, registros nacionales donde están presentes, países en los que operan...
- Arachnys Compass (https://compass.arachnys.com). Arachnys es una compañía de tecnología y gestión de riesgo que ayuda a entidades públicas o privadas mediante la automatización y la inteligencia de datos. Sus servicios son de pago, pero pone a

disposición del público atajos a una impresionante relación gratuita de bases de datos corporativas y de litigación. Se busca por: nombre del negocio, dirección de contacto, responsables, accionistas, información bursátil, información judicial, etc., y también por país. El periodista interesado en investigar una empresa puede acudir a los registros oficiales que se apuntan para el país donde está ubicada, comprobando qué fuentes de información corporativa existen. Habrá algunas bases de datos de acceso público y gratuito, pero otras requerirán un registro o incluso un pago para finalizar la consulta. Es decisión del reportero invertir esa cuantía o no en función de la relevancia de la investigación.

El periodismo de datos es la escuela profesional que más ha avanzado en investigación corporativa, especialmente cuando tiene carácter transnacional. Solo hay que pensar en la tarea del Consorcio Internacional de Periodistas de Investigación (ICIJ) y en sus exclusivas de impacto mundial: Swissleaks, Offshore Leaks, los Papeles de Panamá y los Papeles del Paraíso.

Muchas veces los prolongados trabajos de estos equipos pasan en algún momento por el uso intensivo de bases de datos corporativas, además de practicarse otras técnicas como el raspado o *web scraping*. Consiste en la extracción de datos disponibles en una web en formatos como PDF para convertirlos a otros formatos que permitan desmenuzarlos y analizarlos mejor. El periodista Daniele Grasso ha explicado la gran utilidad que puede tener este ejercicio para una investigación sobre instituciones públicas.[7]

7. Grasso, Daniele: «Cuatro formas de hacer web scraping desde y para la redacción», Elconfidencial.com, 25-10-2016 [http://bit.ly/2v5rtJ9; consultado el 5-1-2018]

Para ampliar información sobre investigaciones corporativas o sobre otras técnicas y recursos del periodismo de datos, además del *web scraping*, se sugiere: a) realizar los cursos ofrecidos por especialistas en esta materia, como los de la experta española del ICIJ Mar Cabra, @cabralens, algunos de los cuales están disponibles en línea (por ejemplo, en https://www.medialab-prado.es/); b) consultar algunos de los buenos manuales disponibles en la red;[8] y c) seguir los pasos de las distintas asociaciones nacionales de periodistas de investigación. En España dicha asociación se creó en 2017, presidida por el periodista Antonio Rubio (http://bit.ly/2ETSaRI).

6. Maltego

Sería injusto finalizar el apartado referido a «Quién» sin mencionar el recurso OSINT Maltego (http://bit.ly/2l9iz3A). Este programa está entre los más avanzados para investigar usuarios y sitios web y aglutina algunos de los servicios esenciales mencionados en los dos capítulos anteriores, ofreciéndolos de manera gráfica.

Es de pago, pero cuenta con una versión gratuita (Maltego CE) de opciones más limitadas. Requiere registro, instalación, paciencia con el aprendizaje y cierta familiaridad con conceptos informáticos, pero sus aportes son muy poderosos. Permite por ejemplo averiguar las direcciones de correo asociadas a un dominio corporativo o comprobar cuántos sitios web se relacionan con él (v=8sTbcqdNqc). También ayuda a localizar posibles emails

8. Como propuesta de estos manuales: Crucianelli, Sandra (2013). *Herramientas digitales para periodistas*, Knight Center for Journalism in the Americas, Universidad de Texas [https://knightcenter.utexas.edu/books/HDPP.pdf].

y números de teléfono de usuarios, las menciones que recibe de otras personas en Internet o sus perfiles en redes sociales (v=k_Nbel0SEzo).

Es difícil explicar Maltego en formato textual. Frente a otros recursos online mencionados resulta un programa complejo.

Capítulo VIII

Qué y cuándo. Textos, imágenes y vídeos

En verificación digital la pregunta «qué» está muy ligada al «cuándo» porque lo primero que se ha de comprobar es si se está ante un contenido original y actual. Hay tres comprobaciones básicas:

- La persona que publica el material puede no ser la misma que lo elaboró o grabó.
- Quizá el contenido haya sido publicado días o meses después de su grabación.
- La fecha indicada en la red social donde se ha encontrado el contenido puede referirse a otra zona horaria.

1. Aparición en Internet y fechas de publicación

1.1. Comprobar apariciones anteriores

Para comprobar si una información es antigua se buscará su título en Internet, respetando la literalidad (título entrecomillado) o recurriendo a términos descriptivos y enunciados parecidos. La búsqueda puede realizarse en Google y otros motores y también en la caja de búsqueda avanzada de redes sociales. Quienes se dedican a la promoción de noticias engañosas suelen publicar la misma en varios idiomas cambiando la ubicación (falsos avisos de

bomba, por ejemplo). Incluso llegan a elaborar notas de prensa y citar supuestos informes que corroboran las mentiras. Hay que comprobarlo todo.[1]

Si la investigación se topa con alguna web que ya no está disponible vienen al rescate Wayback Machine o la caché de Google. Así, para acceder a un tuit que se ha borrado se busca su url. Junto al primero de los resultados que ofrece el buscador, se hace clic en el pequeño icono triangular invertido y se accede a la caché. Aparecerá dicho tuit aunque su contenido se haya eliminado.

Es recomendable hacer uso del operador «site» para buscar dentro de webs antibulos. Un lugar imprescindible es Snopes (https://www.snopes.com), que se dedica desde 1994 a la detección de falsedades y leyendas urbanas. Ahí puede encontrarse hasta el mítico episodio nunca acontecido de Ricky Martin y la mermelada, que en su origen nada tenía que ver con un cantante latino. Lugares de referencia en español son Vost España (https://www.vost.es) y Maldita.es (https://www.maldita.es). También puede realizarse una búsqueda avanzada en Twitter para detectar menciones a la historia en cuentas especializadas como @Malditobulo o @VostSpain (imagen explicativa: http://www.globograma.es/avanzada).

Para comprobar la actualidad de una imagen o vídeo hay que detectar su identificador único, sobre todo en Instagram y YouTube. Después este identificador se buscará en Google para saber si el contenido ha sido embebido ya en alguna web.

– Instagram. Abra el post. En la url completa que aparece en la barra de navegación verá el identificador: https://www.instagram.com/p/**BS5z3EJAQsa**/?taken-by=e_pinter_

1. Para ampliar información sobre la verificación de notas de prensa y estudios: Cobo, Silvia: *Internet para periodistas*, UOC: Barcelona, págs. 168-171.

– YouTube. Abra el vídeo. En la url resultante el identificador será el siguiente: https://www.youtube.com/watch?v=**y31jYDLjasc**. Esa expresión puede rastrearse en Google o desde Inteltechniques - YouTube.

También es posible buscar esas url enteras en Twitter, para saber si alguien más ha hecho referencia a esos contenidos.

1.2. Fechas

Para manejarse con las distintas zonas horarias con que uno puede topar en redes son recurrentes convertidores como Time and Date (https://www.timeanddate.com) y Hora.es (http://www.hora.es/), este último en español. La Hora Universal Coordinada (UTC) suele ser la referencia internacional. España sigue el Horario Europeo Central (UTC+1) entre octubre y marzo y el Horario Europeo Central de Verano (UTC+2) desde el último domingo de marzo hasta el último de octubre. Es frecuente errar en este campo porque las redes sociales ofrecen la hora de publicación de los contenidos de modo distinto. A continuación se ofrecen algunas pistas a partir de información facilitada por First Draft News.

- Twitter. Una primera referencia temporal del tuit aparece junto al nombre de usuario que lo publica. Al pulsar en esa indicación surge bajo el tuit la hora completa. Si el periodista está autenticado, verá dicha hora en la zona que haya marcado como preferente al configurar su cuenta. Si no está autenticado verá la fecha en Horario Estándar Pacífico (PST), ocho horas menos que la hora UTC.

- Instagram. La fecha aparece dentro del código html que la plataforma facilita para embeber ese material en otras webs. Se obtiene pulsando en los tres puntos que acompañan a cada imagen y eligiendo, entre las opciones que aparecen, «Código de inserción». Se copia y pega ese código en un documento en blanco o cuaderno de notas para su mejor análisis. La fecha aparecerá en la parte inferior, primero en hora UTC y a su lado en Horario Pacífico.
- Facebook. La comprobación de fecha es compleja y es mejor estar autenticado. Cada post ofrece una fecha general. Colocando el ratón sobre ella, surge el detalle. La hora se muestra en la zona horaria configurada en el ordenador del investigador.[2]
- YouTube. Llevar el vídeo a YouTube Data Viewer (https://citizenevidence.amnestyusa.org). Aparece en hora UTC.

2. Metadatos

Una forma de comprobar cuándo se creó un documento o se tomó una fotografía/vídeo son los metadatos que la describen. No aparecen a simple vista y por eso también se les llama datos ocultos. Los hay de distintos tipos, como los que describen imágenes (EXIF, Exchangeable Image File Format) o posiciones geográficas (GPS, Global Positioning System). Sobre todo, interesan para tratar de averiguar la fecha de creación de ese archivo, la autoría y el origen geográfico.

2. West, Mick: «How to find the exact upload time of a Facebook photo», Metabunk.org, 1-9-2014 [https://www.metabunk.org/how-to-find-the-exact-upload-time-of-a-facebook-photo.t4367/; consultado el 6-1-2018].

Existen bastantes programas para extraer metadatos. En España uno de los más populares es FOCA (Fingerprinting Organizations with Collected Archives), desarrollado por Eleven Paths. Ofrece dos opciones gratuitas: operaciones básicas en línea (https://metashieldclean-up.elevenpaths.com) y más avanzadas descargando el programa (https://www.elevenpaths.com/es/labstools/foca-2).

En Metashield Clean-up, la primera opción, suba el archivo, pulse «Analizar» y acepte el acuerdo de uso. Se mostrarán los metadatos disponibles, por ejemplo fechas de guardado, autores de los documentos o cuentas de email asociadas. Si el servicio se usa con una imagen aparecerán detalles técnicos como apertura, Flash, distancia focal, número de serie de la cámara, modelo de teléfono, hora de captura y hora de edición. Ello puede servir para aclarar circunstancias y/o para hacer preguntas al presunto autor de la instantánea y determinar si fue él quien tomó la fotografía. Con la versión de descarga de FOCA se puede analizar un archivo, pero también obtener todos los documentos publicados en un dominio. En este caso se abre un nuevo proyecto («*New Project*»), se le da nombre, se indica el dominio que se quiere investigar y se pulsa «Crear». Aparecen los documentos, se descargan y se realiza la extracción de sus metadatos. Este videotutorial ayuda a entender el proceso (v=PK1ECI0gAV0). El programa también investiga contraseñas y servidores para pruebas de intrusión.

La mayoría de los sitios de metadatos dejan analizar el archivo a partir de la dirección url donde esté publicado o tomándolo del ordenador en el que se haya guardado. Siempre que sea posible se recomienda lo segundo (descargar y posteriormente subir el archivo para analizar). Además de FOCA, otros servicios recomendables son: Verexif (https://verexif.com), por estar en espa-

ñol e inglés y permitir detectar datos EXIF pero también borrarlos; Metapicz (https://www.metapicz.com); Exifdata (https://exifdata.com) y el clásico Jeffrey's Image Metadata Viewer (http://exif.regex.info/exif.cgi). Un último recurso es ImOps (https://imgops.com/), que ofrece atajos a opciones externas para el tratamiento y exploración de una instantánea. El tipo de información que ofrecen estos sitios puede ser distinta, conviene probar varios hasta dar con el más ajustado a las necesidades propias.

Las principales redes sociales **eliminan los metadatos** de los archivos. Google Plus es una de las pocas que los mantienen. En otros casos los propios autores borran pistas antes de publicar. Se recomienda al periodista que lo haga con sus archivos antes de compartirlos. Además de Verexif lo permiten PhotoMe (https://www.photome.de) y Metaclean (http://www.adarsus.com/MetaClean.html), estos últimos para instalar en local. En ocasiones ha salido a la luz la fuente de una filtración porque los metadatos del documento que se hizo llegar a la prensa o el rastreo del correo electrónico revelaban la autoría y cuenta de envío, como le ocurrió al equipo de una ministra española que gestionaba información laboral sensible.[3]

3. Pasos para verificar imágenes

Se recuerda la conveniencia de comprobar si se trabaja a partir del archivo original y de contactar con el autor. Incluso es aconsejable pedirle que facilite la imagen inmediatamente ante-

3. Casqueiro, Javier: «El pantallazo de la filtración Báñez», *El País*, 6-7-2012 [https://politica.elpais.com/politica/2012/07/05/actualidad/1341512968_310130.html; consultado el 5-1-2018]

rior e inmediatamente posterior de la misma cámara o teléfono móvil, para poder comparar metadatos. Y otro consejo básico: no se fíe nunca de una captura de pantalla (de un tuit, de una entrada de Facebook). Si se ofrece la imagen de un contenido en una red social, debe ir acompañada de un enlace a su fuente original para comprobar cosas como la hora.

Un buen apoyo para imágenes es la extensión FirstDraftNews-Check (accesible desde el repositorio de Chrome). Funciona como una suerte de nota recordatoria y guía al periodista sobre las comprobaciones que tiene que realizar para verificar material gráfico o audiovisual. Al final ofrece una valoración numérica según los pasos que se hayan dado: desde cero (ninguna comprobación realizada, nivel rojo) hasta cien (todas las comprobaciones realizadas, nivel verde, OK completo para publicar).[4] Siguiendo aproximadamente el orden pautado en esta guía, estos son los pasos para verificar una imagen.

1) Guardarla, sobre todo si el contenido es sensible o puede desaparecer.

2) Comprobar carácter original (QUÉ)

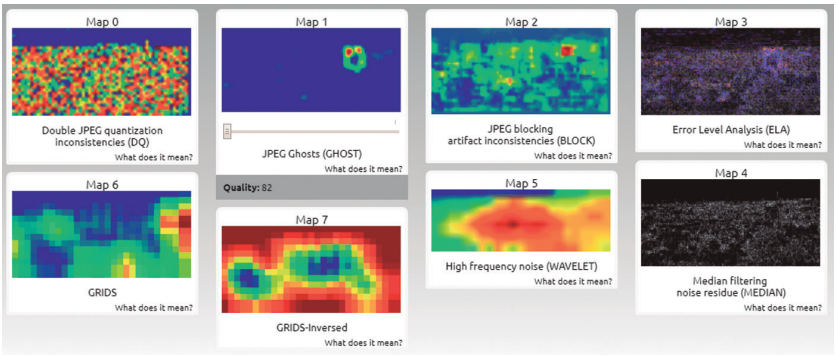
- Búsqueda inversa de imagen. Además de usar la extensión RevEye para rastrear desde los buscadores más habituales se puede recurrir a KarmaDecay (http://karmadecay.com), que investiga en Reddit, así como realizar una búsqueda textual describiendo lo mejor posible esa imagen para detectar otras parecidas.

4. Ambas guías (verificación de fotos y verificación de vídeos) pueden imprimirse: https://es.firstdraftnews.org/2017/08/11/descargue-nuestras-guias-para-verificar-fotos-y-videos/

- Búsqueda en redes sociales por identificador, palabras clave o descripción.
- Comprobación de fechas en redes sociales.
- Inspección de metadatos.
- Análisis técnico. Puede realizarse con el plug-in In Vid (http://www.invid-project.eu/tools-and-services/invid-verification-plugin/), actualmente el recurso gratuito más avanzado para el tratamiento de imágenes JPG o JPEG. Surge de un consorcio que impulsan Agence France Presse, Deutsche Welle y entidades educativas. Además de metadatos y búsquedas inversas, en la sección «Forensic» realiza ocho análisis que ayudan a detectar los engaños más habituales, como el clonado de elementos, la difuminación de contornos (frecuente en las zonas donde se juntan varias imágenes pegadas) o el cortado y pegado de figuras. Bajo cada análisis el enlace «What does it mean» ofrece los pormenores técnicos. InVid facilita un dictamen que debe completarse siempre con otras comprobaciones. Uno de los análisis que realiza es ELA (*Error Level Analysis*), también disponible desde Fotoforensics (https://fotoforensics.com). Esta técnica se centra en la detección de conjuntos de píxeles con compresión distinta del resto, lo que indicaría modificación. Basándose en ella, en 2013 se sospechó que el fotógrafo Paul Hansen había trucado una imagen ganadora del World Press Photo. Una comisión de investigación falló que la instantánea tenía notables retoques formales, pero ninguno prohibido en términos periodísticos (como el clonado).

Otro análisis rápido para imágenes en formato JPG es el que proporciona Izitru (https://www.izitru.com). Su valoración es

Figura 6. Los ocho análisis de una imagen que realiza inVid



Fuente: InVid.

aproximativa, pues basta con haber trasladado el archivo entre varios dispositivos o haberlo abierto con un programa de edición para que aparezca un dictamen dudoso (amarillo). Está disponible como aplicación para iPhone y su uso más útil se da precisamente cuando la fuente dice haber captado el material con su móvil y lo envía desde él al móvil del periodista.

3) Observar detenidamente (QUÉ)

- Preparación para examen detallado: giro, vista inversa, ampliación. Lo permiten diversos programas de edición, también ImgOps e InVid.
- Sombras y reflejos. Hay que averiguar si las sombras que se observan en la imagen son consistentes. Se traza una línea desde un punto cualquiera de un objeto hasta el equivalente en su sombra. Se repite la operación con varios puntos y objetos. Una vez proyectadas hacia el foco de luz principal que aparezca en la imagen, todas las líneas deberán converger en el mismo punto; si alguna se desvía puede haber habido desplazamientos artificiales.

Figura 7. Análisis de sombras

Fuente: FourandSix.com

El análisis de sombras se entiende mejor con los ejemplos que facilita la empresa FourandSix, gran experta en imagen forense (http://bit.ly/2IgtlBJ). Con relación al análisis de reflejos se sigue el mismo principio. Se traza una línea desde un punto cualquiera de un objeto hasta su equivalente en un espejo. Se repite la operación con otros objetos. Todas las líneas deben converger en un mismo punto. Si alguna se desvía revelará un desplazamiento artificial. (http://www.fourandsix.com/blog/2011/7/7/photo-forensics-from-reflections.html). Si bien el análisis de sombras y reflejos responde a principios físicos y por tanto supuestamente fiables, todo aficionado a la fotografía conoce los múltiples efectos engañosos que

la luz puede provocar. Se recuerda que ninguna herramienta es perfecta, que ningún análisis es determinante por sí solo.

- La luz. No es la misma en invierno o en verano (las sombras son más largas en el primer caso). Además, debe provocar el mismo efecto en todos los ojos. Si un rostro se corta y pega en una imagen, como suele hacerse para fingir que alguien famoso ha estado junto a un personaje o en un lugar indebido, es probable que sus ojos muestren reflejos distintos a los del resto de figuras.
- Movimientos. Atender a las partes del cuerpo donde se sitúan las articulaciones. En la foto viral de Obama tocando el trasero a Melania, la parte inversa del codo de él mostraba pliegues extraños (http://bzfd.it/2GfxIw0).
- Encuadre. A veces puede estar ofreciéndose solo una parte de la realidad. Así, aparece un soldado disparando a alguien, pero al ampliar se observa que hay público alrededor: es un espectáculo teatral. La proporción habitual de las imágenes es 4x3 (en los vídeos, 16:9). Si el archivo muestra otras dimensiones, quizá se haya hecho desaparecer intencionalmente una parte. En 2014, una primera imagen difundida del niño Marwan se hizo viral y muchos pensaron que el pequeño había atravesado solo el desierto hasta un campo de refugiados en Jordania. Una segunda imagen ampliada mostró que se encontraba dentro de un gran grupo (http://bit.ly/2HpHL1d y http://bit.ly/2Hnubvg).[5]

5. Fosset, Katelyn: «No, the Syrian refugee Marwan did not cross the desert alone», Foreignpolicy.com, 18-2-2014 [http://foreignpolicy.com/2014/02/18/no-the-syrian-refugee-marwan-did-not-cross-the-desert-alone/; consultado el 8-1-2018]

4) Investigar a la fuente (QUIÉN)

- Dando todos los pasos que se han explicado con anterioridad. La situación perfecta es la de haber hablado con ella.

5) Investigar el lugar (DÓNDE)

- Comprobar la localización en los datos EXIF en busca del punto exacto de toma (latitud y longitud).
- Detectar elementos significativos: paisaje, arquitectura (edificios destacados), vegetación, uniformes, cartelería, mobiliario urbano y señalización. Hay que dar prioridad a los objetos de carácter más permanente: una señal de tráfico frente al cartel de un concierto. ¿Se distingue el nombre de alguna calle en los edificios? ¿Hay palmeras en Euskadi? ¿A qué escuela pertenece el uniforme del colegial, a qué país el del soldado? Wikipedia ofrece los trajes militares más habituales por Ejército: http://bit.ly/2ovmgUU. Como lo mejor es practicar, este reto de observación de First Draft News pone a prueba la perspicacia: http://bit.ly/2FrEiiJ
- Buscar otras referencias, materiales sobre el mismo episodio o desde otro ángulo.
- Preguntar detalles geográficos al autor para ver si contradice los datos obtenidos.

6) Investigar el momento (CUÁNDO)

- Repasar datos EXIF
- Comprobar las fechas
- Analizar el clima (inclemencias, vestimenta, vegetación). Ha de concordar con el habitual en ese sitio en esa época del año y puede verse en Wolfram Alpha (https://www.wolframalpha.com/) o Weather Underground (https://www.wunderground). El primer recurso es el más conocido: en su caja de búsqueda,

teclear la ciudad y la fecha en inglés («London 15/10/2017»). Informará del tiempo que hizo ese día en ese lugar. Un ejemplo en el que el clima ha hecho sospechar de la autenticidad de una imagen: la fotografía que el depuesto presidente de la Generalitat, Carles Puigdemont, publicó en Instagram sugiriendo que estaba en Barcelona cuando había escapado a Bélgica (30 de octubre de 2017, http://bit.ly/2p4egdH). No había apenas nubes ese día y hora en la ciudad condal. Otro recurso es Suncalc (http://suncalc.net/), utilizado por muchos fotógrafos para calcular a qué hora encontrarán un sitio con la mejor luz. Moviendo su línea de desplazamiento sobre un punto geográfico, simula dónde se sitúa el sol a cada momento del día. Así se puede calcular si la imagen corresponde por su iluminación y sombras al lugar e instante que se le atribuyen.

4. Pasos para verificar vídeos

También en este caso InVid facilita muchas de las operaciones requeridas: zoom, revisión fotograma a fotograma, comprobación de fecha de subida, lectura de metadatos, capturas de pantalla para búsqueda inversa. Funciona con vídeos publicados en YouTube y Facebook.

Por lo demás, se ha de seguir la lógica de lo indicado para fotografías. Estos son los pasos recomendados:

1) Guardar

- Hay varias opciones para **descargar vídeos de Facebook**. La más sencilla consiste en hacer clic en la fecha del

material para obtener su url específica en la barra de navegación. Aquí se sustituye lo que queda antes de la palabra Facebook (https://www.facebook...) por «m» (https://m.facebook...) para pasar la interfaz a modo móvil. Se pone en marcha el vídeo y se pulsa sobre él botón derecho del ratón o equivalente en Mac. Ya estará disponible la opción «Guardar vídeo».

- Para descargar vídeos se recomiendan: a) Keepvid (https://keepvid.com) para YouTube; b) Deturl http://deturl.com), que sirve para YouTube, Vimeo y otras plataformas y además permite rotar, voltear y revertir el vídeo (siendo posible así leer letras que aparezcan en sentido contrario); y c) 4Kdownload (https://www.4kdownload.com), que requiere instalación pero es muy rápido y tiene una versión de pago con opciones muy atractivas (descarga de canales completos, por ejemplo).
- Video Vault (https://www.bravenewtech.org) es un servicio gratuito para registrar videos comprometedores vinculados con ataques a los derechos humanos. Se envía la url a su equipo, lo archivan y devuelven un enlace permanente.
- Hunch.ly (https://www.hunch.ly/) es de pago y para investigaciones avanzadas. Guarda las páginas web por las que ha pasado el verificador por si necesita justificar la ruta que ha seguido. Aquí hay varios videotutoriales (v=wA1ec0dPYhw).
- CameraV (https://guardianproject.info/apps/camerav/) y Eyewitness to Atrocities (http://www.eyewitnessproject.org) son dos aplicaciones para el móvil destinadas a proteger las imágenes o vídeos sensibles tomadas con el aparato. Las «esconden» en ese dispositivo por si alguna

persona lo intercepta (por ejemplo, antes de pasar una aduana en un país autoritario) y las envían a un servidor remoto. El segundo recurso es más intuitivo pero retiene muchos de los derechos de las imágenes, por lo que solo conviene utilizarlo en casos de peligro extremo.

2) Comprobar carácter original (QUÉ)

- Búsqueda en redes sociales por identificador o palabras clave.
- Búsqueda inversa de vídeo en YouTube Data Viewer o InVid.

3. Observar detenidamente (QUÉ)

- Visualización fotograma a fotograma. A veces es determinante para detectar un engaño, como en el viral del águila que captura a un niño (v=guoJUqc_Jtc). Puede hacerse en Anilyzer (http://anilyzer.com/) o Watchframebyframe (http://www.watchframebyframe.com/), para YouTube y Vimeo. En el ordenador propio puede verse el vídeo fotograma a fotograma con programas avanzados de edición o, al menos para verlo a cámara lenta, con el siguiente procedimiento (Windows Media): pulse sobre el archivo abierto con el botón derecho del ratón. Elija «Mejoras>Configuración de velocidad de reproducción>Lenta».
- Aplican las pautas de observación que se han ofrecido para fotografías y algunas más. El periodista puede detenerse en vestimenta, vegetación, mobiliario urbano, señalización, etc., pero también considerar cómo se mueven las personas que aparecen, así como en qué idioma y dialecto se expresan.

4. Investigar a la fuente (QUIÉN)

- Repetir las mismas preguntas que se hicieron en el caso de fotografías (perfiles en redes sociales, dominio de su sitio web, presencia en sitios corporativos...).

5. Investigar el lugar (DÓNDE)

- Además de las pautas ya mencionadas (edificios singulares, referencias cruzadas con otros vídeos, etc.) se dedicará el próximo capítulo a la geolocalización.

6. Investigar el momento (CUÁNDO)

- Datos EXIF, fechas en redes sociales, sombras, clima, vegetación.

El futuro de la verificación de imágenes y vídeos presenta incógnitas por la sofisticación en los engaños que trae consigo la inteligencia artificial. De hecho, hay quien asegura que la primera víctima de la misma podría ser la verdad. En el pasado la falsedad todavía podía reconocerse a cámara lenta. Sin embargo, será difícil para el ojo humano reconocer un algoritmo que convierte una escena de verano en una del invierno más total (v=9VC0c3pndbI), o distinguir que en un vídeo de Barak Obama en realidad el audio y el movimiento de la boca se han añadido posteriormente (v=9Yq67CjDqvw).

5. Mensajería instantánea y emisiones en directo

Los sistemas de mensajería instantánea suponen otro gran reto. Son origen de bulos que no se pueden comprobar porque surgen en grupos cerrados y se difunden muy rápidamente, especialmente en el caso de imágenes, vídeos o cadenas de engaño.

Algunas posibles actuaciones son las siguientes:

- Comentar esos contenidos en las redes sociales, preguntando a la comunidad si los ha recibido o tiene información sobre su procedencia.
- Apuntarse a grupos y foros sobre verificación o bulos en los que suelen ser detectados pronto.
- Tener en cuenta los hábitos locales por si se dan incongruencias en cuanto al origen atribuido al material. Por ejemplo, en Irán Telegram está más extendido que WhatsApp, y en China domina WeChat. Aquí hay datos orientativos referidos a Android: http://bit.ly/1Ylrf6M.

En España existen varios canales de Telegram sobre bulos (MalditoBulo, El Tragabulos). Puede conversarse sobre ellos en la comunidad de Maldita.es.

Las emisiones en directo o livestreaming desde sitios como Periscope (https://www.pscp.tv) o Facebook Live (https://www.facebook.com/live) también se están convirtiendo en fuente de noticias que abren informativos. En algunos casos generan grandes debates éticos, pues se han llegado a ver torturas, suicidios y asesinatos en directo. Fue muy impactante el caso de Philando Castile, disparado por un policía. Su pareja emitió los momentos inmediatamente posteriores a su muerte (v=VeVv9kJLAk4). También las cámaras colocadas en salpicaderos de coches o en el uniforme de personal de seguridad pueden ofrecer imágenes de impacto que hay que verificar.

En estas emisiones en directo el engaño es más fácil en el sentido de que se puede teatralizar una escena. Pero también hay vías que facilitan la verificación: existe la oportunidad de interactuar con el usuario-fuente original y con otros testigos que están realizando comentarios a esa emisión. Todos están en línea. Es fundamental guardar el material.

Capítulo IX
Dónde. Geolocalización

La geolocalización es una de las dimensiones de la verificación digital que está proporcionando ejercicios periodísticos más aclamados. Podríamos definirla como la investigación destinada a detectar la ubicación real de un elemento (sujeto u objeto) a partir de las pistas que deja en la red. Se observan detalladamente imágenes, vídeos y publicaciones en Internet y se van anotando emplazamientos que después se comprueban sobre un mapa (normalmente una imagen satelital).

A veces se ponen de manifiesto mentiras o contradicciones. Por ejemplo: El Kremlin negaba oficialmente que tuviese soldados desplegados en Ucrania, pero salieron a la luz selfis de rusos en este país, así como fotografías de medallas que se les habían concedido por su participación en el combate.[1] En el documental *Selfie soldiers. Russia checks in to Ukraine* (v=2zssIFN2mso), un reportero de Vice reproduce la trayectoria de uno de esos soldados por Ucrania a partir de las fotos que publica en la red rusa VKontakte (https://vk.com), similar a Facebook. Para geolocalizar hay que buscar material en las redes que son de mayor uso en el país investigado (se recuerda el mapa de Vincos).

1. Escalera, Javier: «Selfies de rusos con metralletas para mostrar que Putin juega sucio en Siria», Elconfidencial.com, 12-11-2015 [https://www.elconfidencial.com/mundo/2015-11-12/selfies-de-rusos-con-metralleta-para-mostrar-que-putin-juega-sucio-en-siria_1091096/; consultado el 4-1-2018]. Roderick, Paul: «Russian combat medals put lie to Putin's claim of no Russian troops in Ukraine», Forbes, 6-9-2016 [https://www.forbes.com/sites/paulroderickgregory/2016/09/06/russian-combat-medals-put-lie-to-putins-claim-of-no-russian-troops-in-ukraine/#68f96b4e3809; consultado 5-1-2018].

Bellingcat y DFRLab son las grandes referencias en materia de geolocalización. Otras entidades son los Digital Verification Corps de Amnistía Internacional (https://medium.com/@samdubberley) y la ONG Human Rights Watch (https://www.hrw.org), que la aplican a los derechos humanos. La iniciativa opositora rusa Conflict Intelligence Team (@CITeam_en) se enfrenta frecuentemente a El Kremlin con informaciones basadas en geolocalización de los conflictos bélicos en que interviene Rusia.

El webdoc en español de Yolanda Álvarez «Guerra a la mentira» (TVE, http://lab.rtve.es/webdocs/guerra-mentira) es un buen punto de partida para conocer el porqué de la gran atención actual hacia la geolocalización. La siguiente es una lista de trabajos representativos que han ido revistiéndola de credibilidad como vía para desmontar propaganda gubernamental, descubrir prácticas políticas poco edificantes o reconstruir relatos incompletos, aunque muchas veces con matices.

1. Casos prácticos

- Ataque químico en Guta (Siria). El 21 de agosto de 2013 aparecieron imágenes de adultos y niños sirios temblorosos y en estado de shock. Fuentes médicas aseguraron que se he había producido un ataque químico. Higgins recabó materiales testimoniales, comprobó su ubicación y su congruencia y atribuyó el ataque al Ejército de Bashar al Assad. Esto ocasionó una agria polémica con el mítico periodista Seymour Hersh, que mantenía otra versión. Hersh descubrió la masacre de My Lay cometida por Estados Unidos en Vietnam en 1969 y las torturas en la cárcel de Abu Ghraib (Irak) en 2004. Colisionaron

dos modos de entender el periodismo internacional: el clásico, donde muchas veces las exclusivas se basan en filtraciones de fuentes anónimas de alto rango, y el digital, en el que las afirmaciones se basan en pruebas que están a la vista en Internet.[2]

- Derribo del avión MH17 en Ucrania. El 17 de julio de 2014 un vuelo de Malaysia Airlines con dirección Países Bajos cae en la región oriental ucraniana de Donbass, dejando 298 fallecidos. La zona está en pleno conflicto: Rusia apoya de manera encubierta el levantamiento en este territorio que desea anexionarse y el gobierno de Ucrania procura evitarlo. Ambos se culpan mutuamente de haber derribado el avión. Bellingcat rastrea vídeos en redes sociales y detecta en ellos un misil tierra-aire BUK trasladado de Rusia a Ucrania que desaparece tras la caída del avión. Apunta que el aparato fue atacado con él desde posiciones prorusas. En 2017 la comisión oficial creada por Países Bajos para investigar el siniestro da eco internacional a estas investigaciones al corroborar sus principales conclusiones.[3]
- Localización de fosas comunes de ISIS. En septiembre de 2014 Human Rights Watch ofrece indicios de que este grupo terrorista, cuya crueldad solo se empieza a atisbar, ha llevado a cabo ejecuciones masivas. Primero recopila fotografías en las que se observa la detención y el traslado de grupos de hombres finalmente desaparecidos. Después muestra vía imagen satelital grandes montículos de tierra removida en las mismas zonas donde se han denunciado ejecuciones.[4]

2. Higgins, Eliot: «A History of sarín use in the Syrian conflict», Bellingcat, 6-9-2017 [https://www.bellingcat.com/news/mena/2017/09/06/history-sarin-use-syrian-conflict/].
3. Recopilación de artículos sobre el MH17 en Bellingcat: https://www.bellingcat.com/tag/mh17/.
4. «Iraq, ISIS execution site located», Hrw.org, 26-6-2014 [https://www.hrw.org/news/2014/06/26/iraq-isis-execution-site-located; consultado el 4-1-2018].

- El caso Aaron Schock. Hasta febrero de 2015 este joven congresista bien parecido y con mucho futuro político difundía en su cuenta de Instagram fotos de viajes y actividades deportivas extraordinarias. En un contexto altamente politizado, algunos medios comenzaron a investigarle y Associated Press geolocalizó las instantáneas. Descubrió que los emplazamientos mostraban coincidencias preocupantes con gastos cargados al partido, sobre todo en concepto de viajes. Schock dimitió.[5]
- Corrupción en Rusia. La hija de Dmitry Peskov, portavoz del presidente de Rusia, Vladimir Putin, publicó en Instagram selfis desde uno de los yates más caros del mundo. Aunque no pudo demostrarse que Peskov estuviese allí, la investigación dejó sospechas razonables de que el portavoz y su círculo más íntimo estaban viviendo por encima de sus posibilidades. Algunos pusieron en duda los descubrimientos porque fueron impulsados por el opositor a Putin Aleksey Navalny.[6]
- La situación de los rohinyás. A lo largo de 2017 empeoró el contexto para estos refugiados, rechazados por varios estados de Asia, especialmente Birmania. El gobierno insistía en que no se estaba empleando la violencia contra ellos, pero Amnistía Internacional y Human Rights Watch publicaron trabajos basados en imágenes satelitales que desmontaban esa afirmación. Numerosos enclaves rohinyás aparecían incendiados y la destrucción urbana era mayor de la reconocida.
- Ataque químico en Khan Sheikhoun. En abril de 2017, *The New York Times* analizó el ataque químico que sufrió esta localidad

5. Gillum, Jack y Braun, Stephen: «Lawmaker with lavish decor billed private planes, concerts», AP, 24-2-1015 [https://apnews.com/e2f1f52c3eb34caca7d74e5bf90f27f9/lawmaker-lavish-decor-billed-private-planes-concerts; consultada el 4-1-2018]
6. Toler, Aric: «Yachtspotting: OSINT methods in Navalny's corruption investigation», Bellingcat, 19-8-2015 [https://www.bellingcat.com/resources/case-studies/2015/08/19/yachtspotting/; consultado el 4-1-2018].

siria. Se basó en investigación digital forense y geolocalización de materiales publicados en la red, especialmente fotografías y vídeos. El resultado fue muy alabado, con la conclusión de que los gobiernos de Rusia y Siria habían falseado hechos para generar dudas sobre la autoría del ataque.[7]

- Juicio a Mahmoud al Werfalli. En septiembre de 2017 la Corte Internacional de Justicia emitió una orden de arresto contra este militar libio por crímenes de guerra. Por primera vez en la historia se basó para ello en vídeos subidos a las redes que mostraban sus presuntos asesinatos sumarios. Algunos de esos vídeos fueron geolocalizados por Bellingcat con ayuda de una campaña de colaboración pública (*crowdsourcing*). Los materiales han servido para procesarle y la curiosidad de muchos ahora es saber si servirán para condenarle.[8]

2. Google Maps y Google Earth

Google Maps (https://www.google.com/maps) y la versión de escritorio de Google Earth (https://earth.google.com/download-earth.html) son los principales recursos de geolocalización. La posibilidad de acceder desde ellos a una vista satelital y a una vista a pie de calle (*street view*) facilita la comprobación de emplazamientos.

7. Browne, Malachy; Reneau, Natalie; Scheffler, Mark: «How Syria and Russia spun a chemical strike», *The New York Times*, abril 2017. [https://www.nytimes.com/video/world/middleeast/100000005063944/syria-chemical-attack-russia.html; consultado el 3-1-2018]

8. Triebert, Christian: «Geolocatin Libya's social media executioner», Bellingcat, 4-9-2017 [https://www.bellingcat.com/news/mena/2017/09/04/geolocating-libyas-social-media-executioner/; consultado el 4-1-2018]

En Google Maps es importante:

- Dominar la **vista a pie de calle**. El muñeco amarillo que aparece en la esquina inferior derecha se arrastra con el ratón hasta el punto deseado para iniciar esta perspectiva. Permite situarse en el lugar exacto desde donde supuestamente se tomó una fotografía. La vista de calle solo está disponible en los tramos marcados con una línea azul; esta aparece al empezar el arrastre del muñeco.
- Saber **medir el tiempo de trayecto** entre dos puntos. Así se puede calcular lo que tarda un sujeto en ir de un lugar a otro y comprobar si dos fotografías pueden pertenecer al mismo autor o episodio. Por ejemplo, en un ataque terrorista que se sigue de segundos y terceros altercados distantes, empiezan a aparecer fotografías del supuesto atacante. ¿Ha tenido tiempo para ir de un lugar a otro? Pulsar sobre un punto inicial y con botón derecho del ratón (equivalente en Mac) elegir «Ruta desde aquí» (*directions from here*); pulsar punto de destino y elegir «Ruta hacia aquí» (*directions to here*). Se ofrecerán los trayectos a pie, en bicicleta, transporte público y coche. La distancia recta entre dos puntos se obtiene eligiendo la opción «Medir distancia» (*measure distance*) que aparece también haciendo clic en el botón derecho del ratón.
- Determinar la **latitud y longitud** de un punto para buscar más imágenes de la misma zona. Pueden conocerse en Itouchmap (https://itouchmap.com/latlong.html), pero también en Google Maps. Hay que colocarse sobre el lugar de interés y pulsar el botón derecho del ratón. Surgen varias opciones: eligiendo «Qué hay aquí», se muestran la latitud y longitud en un recuadro en la parte inferior y también en la url que aparece en la barra de navegación. A partir de estas coordenadas

pueden lanzarse búsquedas geográficas muy específicas en Twitter y Tweetdeck con el operador «geocode». Por ejemplo, la siguiente búsqueda establece que se encuentren tuits dentro de un radio de 0,5 km desde el Puente de Segovia de Madrid: [geocode:40.4139861,-3.72488,0.5km]. El primer número es la latitud, el segundo la longitud y en tercer lugar se indica el radio de búsqueda. Siempre hay que asegurarse de que no hay un espacio en blanco tras la coma que separa latitud de longitud, que aparece por defecto en Google Maps. Otro operador, aunque menos preciso que el de latitud y longitud, es «near». La cadena [explosión near:Rome within:4Km] ofrecería tuits relacionados con una explosión y emitidos a una distancia máxima de cuatro kilómetros de Roma.

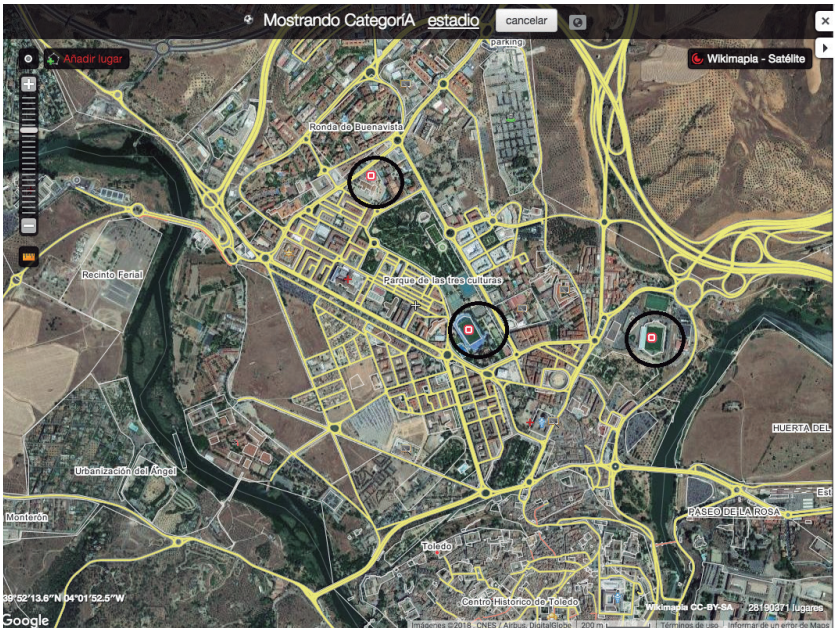
- Conocer el **deslizador de tiempo**. Está disponible en vista a pie de calle y aparece solo en algunos enclaves a modo de un pequeño reloj que gira en sentido inverso (esquina superior izquierda). Pulsando en él se aprecia el aspecto que tenía ese sitio en anteriores fotografías de Google Maps. Así, será posible contrastar si la imagen que le llega al periodista es actual o del pasado. Esta captura de pantalla de la Fontana di Trevi en Google Maps muestra el aspecto del deslizador: http://www.globograma.es/fontana/.

Los expertos en geolocalización trabajan sobre todo con Google Earth Pro, que debe descargarse en el ordenador. La última versión multilingüe ocupa bastante espacio y puede ralentizar algunas funciones, pero en algunos aspectos sigue siendo más avanzado que Google Maps. Por ejemplo, permite imprimir capturas de pantalla en alta resolución y cuenta con vista 3D, capa de fotografías y vista de relieve (*terrain*). Esta última es útil cuando se analizan emplazamientos sin apenas edificios o alejados de ciudades.

A estas posibilidades se accede desde la parte inferior del menú vertical izquierdo. First Draft News ofrece videotutoriales que permiten entenderlo mejor: cómo moverse por el mapa con el ratón (v=L93QjLUQpvM), cómo utilizar la vista de calle y el menú izquierdo (v=1zgg-muiMs8) y cómo aplicar esta herramienta a un caso real de verificación (v=Zvf0KUOACw).

Por último, Google Earth Pro también cuenta con su propio deslizador de tiempo o histórico de imágenes, así como con un simulador de luz solar, aunque no resulta tan operativo como SunCalc. Se accede a ellos desde el menú horizontal superior. En este enlace, una imagen ampliada lo muestra mejor: http://www.globograma.es/google-earth/.

Figura 8. Capa «Estadios» en la ciudad de Toledo en Wikimapia



Fuente: Wikimapia.org/Google

Hay otros recursos de geolocalización útiles. Se sugieren Wikimapia (http://wikimapia.org) y OpenStreetMap (https://www.openstreetmap.org/), ambos basados en la colaboración ciudadana. A partir de mapas de Google, Wikimapia permite buscar elementos específicos dentro de una ciudad. Por ejemplo, solo mezquitas, hospitales, escuelas, polideportivos o edificios militares. OpenStreetMap se basa en mapas alternativos a Google.

Según el interés geográfico, destacan otros servicios que conviene utilizar porque pueden facilitar imágenes distintas al proceder de otros proveedores o haber sido tomadas en otras fechas: Yandex (http://www.yandex.com/maps) para Rusia, este de Europa y Turquía; Baidu (https://map.baidu.com/) en el caso de China; Naver (https://map.naver.com/), recomendable en investigaciones sobre Corea del Sur. Para operar con ellos, lo mejor es recurrir al traductor de Google y buscar la localización que interesa en su idioma original. Un último servicio crecientemente utilizado, sobre todo en móvil, es HereWeGo (https://wego.here.com), de origen finlandés/alemán.

3. Información geolocalizada en redes

En los siguientes enlaces hay consejos para encontrar material procedente de emplazamientos concretos en distintas redes sociales. Es una operación que se ha convertido en básica para periodistas encargados del seguimiento de noticias de última hora.

- Cómo encontrar **tuits geolocalizados**. Lo más sencillo y preciso es utilizar el mencionado operador «geocode», que funciona en Tweetdeck y en Twitter. La búsqueda avanzada de esta red

social (https://www.twitter.com/search-advanced) ofrece además la opción «Cerca de este lugar», equivalente al operador «near». Hay otras dos herramientas aún experimentales que pueden probarse en línea para obtener visión de conjunto de los tuits que parten de una zona: una es Onemilliontweetmap (https://onemilliontweetmap.com/) y la otra MAPDTweetmap (https://www.mapd.com/demos/tweetmap/).

- Cómo encontrar **vídeos geolocalizados en Facebook Live Map**. Esta plataforma se ha convertido en una fuente imprescindible de información en noticias de alcance por la gran cantidad de vídeos que concentra de manera inmediata. Aunque no tiene caja de búsqueda para introducir palabra clave o lugar de interés, sí hay una vía indirecta para detectar grabaciones procedentes de una localización concreta. Se halla la latitud y longitud de ese lugar de interés en Google Maps. Se vuelve a Facebook Live Map, donde se abre cualquier emisión. En la url superior aparecerán la latitud y longitud del lugar del que proceda esa emisión; solo deben sustituirse por las del «lugar objetivo». Después puede jugarse con el zoom que aparece en la url: 10X es el máximo. Este videotutorial de First Draft News explica muy bien el procedimiento (v=clZSZiyZ0Y0). **Periscope**, el servicio de retransmisión de vídeos en vivo de Twitter, ofrece un zoom mucho más potente que Facebook Live Map, pero no está disponible en versión escritorio sino solo en el móvil y además presenta muchos menos videos, lo que le resta opciones.
- Cómo encontrar **material geolocalizado en Instagram**. Esta red sí permite buscar por etiqueta asociada a cualquier suceso y también por localización. Solo hay que introducir el lugar de interés en la caja de búsqueda y aparecerán los post relacionados con ese emplazamiento. (v=VfLnwKibJfM).

- Cómo encontrar vídeos geolocalizados en YouTube. Esta plataforma no contiene opciones de geolocalización, pero el recurso externo GeoSearchTool sí (https://youtube.github.io/geo-search-tool/search.html), y dispone de una búsqueda avanzada muy sencilla de utilizar. Videotutorial de su uso (v=OAfb8q5XFR4).

En todas las redes anteriores, pero sobre todo en Facebook Live Map, Periscope e Instagram, dada la pronta desaparición de los materiales conviene dominar las opciones de guardado.

4. Limitaciones de la geolocalización

Solo un porcentaje ínfimo de los contenidos que aparecen en redes sociales están geolocalizados automáticamente (es decir, han sido publicados con la opción «geolocalización» activada). Por este motivo, muchas herramientas que dicen geolocalizar lo hacen detectando el lugar que indica el usuario en su perfil, además de ese pequeño porcentaje automático. Pero esta «bio» no es indicador seguro porque cada vez más personas utilizan ese campo para introducir otros datos o porque el usuario puede haberse mudado, estar viajando o haber decidido mentir.

Es muy sencillo fingir la ubicación desde un teléfono inteligente y existen programas de escritorio que simulan una interfaz móvil y también lo permiten de manera simple, como Bluestacks (https://www.bluestacks.com). Todo ello significa que las impresiones de ubicación que se obtienen con las indicaciones de las redes sociales deben ser consolidadas con más técnicas y procedimientos de geolocalización y verificación digital. El ejemplo a seguir son

los amplios trabajos de comprobación y contraste que realizan expertos como los de Bellingcat.

Además de los vistos aquí hay otros muchos recursos para un desempeño profesional en este ámbito tanto en su web (https://www.bellingcat.com/tag/geolocation/) como en la de First Draft News (https://firstdraftnews.com/?s=geolocation). La habilidad para ubicar emplazamientos también puede entrenarse con el juego Geoguessr (https://geoguessr.com/) o participando en los ejercicios breves que los especialistas proponen a menudo en Twitter con etiquetas como #digitalsherlocks o #verificationtraining.

La cuenta @quiztime ofrece un breve ejercicio de geolocalización diario.

Capítulo X
Por qué. Sesgos y motivación

En el punto de arranque de una mentira puede estar el «buen samaritano» que retuitea sin saberlo un aviso inexacto de emergencia, pero también el régimen autoritario que planifica el **descrédito de un disidente** a través del llamado «troleo patriótico». En medio puede haber alguien que simplemente disfruta poniendo en evidencia la falta de comprobación en los medios, como Tommaso Debenedetti, conocido por ello.

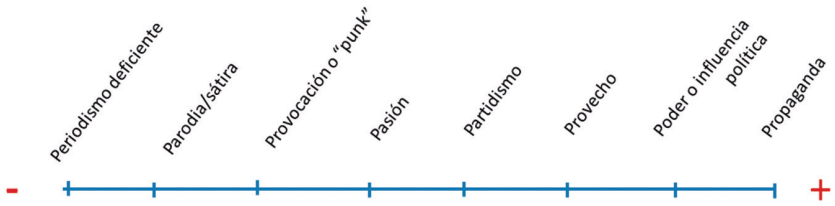
Claire Wardle ha analizado los tipos de información de baja calidad en línea y sus motivaciones.[1] Hay una distinción esencial y se basa en la intencionalidad. En inglés existen los términos *misinformation y disinformation*. El primero equivaldría a **información errónea** (insuficiente, parcialmente omitida, etc.) y el segundo, que es para el que se suele reservar el término español «desinformación», implicaría cierto propósito manipulador: se busca dañar algo o a alguien y con este objetivo se distorsionan algunos aspectos. Los bulos pasarán de ser errores a falsedades (o mejor aún, falacias) si contienen como ingrediente esa meta de perjudicar, beneficiando a la inversa al autor.

Esta **cinta métrica de la mentira** es una adaptación de las ocho «letras P» que Eliot Higgins y Claire Wardle han identificado como palancas para la información errónea o la desinformación. No es una clasificación rígida, pues a veces una sátira

1. Wardle, Claire: «Fake news. It's complicated», Firstdraftnews.com, 14-3-2017 [https://es.firstdraftnews.org/2017/03/14/noticias-falsas-es-complicado/; consultado el 4-1-2018]

puede tener consecuencias nefastas y un error inocente convertirse en falacia, pero en general hacia la derecha se sitúan los casos más graves con peso social y político. «Periodismo deficiente» incluye la información incorrecta que un usuario ofrece y los medios convierten en noticia. Por ejemplo, publicar que el futbolista Ronaldo abandonó su Lamborghini en la sierra de Madrid cuando solo se trataba de un vehículo similar. En «Provecho» se situarían las falsedades con fines lucrativos.

Figura 9. Cinta métrica de las mentiras



Fuente: Elaboración propia a partir de Claire Wardle y Eliot Higgins

Este capítulo trasciende las técnicas de verificación digital y se pregunta por algunos aspectos de la psicología humana y sus motivaciones, así como por la forma en que estas pueden deducirse a partir de los contenidos a disposición del periodista. La razón es que en las clases con estudiantes de Periodismo se ha observado que estos aprenden rápidamente las herramientas de comprobación en Internet, pero fallan más a la hora de detectar la **manipulación ideológica o política** que muchas veces está tras las corrientes digitales. Hay un flanco de la investigación en el que más que conocer recursos informáticos lo que se requiere es capacidad de reflexión.

1. Anonimato

Ya se ha mencionado la relevancia de las fuentes para el periodismo. Cuando son anónimas se están ocultando sus motivaciones y por tanto una importante información. Ahora que la relación entre política y desinformación ha cobrado tanta relevancia, cualquier pista sobre las intenciones de quien aporta los datos es de ayuda.

El **anonimato es imprescindible** en zonas donde la fuente corre peligro, así como para garantizar la libertad de expresión y la independencia de los poderes que gobiernan. También lo es en investigaciones en materia de seguridad o inteligencia donde quien habla se juega el puesto de trabajo. Estados Unidos emprendió bajo el gobierno de Barack Obama una guerra explícita contra los llamados *whistleblowers* o filtradores, pero hay que recordar la influencia positiva que uno solo de ellos tuvo décadas antes para la historia del periodismo a través del caso Watergate.

En los últimos años el anonimato y el *off the record* se han extendido sin justificación en el periodismo político, incluso entre cabeceras de referencia. Margaret Sullivan (@sulliview), antigua defensora del lector en *The New York Times* y actualmente en *The Washington Post*, es conocida por recalcar su peligrosidad. El periodista Mark Schaver mantuvo entre 2010 y 2013 un rastreador de fuentes anónimas en los medios (http://bit.ly/2CO9ydG). Deja la sensación de que para entonces el fenómeno ya era una plaga.

Es peligroso que sean fuentes anónimas las que sostienen un titular. Se explica en el hilo de Twitter que surgió cuando el periodista e historiador Yoni Appelbaum se preguntó de dónde venía una información catastrofista sobre Corea del Norte: «Comprueba siempre las fuentes», fue su conclusión.[2]

2. Hilo de Yoni Appelbaum: (https://twitter.com/YAppelbaum/status/847166432806944768).

Nunca el anonimato es tan relevante como en una gran filtración al estilo de las que han pespunteado la escena política internacional desde la aparición de Wikileaks (2006). Cuando estas filtraciones se producen en procesos electorales, no preocuparse por el origen de los datos es una imprudencia. Durante la campaña electoral de Estados Unidos en 2016 aparecieron correos electrónicos del Comité Nacional Demócrata y del colaborador de Hillary Clinton John Podesta que fueron muy comentados en los medios y las redes (#DNCleak, #podestaemails). De esos correos electrónicos surgió uno de los bulos más simbólicos de los últimos años: Pizzagate. Los mensajes de los demócratas fueron distorsionados hasta acusarse al equipo Clinton de estar implicado en una red de pederastia con sede en el restaurante Pizza Comet Ping Pong. El bulo llevó incluso a un ciudadano a presentarse en el local con una escopeta para combatir a los supuestos pederastas y tiene una extraordinaria fuerza de permanencia en el imaginario colectivo. Para desgracia del restaurante, todavía muchas personas piensan que la historia es real. Con esta experiencia previa, en los últimos días de las elecciones francesas de 2017 se produjo un ciberataque y el robo de un gran conjunto de emails del entorno del candidato presidencial Emmanuel Macron (#macronleaks). La prensa decidió no hacerse eco de ellos hasta que hubiera resultados electorales.

2. Descripciones de fuentes veladas

En ocasiones el autor de los comentarios es descrito de forma **velada**, con pinceladas gruesas. Hay que examinarlas a fondo para obtener pistas sobre su campo de acción. La lectura entre

líneas de un artículo periodístico con el fin de detectar las fuentes que hay tras él es todo un arte.[3] Como muestra, un breve análisis realizado por el periodista Benjamin Wittes sobre lo mucho que puede extraerse de expresiones aparentemente planas como «declinó comentar» o «no hay comentarios»:

> Algunos periódicos tienen la norma de no afirmar que el Sr. Fulanito declinó comentar cuando de hecho el Sr. Fulanito sí que ha comentado, aunque sea *off the record*. No todos los periódicos mantienen tal política, así que esta es una norma débil. Pero siempre merece la pena preguntarse quién NO es mencionado en una noticia rechazando comentarla, especialmente si dicha persona es nombrada en el relato o es protagonista del mismo.
>
> A la inversa, los «no hay comentarios» institucionales enfáticos no significan que el personal de esas instituciones no haya sido la fuente. Además, el lenguaje específico de las citas de «sin comentarios» a menudo puede ser revelador. Alguien diciendo que no sería apropiado para él comentar no significa que no haya cometido ese acto inapropiado. Que el periódico reporte que una persona de hecho no comentó es muy distinto a que reporte que declinó ser citado. Y ambas situaciones son distintas a que el periódico reporte que una persona no ha devuelto las llamadas o no pudo ser localizada. En otras palabras, presta atención exactamente

3. Lecturas sobre fuentes anónimas y veladas en Washington, pero cuyas enseñanzas son de aplicación internacional: Bacon, Perry: «When to trust a story that uses unnamed sources», Fivethirtyeight.com, 18-7-2018 [https://fivethirtyeight.com/features/when-to-trust-a-story-that-uses-unnamed-sources/; consultado el 4-1-2018] y «Which anonymous sources are worth paying attention to?», Fivethirtyeight.com, 19-7-2018 [https://fivethirtyeight.com/features/which-anonymous-sources-are-worth-paying-attention-to/; consultado el 4-2-1018]. Wittes, Benjamin: «How to read a news story about an investigation: eight tips on who is saying what», Lawfare, 4-9-2017 [https://lawfareblog.com/how-read-news-story-about-investigation-eight-tips-who-saying-what]. Webb, Rick: «How to read the news to reduce fake news consumption», Medium.com, 2-2-2017 [https://medium.com/@RickWebb/how-to-read-the-news-to-reduce-fake-news-consumption-3ab91cc73677; consultado el 4-1-2018].

a lo que el periódico está diciendo sobre el «sin comentarios» de una persona o entidad.[4]

La tabla 1 aglutina consejos para protegerse lo mejor posible de los riesgos de fuentes anónimas y veladas. En verificación digital, el propósito de dedicarle tanto esfuerzo a ello siempre será reducir el consumo de falsedades y su expansión en línea. A la izquierda se mencionan aspectos que pueden hacer valorar positivamente a una fuente aunque no se dé su nombre. A la derecha se ofrecen expresiones periodísticas frecuentes sobre el anonimato.

3. Medios y polarización

El anonimato y las filtraciones también sirven para alimentar una agenda creciente de **polarización política** que se ha extendido a los medios. La interpretación de la actualidad varía mucho de unos a otros y algunas cabeceras pueden incluso obviar noticias o filtraciones de alcance mundial si consideran que son perjudiciales para sus intereses. Por eso es importante conocer su orientación.

El Digital News Report 2017 ofrece un mapa de audiencias que refleja la ideología de los usuarios de los principales medios en los distintos países de la Unión Europea. Se basa en encuestas a los propios usuarios. Es un modo indirecto, quizá menos discutido, de definir a un medio políticamente. En España los lectores de *Público* son los que aparecen más a la izquierda y los del periódico *ABC* más a la derecha. Aunque algunas cabeceras destacaron que era un ejercicio simplista, el mapa ayuda a los estudiantes a orientarse en

4. Wittes, Benjamin: *op. cit.*

Tabla 1. Indagar en fuentes anónimas/veladas

La fuente se explicita	«El portavoz del secretario general ha confirmado»
Se cita a más de una fuente	«3 expertos» «2 jueces»
Las fuentes son diversas	«Fuentes de los dos partidos políticos»
Hay cierta precisión dentro del anonimato	«2 asesores del Ministerio de Educación» «Altos cargos del Ministerio de Exteriores»
Las fuentes se mueven en un entorno con libertad de expresión	«Fuentes del Gobierno de Finlandia» frente a «Fuentes del Partido Comunista chino»
Las fuentes se expresan de manera clara, no especulan	«La fuente dice que el ministro ha solicitado una penalización»
Las fuentes hablan de hechos, no califican características o rasgos de otra persona o grupo (especialmente si esos rasgos son negativos)	«La fuente afirma que la oposición se ausentó ayer de la reunión» frente a «La fuente afirma que la oposición se está comportando de manera irresponsable»
Las fuentes hablan de algo que pasó, no que pasará o podría pasar	«La fuente dice que el ministro ha presentado su dimisión» frente a «La fuente dice que el ministro podría presentar su dimisión mañana»
Los testimonios se apoyan con documentos	«La carta, a la que ha tenido acceso este medio, corrobora esa decisión»
Se conoce/confía en el periodista, lo que hace que expresiones que en otro momento serían rechazadas por ambigüedad se acepten por estar en la órbita de las que suele emplear	«Fuentes del Ministerio», «Fuentes familiarizadas con el caso» o «cercanas a la familia», «Fuentes conocedoras de los planes del acusado»
Se conoce el medio, su situación y tendencias y el contenido es original, propio	«Según las comprobaciones realizadas por este medio» frente a «Según los datos aportados por varias cabeceras locales»
No hay desmentidos	«Este medio se ha puesto en contacto con el Ministerio, que no ha desmentido los datos»

países cuya prensa desconocen.[5] Wikipedia también puede ser de utilidad. En sus entradas sobre medios a menudo ofrece apuntes espontáneos sobre su tendencia ideológica, y remite a artículos y casos que suponen ejemplos, un riesgo que directorios más formales no suelen correr.

En el entorno nacional se conoce «de qué pie cojea» cada medio, pero en el internacional no, y el lector tiende a ser más crédulo con lo que se le cuenta. Del mismo modo, cuando se consultan medios digitales, su mayor frescura hace pensar que son independientes. Si se suman las dos circunstancias se obtiene que cuando se consultan medios digitales extranjeros la pérdida de conciencia sobre inclinación política es casi total, como demuestran algunas prácticas de clase.

Un estudiante puede considerar que una noticia muy hostil con los refugiados es fiable porque la difunde un periódico extranjero de gran tirada; no ha considerado que pueda ser uno de los diarios más sensacionalistas de toda Europa. **Hay que realizar las mismas preguntas** sea cual sea la marca que presenta la noticia: ¿cómo es el medio que distribuye esta información?, ¿cuáles son sus preferencias ideológicas?, ¿qué interés puede tener para que esto se conozca?

No existe directorio universal de medios según su calidad o ideología. Sería altamente discutido y discutible. Pero algunas entidades sí se han atrevido a ofrecer a sus lectores servicios en los que identifican medios/sitios que frecuentan la falsedad. Un ejemplo es Décodex, de *Le Monde* (http://www.lemonde.fr/verification/), una suite de recursos de verificación que incluye un buscador. Si se encuentra una noticia de un sitio web que no se

5. Reuters Institute for the Study of Journalism (2017). *Digital News Report 2017*, Oxford University [https://reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital%20News%20Report%202017%20web_0.pdf; consultado el 4-1-2018].

conoce, se introduce la dirección en él y el sistema detectará si forma parte de su lista de sospechosos. Décodex tiene registrados unas mil webs y perfiles sociales. Se ha popularizado por el prestigio del medio y de su equipo de *fact-checking*, Les Décodeurs.

4. Malas prácticas digitales

La profesora Melissa Zimdars elaboró en 2016 un directorio de medios/sitios sospechosos con etiquetas para clasificar sus prácticas digitales perjudiciales. El listado se hizo viral y fue muy debatido, pero las etiquetas funcionan para identificar los principales envoltorios que presentan actualmente la información errónea y la desinformación. Con el orden modificado para que sigan una línea paralela a la cinta métrica de las mentiras antes propuesta, esas etiquetas serían: *clickbait*, rumores, noticias basura, sátira, noticias políticas, sesgo extremo, noticias falsas, teorías de la conspiración, discurso del odio y propaganda estatal.

A esas malas prácticas Zimdars añadió las etiquetas «proceder con cautela», «creíble» y «desconocido»: sitios que generen dudas, sitios que en general difundan información aceptable y casos en los que por algún motivo no se ha valorado al medio. Conocer estas etiquetas ayuda a detectar tales prácticas cuando se encuentran en línea.[6]

1. *Clickbait*: se ofrecen titulares exagerados o que no corresponden con lo que hay en el interior, aunque lo que haya sea verdadero.

6. Zimdars, Melissa: «False, misleading, clickbait and/or satirical news sources», Docs.google.com [http://bit.ly/2fsQjcH]

2. Rumor: se mueven cotilleos y hechos todavía no verificados.

3. Noticia basura o pseudociencia: medicamentos milagrosos, descubrimientos espectaculares, avances no demostrados, etc.

4. Sátira: se usa el humor, la ironía, la exageración o el ridículo para comentar la actualidad.

5. Noticias políticas: el medio suele dar información verificable pero en apoyo a una orientación política específica.

6. Sesgo extremo: se mantiene un punto de vista muy definido y se apoya con información descontextualizada y opiniones disfrazadas de hechos.

7. Noticia falsa: las fuentes fabrican por completo la información, diseminan contenido engañoso o distorsionan de manera burda una noticia (por sus implicaciones, la definición de esta modalidad se verá al detalle más adelante).

8. Teorías de la conspiración: se promueven leyendas urbanas o virales falsos, como los de autorías ocultas del 11-S, la tierra como objeto plano, etc.

9. Discurso del odio: se promueve el racismo, la misoginia o cualquier otra forma de discriminación.

10. Propaganda estatal: se difunde información desde un estado autoritario y por tanto no libremente.

11. Requiere cautela: el contenido puede ser verídico pero obliga a ulterior comprobación y contraste con otras fuentes.

12. Creíble: se emite información en consistencia con las prácticas éticas reconocidas en la profesión periodística.

13. Desconocido: El medio no ha podido ser evaluado.

5. Fiabilidad

Los campos académicos de la Documentación y la Comunicación han aportado mucha bibliografía de calidad para evaluar la fiabilidad de fuentes digitales. Si el lector no conoce ninguna propuesta se sugiere seguir un cuestionario (tabla 2). Es de aplicación ágil en periodismo, aunque proceda del ámbito OSINT, donde se aplica a las investigaciones con la intención de evitar que la subjetividad impida calificar objetivamente una información.[7]

El nivel A1 es el más óptimo. Indica que la fuente es completamente fiable y la información cuenta con garantías. Los niveles E5 y F6 son los menos deseables.

6. Posverdad y noticias falsas

La empresa que edita los diccionarios Oxford convirtió **posverdad** en palabra del año en 2017. Hace referencia a aquellas circunstancias en que «los hechos son menos influyentes sobre la opinión pública que las emociones o las creencias personales». Pese a lo lejos que ha llegado el concepto, un periodista que investiga en red no cae en la **trampa del relativismo** ni da la verdad por perdida de entrada, al igual que un inspector de policía no emprende la investigación de un delito pensando que no hallará al autor porque «todo depende». Los hechos tienen más importancia que las opiniones. A partir de ellos es esencial ofrecer al ciudadano la mejor verdad posible.

7. US Department of Justice: *Law enforcement intelligence. A guide for state, local and tribal law enforcement agencies, US Department of Justice*, 2009 [https://it.ojp.gov/documents/d/e050919201-IntelGuide_web.pdf; consultado el 4-1-2018]

Tabla 2. Evaluación de fiabilidad

Fuentes		Información	
A. Completamente fiable	– No hay duda de autenticidad – La fuente es competente – La historia es creíble	1. Confirmado	– Confirmado por otra fuente independiente – Lógico por sí mismo – En línea con otra información disponible sobre el asunto
B. Usualmente fiable	– Alguna duda sobre la veracidad y autenticidad – Alguna duda sobre la competencia – La mayoría de las veces es una fuente fiable	2. Probablemente cierto	– No confirmado – Lógico por sí mismo – En línea con otra información disponible sobre el asunto
C. Bastante fiable	– Dudas habituales de veracidad y autenticidad – Dudas habituales sobre la competencia – A veces resulta ser una fuente fiable	3. Posiblemente cierto	– No confirmado – Razonablemente lógico por sí mismo – De alguna manera en línea con otra información disponible sobre el asunto
D. Usualmente no fiable	– Dudas concisas sobre la veracidad y autenticidad – Dudas concisas sobre la competencia – Antecedentes ocasionales de fiabilidad	4. Dudosamente cierto	– No confirmado – No ilógico por sí mismo – Considerado increíble a primera vista, pero posible
E. No fiable	– Grandes dudas sobre la veracidad y autenticidad – Grandes dudas sobre la competencia – Antecedentes de información no fiable	5. Improbable	– Lo contrario está confirmado – Es ilógico por sí mismo – Contradice otra información
F. Sin valoración posible	No hay suficiente información para juzgar	6. Sin valoración posible	No hay suficiente información para juzgar

Uno de los motivos que los votantes de Trump esgrimieron para apoyarle es que habían dejado de creer a los grandes medios que denunciaban sus mentiras porque vivían en una **burbuja eli-**

tista y liberal. La pérdida de confianza en los *legacy media* es uno de los grandes quebraderos de cabeza de sus directivos, sobre todo por la tendencia creciente entre los ciudadanos de considerar que ahora las redes sociales ya pueden funcionar como fuente informativa.[8] Estas circunstancias y otras rodearon la victoria del político republicano pero una destacó por su carácter novedoso: la proliferación digital de noticias falsas de apoyo a su candidatura. Entre las más extendidas: que el Papa Francisco apoyaba al multimillonario en la carrera por la presidencia.

Un artículo impactante de Craig Silverman mostró que en Facebook **las noticias falsas** habían generado más **interacción** (*engagement*) que las publicadas por los grandes medios sobre la campaña.[9] En su formato original, podían ser definidas como «informaciones que mienten en todo o en parte, que se publican en sitios donde se imita el aspecto de medios respetados, que suelen recurrir a titulares impactantes o engañosos para captar lectores, que están planificadas para una máxima difusión e interacción con la ayuda de tácticas de automatización, y que tienen dos propósitos principales y a veces combinados: a) obtener clics y generar dinero con la publicidad, o b) impulsar determinadas ideas, propuestas o candidaturas, a veces denigrando las contrarias».

8. Este artículo analiza la «burbuja liberal» que llevó a que la prensa subestimase las opciones de Trump. Silver, Nate: «There really was a liberal media bubble», Fivethirtyeight.com, 10-3-2017 [https://fivethirtyeight.com/features/there-really-was-a-liberal-media-bubble/]. Este otro destaca los cambios en fuentes de información en EEUU: Gottfried, Jeffrey y Shearer, Elisa: «News use across social platforms», Pew Center, 26-5-2016 [http://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016/; consultado el 4-1-2016]

9. Silverman, Craig: «This analysis shows how viral fake election news stories outperformed real news on Facebook», Buzzfeed, 16-11-2016 [https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook; consultado en 4-1-2018].

Dos recursos pueden ser de ayuda para la detección de estos engaños. A partir de un término, el buscador Hoaxy (https://hoaxy.iuni.iu.edu) detecta noticias relacionadas en sitios sospechosos. Pulsando en cada una de ellas se muestra una visualización con las cuentas principales que las han impulsado en Twitter. FightHoax (http://fighthoax.com) utiliza la inteligencia artificial (*machine learning*) para analizar patrones lingüísticos en noticias y detectar si pertenecen a bulos. De momento la herramienta solo se puede probar previa petición a sus responsables.

La expresión «noticias falsas» ha llegado desvirtuada a 2018, siendo utilizada por muchos políticos para denigrar informaciones disidentes. Es habitual que Trump llame a algunos medios «*fake news*», como hizo con la CNN en su primera rueda de prensa tras la victoria. Por eso los expertos recomiendan olvidar esas dos palabras y concretar de qué tipo de información errónea o desinformación se habla en cada caso.

7. Algoritmos y burbujas

Lo que impulsó la ola de noticias falsas fue en primer lugar la decisión interesada de difundirlas, pero también el propio funcionamiento de las redes sociales, que mostraban los contenidos con más tirón basándose en los dictados de algoritmos. Estos son cálculos matemáticos que ejecutan una acción u otra en función de las instrucciones que hayan recibido para afrontar cada problema. Los de Facebook estaban planteados para ofrecer a cada persona aquello que le hiciese pasar más tiempo en la plataforma. Si una noticia sensacionalista o de mal gusto entretenía al usuario los algoritmos mostraban más del mismo tipo. El resultado es una mayor exposición

a noticias cuyo principal mérito no es ser de calidad sino ser llamativas. Las noticias falsas de corte político encajaban bien en ese paisaje.

Los algoritmos perniciosos no sólo se dan en Facebook. Algunos análisis han probado que YouTube también promociona automáticamente contenidos indeseables dentro de supuestos canales para niños.[10]

Como los usuarios tienden cada vez más a compartir un contenido si confían en la persona que lo comparte,[11] se desarrollan **burbujas digitales de pensamiento**. El internauta lee una actualidad básicamente conformada por cosas que le gustan a él y a su círculo. El periodista hará bien en ser consciente de esos algoritmos y burbujas que pueden afectar cualquier punto de vista ajeno y también analizar los que le envuelven a él mismo, porque refuerzan sus **puntos de vista personales** de partida. El llamado «sesgo de confirmación» hace que recordemos y demos más validez a la información que confirma nuestras propias creencias. Para evitarlo es recomendable seguir en redes sociales también a personas con las que se esté en desacuerdo.

Algunas publicaciones han lanzado iniciativas para romper la espiral de desinformación. En Blue Feed, Red Feed el conservador *The Wall Street Journal* ofrece dos hilos con la interpretación republicana y demócrata de asuntos informativos sensibles. El diario progresista *The Guardian* destaca en su espacio «Explota tu burbuja» artículos conservadores de calidad (https://www.theguardian.com/us-news/series/burst-your-bubble y http://graphics.wsj.com/blue-feed-red-feed/).

10. BBC Trending: «The disturbing YouTube videos that are tricking children», BBC, 27-3-2007 [http://www.bbc.com/news/blogs-trending-39381889; visitado el 4-1-2018]

11. La confianza en la fuente pesa más que la credibilidad del medio. American Press Institute: *Who shared it?: How Americans decide what news to trust on social media*, Americanpressinstitute.com, 20-3-2017 [https://www.americanpressinstitute.org/publications/reports/survey-research/trust-social-media/; consultado el 4-1-2017]

Capítulo XI

Cómo. *Bots* y análisis de redes

Los *bots* son relevantes para entender cómo se expande una información falsa en línea y cómo se organizan campañas encubiertas. La propaganda existe hace siglos, pero la tecnología la ha llevado a una nueva dimensión, especialmente en su vertiente política y estatal. Se ha empezado a hablar de **propaganda automatizada**, definida por *The Computational Propaganda Project* (COMPROP, http://comprop.oii.ox.ac.uk) como «el uso de algoritmos, automatización y filtración/gestión humana para distribuir información engañosa a propósito en las redes sociales».[1]

En una campaña automatizada suelen combinarse *bots*, perfiles falsos, noticias falsas e inserciones publicitarias divisivas, todo diseñado para aprovechar el funcionamiento de algoritmos que potenciarán esa corriente inducida. Como las noticias falsas y los algoritmos ya se analizaron, este capítulo se centra en los otros elementos.

1. *Bots*, perfiles falsos, cíborgs y otros

Los *bots* existen en Twitter desde el año 2006 y en 2010 ya aparecían en las elecciones de Estados Unidos. En el contexto

1. Filtración/gestión aparece en el texto original como «*curation*». Woolley, Samuel C y Howard, Philip N. (2017). *Computational Propaganda Worldwide*. Oxford Internet Institute, pág. 3 https://www.oii.ox.ac.uk/blog/computational-propaganda-worldwide-executive-summary.

político son cuentas robóticas programadas para amplificar artificialmente mensajes o tendencias. Pueden darse en cualquier red social, aunque son más frecuentes en Facebook y sobre todo en Twitter, donde se estima que entre un 9 y un 15% de las cuentas son *bots*.[2] Una sola persona puede administrar un gran conjunto de ellos, dándoles la orden para actuar. Impiden debates reales sobre las cosas, generan ruido e infoxican. Se emplean en pseudocampañas, corrientes falsas que simulan que algo o alguien cuenta con un apoyo generalizado cuando no es así. En inglés a esas campañas se las llama astroturfing por la marca de césped artificial del mismo nombre y por su relación con el término *grassroot* (de raíz o de base), el que se usa para describir iniciativas en las que el apoyo popular sí es real.

Hay que puntualizar que los *bots* **no son elementos negativos** *per se*. En esencia son solo tareas informáticas programadas que permiten comodidades como recibir un boletín o conversar vía mensajería instantánea con el lector, como hace la iniciativa española Politibot (https://politibot.io). El problema es que han empezado a usarse masivamente para difundir publicidad o mensajes basura (*spam*) y, en su vertiente política, se vinculan con la propaganda gris (la fuente no se identifica) y negra (se finge que la fuente es otra). En estas ocasiones se está manipulando a una opinión pública que desconoce quién está tras la iniciativa y no sabe que esta es planificada.

El grupo que conforma Bots de Twitter (http://botsdetwitter.wordpress.com, @botspoliticosno) denuncia el uso político de los *bots* en España y se mantiene en el anonimato para no ser acusado de sesgo. Facilita en su página mucha información

2. Varol, Onur; Ferrara, Emilio et alt: Online-human bot interactions: detection, estimation, and characterization, ICWSM 2017, Marzo 2017 [https://arxiv.org/abs/1703.03107; consultado el 15-1-2018]

sobre los *bots*.[3] Estos son los rasgos típicos de este tipo de cuentas:

- Carácter permanente y sistemático.
- Mimetismo o imitación de expresiones humanas (pero son cuentas automáticas).
- «Me gusta», publicación de entradas, compartido o retuiteo masivo de mensajes para generar tendencias en las redes sociales o distorsionar los resultados de un término en los buscadores.
- Coordinación con campañas paralelas en distintas redes sociales.
- Estrategia vertical (las cuentas asociadas emiten el mismo mensaje en idéntico momento), horizontal (hacen que gotee a lo largo del tiempo), o mixto.
- Posible funcionamiento zombi de las cuentas, que se mantienen en letargo durante largos periodos hasta que reciben la orden de lanzar unánimemente la campaña.
- Preferencia por ahondar en debates polémicos o cuestiones divisivas (inmigración, religión); alineamiento con bulos, leyendas urbanas y teorías de la conspiración.
- Secuestro de *hashtags* o etiquetas ajenas mediante el lanzamiento masivo de mensajes que las usan; el objetivo es difundir spam propio o anular una protesta cívica o política emergente; paralelamente pueden lanzarse otras etiquetas alternativas que difundan el pensamiento propio.

3. Bots de Twitter: «Perfiles falsos de Twitter. Un reto para 2015», Botsdetwitter.com [https://botsdetwitter.wordpress.com/2015/03/01/perfiles-falsos-en-twitter-un-reto-para-2015/; 1-3-2015; consultado el 4-1-2018]

Los *bots* más básicos se identifican fácilmente por la ausencia de foto y descripción en el perfil. Un ejemplo son los de corte independentista detectados sobre Cataluña por el corresponsal de EFE en Bruselas, Javier Albisu (http://bit.ly/2CHnyRL). Para disimular, los autores los combinan cada vez más con **perfiles falsos o ficticios** tras los que sí hay un humano que participa en la conversación, interviniendo incluso como distintos personajes gracias a la gestión multicuenta que permiten servicios como Tweedeck o Hootsuite. Una misma cuenta puede funcionar intermitentemente como bot (automatizada) y como perfil falso (humano). Son los llamados **perfiles mixtos** o **perfiles cíborg**.

Muchos asocian los perfiles falsos o ficticios con los trols, que molestan o violentan desde el anonimato, y con los odiadores o haters, que acosan digitalmente a sus víctimas. Sin embargo, los perfiles falsos tienden a comportarse cada vez más con amabilidad. Interactúan con personajes relevantes que terminan siguiéndoles, ganan seguidores y se convierten incluso en referencia para la prensa. Cuando ya son influyentes empiezan a extremar su mensaje, a tuitear sobre asuntos divisivos o a difundir grandes mentiras. Entonces sus comentarios tienen todos los puntos para hacerse virales. A los perfiles falsos manejados por gobiernos o grupos políticos se les suele dar el nombre de *sockpuppet accounts* o **cuentas títere**.

El caso de Jenna Abrams (@Jenn_Abrams) es paradigmático de los perfiles falsos. Durante años fue citada por grandes medios de Estados Unidos. Primero hablaba de moda o famosas como Kim Kardashian. Cuando ya era conocida empezó a expresar opiniones polémicas. @SouthLoneStar es otro ejemplo claro. Viralizó la mentira de que una musulmana que caminaba y hablaba por el móvil junto a víctimas de un atentado en Londres no había mostrado empatía por las mismas. En octubre de 2017

Twitter identificó ambos perfiles como dos de las 2.752 cuentas con las que se infoxicó desde Rusia en las elecciones de Estados Unidos (después la cifra ascendería a más de 50.000).

Otro caso conocido: en 2014 un usuario llamado Carlos (@spainbuca) se hizo pasar por controlador aéreo español en un aeropuerto de Ucrania, ganando la confianza de corresponsales en la zona y de periodistas que seguían la información del lugar (incluida esta autora). Llegó a ser entrevistado incluso por la cadena RT, aunque con el rostro oculto. Cuando un avión MH17 fue derribado sobre Ucrania, difundió una versión alterada que culpaba a militares ucranianos de la operación. La embajada española desmintió la existencia de este controlador, que canceló su cuenta. Posteriormente el perfil reapareció como Lyudmila. Vladimir Putin llegó a citar a @spainbuca como fuente real en una conversación con el cineasta Oliver Stone, pese a llevar tiempo desacreditado.[4]

Un último caso importante de perfil falso es el de aquella cuenta que **usurpa la identidad** de otra persona, participando en redes como si fuera ella. De todas las opciones mencionadas es la única ilegal en sí misma, ya que los *bots* y los perfiles falsos no lo son, aunque varios gobiernos planean actuar contra ellos. En el caso de los haters, la actividad es delictiva cuando constituye amenaza o acoso o cuando atenta contra derechos como el del honor. Sin embargo, sus «crímenes» casi nunca son perseguidos.

La labor de *bots*, perfiles falsos y cíborgs en pseudocampañas se combina con **cuentas corporativas** o de partido que emiten propaganda abiertamente, así como con la ayuda de **usuarios fuente**, perfiles influyentes que pueden ser reales (tertulianos o

4. Zhdanova, Mariia y Orlova, Dariya: *Computational propaganda un Ukraine: caught between external threats and internal challenges*, OIIO, working paper n. 2017.9, Londres, septiembre de 2017 [http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-Ukraine.pdf; consultado el 8-1-2018

youtubbers conocidos, por ejemplo) u ocultar cuentas de partido. Ambos generan buena parte del contenido que retuitea la red falsa y que se combina con otra información intrascendente para disimular.[5]

Además, en las campañas automatizadas puede haber contratación de anuncios en redes sociales. Se aprovecha la segmentación y personalización que pemiten plataformas como Facebook para dirigir el mensaje a un grupo con características concretas en el que se sabe que el argumento puede arraigar. A veces estos anuncios ni siquiera apoyan a un candidato, sino que pretenden confundir y generar desconfianza en todo y en todos. Los anuncios rusos que Facebook reconoció haber encontrado durante la campaña estadounidense seguían esa línea: eran realmente extraños y provocaban desconcierto.

2. Cómo detectar un bot o perfil falso

Los *bots* más elementales de Twitter solo replican mensajes, no contestan a las preguntas o comentarios y tienen listas llenas de usuarios ajenos a su supuesta especialización o que a su vez son *bots*. Pero hay otros más cuidados: muestran fotos de personas reales, miman la descripción de su biografía, incluyen enlace a una página web y vigilan la composición de sus listas. El investigador puede encontrar desde la automatización más burda a un uso mixto o cíborg muy sofisticado. Muchos de los consejos del apartado «Quién» pueden seguirse para comprobar la «realidad»

5. Bots de Twitter: «Las trampas éticas del Partido Popular en Twitter», 29-7-2015 [https://botsdetwitter.wordpress.com/2015/07/; consultado el 8-1-2018]

tras una cuenta. Henk van Ess propone **10 pasos** para evaluar si se está ante un bot o perfil ficticio. Se ha alterado ligeramente su enunciado y orden para culminar con el análisis de redes, al que se dedicará atención especial.[6]

1) Investigar **cuándo se abrió la cuenta**. Puede hacerse desde la búsqueda de Twitter o en recursos como Foller.me.

2) Analizar su **primer tuit**. Twitter eliminó ese servicio, pero las primeras palabras de un tuitero aún pueden conocerse. Primero se averigua cuándo abrió la cuenta el usuario y luego se seleccionan los tuits de esa fecha en la sección de búsqueda avanzada.

3) Analizar **los seguidores.** En TwitterAudit (https://www.twitteraudit.com) se ve el porcentaje de seguidores reales y falsos que tiene una cuenta. Un análisis más detallado de sus rasgos y preferencias es posible con Twopcharts, Followthehashtag o Followerwonk. ¿Sobre qué tuitean? ¿Con quién se relacionan? ¿Dónde residen? Las cuentas falsas suelen tener seguidores repartidos equitativamente por todo el mundo, mientras las reales concentran la mayoría de seguidores en su propio país.

4) Buscar a ese tuitero en Facebook por su alias o por un correo electrónico que se crea pueda tener. Si también muestra actividad automatizada es otro motivo para dudar: sucesión de entradas sin comentarios, imágenes con muchas personas etiquetadas, ubicación en países donde esa red no es muy popular, pertenencia a grupos sospechosos, etc.

6. Van Ess, Henk: «The ultimate guide to bust fake tweeters: a video toolkit in 10 steps», Poynter.org, 4-10-2017 [https://www.poynter.org/news/ultimate-guide-bust-fake-tweeters-video-toolkit-10-steps: consultado el 8-1-2018]

5) Investigar posibles **cuentas en otras redes sociales**. Puede recurrirse a Inteltechniques, sección User Names.

6) Buscar **palabras concretas representativas** entre los contenidos del usuario. Por ejemplo, partidos políticos o términos xenófobos o vinculados a teorías de la conspiración. Esto puede hacerse desde la búsqueda avanzada de Twitter o con Tweetbeaver (http://tweetbeaver.com, apartado *Search within a user timeline*). Este recurso además permite descargar los datos para un análisis detallado en Excel.

7) Consultar su **posicionamiento en rankings**. Por ejemplo, escribiendo http://klout.com más el alias del usuario. Como se ha explicado, los rankings deben ser consultados con cierto escepticismo. Jenna Abrams era probablemente considerada una persona influyente en muchos de ellos.

8) ¿Es una **cuenta apagada o activa**? Sus interacciones se pueden comprobar en Socialmention (http://www.socialmention.com). También en Twopcharts, Followthehashtag y Followerwonk.

9) Comprobar **cuándo tuitea**. Sus **patrones de actividad/sueño** deben ser coincidentes con los de un humano, con prudencia pues esto también se puede trucar programando los tuits. Para comprobar estos patrones: Foller.me, Twopcharts o Account Analysis (https://accountanalysis.lucahammer.com/).

10) *Big data* o análisis de grandes cantidades de datos (mediante análisis de redes).

El recurso **Botometer** (https://botometer.iuni.iu.edu) puede ser útil. Diseñado por el conocido Observatorio de Medios Sociales de la Universidad de Indiana (**OSoMe**), orienta en la detección de cuentas automatizadas o de spam. Al introducir un alias explica si el perfil, sus seguidores o sus contactos son sospechosos. Analiza aspectos como el sentimiento asociado a

los tuis (enfado, amabilidad) o su distribución temporal. Una propuesta en la misma línea es Botcheck.me (http://botcheck.me). Aseguran acertar con el diagnóstico más de un 90% de las veces.

3. Análisis de redes

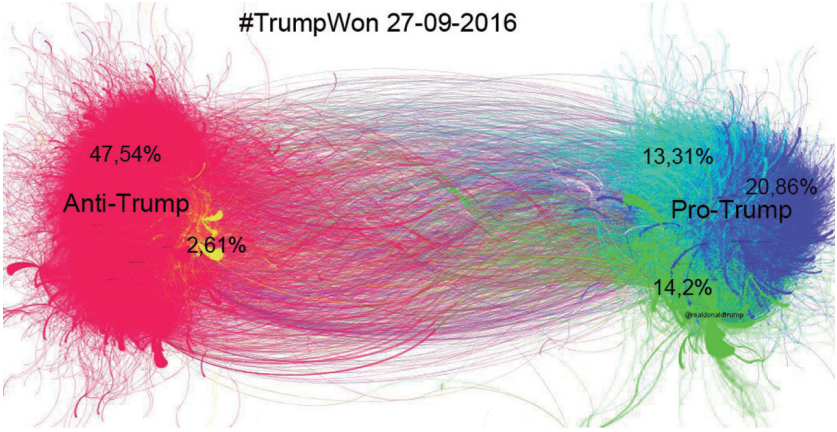
El análisis de redes es una metodología científica que permite examinar las relaciones entre usuarios a partir de los datos de su actividad en lugares como Twitter. Se pueden observar aspectos como si están conectados entre sí, qué interacciones desarrollan (retuits, menciones o comentarios) o qué lugar ocupan dentro de su comunidad (si son figuras centrales o secundarias). El cálculo y representación de esa información es complejo y requiere una abstracción matemática llamada grafo.

Un grafo es un conjunto de nodos o vértices vinculados a través de aristas. Se suelen representar como diagramas de puntos o círculos conectados por líneas en forma de red. Los analistas tienden a modelar los nodos como individuos y las aristas como sus relaciones. Los nodos más vinculados se atraen, los menos se repelen haciendo aflorar «estructuras de afinidad», como explica en sus clases Mariluz Congosto (@congosto), investigadora de referencia en esta materia.

Un ejemplo sirve para entenderlo. En septiembre de 2016 se convirtió en tendencia la etiqueta #TrumpWon, que aseguraba que Trump había vencido en un debate electoral contra Clinton. Se empezó a sospechar que se trataba de una campaña impulsada desde Rusia. Congosto examinó los primeros cinco mil mensajes con la etiqueta y concluyó que había sido impulsada principalmen-

te desde Estados Unidos al ser usada tanto por partidarios de Trump como por detractores que la criticaban. Solo días después *The Washington Post* publicó un estudio similar. No habían sido los rusos.[7]

Figura 10. Usuarios impulsando la etiqueta #Trumpwon



Fuente: M.ª Luz Congosto, Barriblog.

El análisis de redes vertebra artículos periodísticos muy interesantes referidos a todo tipo de sectores. El blog de Congosto, Barriblog (https://www.barriblog.com), es una buena opción para conocer ejemplos, así como la cuenta de Victoriano Izquierdo, @victorianoi, de la empresa Graphext, y el sitio del especialista Esteban Moro (@estebanmoro, http://estebanmoro.org). Otra posibilidad para los curiosos es buscar en Google imágenes sobre «social network analysis examples».

7. Congosto, Mariluz: «Desmontando el origen ruso del hashtag #TrumpWon», Barriblog.com, 30-9-2016 [http://www.barriblog.com/2016/09/desmontando-origen-ruso-del-hashtag-trumpwon/; consultado el 4-1-2018]. Lotan, Gilad: «No, Russians did not start the #TrumpWon debate meme. Here's what really happened», *The Washington Post*, 3-10-2016 [https://www.washingtonpost.com/news/monkey-cage/wp/2016/10/03/no-russians-did-not-start-the-trumpwon-debate-meme-heres-what-really-happened; consultado el 4-1-2018]

Con estas exploraciones la respuesta a la pregunta «por qué», así como la caracterización de usuarios y validación de fuentes, es más precisa. ¿Es esa tendencia espontánea? ¿Es autóctona o está alentada desde el extranjero? ¿Los usuarios presentan rasgos de *bots*? Las etiquetas #Taksim y #Gezi que surgieron contra el gobierno de Turquía en 2013 fueron impulsadas desde el interior del país por tuiteros que ni siquiera eran a priori influyentes pero que lograron extenderlas. En otros casos la visualización muestra corrientes promovidas simultáneamente por *bots* que las expanden «geométricamente» y no con rasgos orgánicos, irregulares, naturales.

En el análisis de redes hay tres fases: a) recopilación de datos: por ejemplo, bajarse el conjunto de tuits; b) graficado o conversión de esos datos a un modo visual más comprensible que una tabla; c) análisis. Graphika (https://www.graphika.com) hace las dos primeras cosas, pero es de pago. Aquí hay un videotutorial de su funcionamiento en inglés (v=yqwWYLDplp0).

Dentro de los recursos gratuitos para generar ficheros de datos se destacan:

- Sencillos aunque de capacidad muy limitada. SocioViz (http://socioviz.net), que en su versión gratuita ofrece el análisis de un máximo de cien tuits de los siete últimos días. Netvizz (https://apps.facebook.com/netvizz), aplicación para obtener datos de grupos y seguidores de páginas en Facebook. Ambos se utilizan online.
- Más complejos pero mucho más completos. Requieren instalación, pero en ellos se puede hablar de verdadero análisis de redes por la cantidad de tuits capaces de gestionar: T-Hoarder (https://github.com/congosto/t-hoarder/wiki, de Congosto; Tinfoleak (http://www.vicenteaguileradiaz.com/tools/), de

Vicente Aguilera, en su versión avanzada de descarga; y por último DMI-tcat (https://github.com/digitalmethodsinitiative/dmi-tcat), de Erik Borra y Bernard Rieder.

Los datos obtenidos con estas aplicaciones pueden llevarse a Gephi (https://gephi.org/). Este paquete de software gratuito que requiere instalación se ha hecho popular por su facilidad de uso, dentro de la complejidad que tiene esta materia.[8] Para dar unos primeros pasos con él se recomiendan dos ejercicios disponibles en la página web del profesor José Luis Molina. La curva de aprendizaje es compleja al inicio, pero después se allana y ofrece muchos beneficios:

- Ejercicio con SocioViz y Gephi.[9]
- Práctica de redes sociales con Netvizz y Gephi.[10]

4. Fábricas de trols y desinformación

La cuenta @Jenn_Abrams se creó desde Internet Research Agency (IRA), una «fábrica de trols» o «granja de trols». Son lugares donde se contrata a gente para difundir bulos o trolear a personas según lo pautado en argumentarios específicos. Buzzfeed fue el primer medio en hablar de IRA en 2014 tras una filtración, pero la popularizó Adrian Chen (*The New*

8. CARTO (https://github.com/CartoDB/cartodb) es otro software semigratuito bastante utilizado, especialmente en investigaciones orientadas a detectar patrones geográficos.
9. Molina, José Luis: «Obtener una matriz de datos de Twitter para Gephi con Socioviz» [http://bit.ly/2yoNwrm]
10. Patraca, Beatriz: «Práctica de redes sociales con Gephi» [http://bit.ly/2FxJd0G]

York Times) con el artículo «The Agency» (2015).[11] El reportero hablaba con personas que habían trabajado en la compañía, como después harían periodistas como Xavier Colas: «No puedo decir con certeza qué era mentira y qué no», le dice uno de aquellos trols al español.[12]

Los *bots* y las fábricas de trols recibieron atención extraordinaria tras el triunfo de Trump. Junto a las noticias falsas, comenzó a investigarse si habían funcionado como parte de una campaña de connivencia entre el equipo del millonario y el gobierno ruso para que el primero llegara a La Casa Blanca. Se mezclaron seis aspectos que generaron una tormenta política perfecta:

- La propaganda detectada a través de *bots* y perfiles falsos.
- La sistematicidad en los mensajes que emitían estas cuentas, que ya no eran solo frases repetitivas sino noticias falsas planificadas.
- Los ciberataques para el robo de material sensible que luego se distorsionaba y difundía con ayuda de los *bots* (como ocurrió con los emails del equipo demócrata).
- La posible implicación en esa gran operación de «enemigos públicos» como Julian Assange, de Wikileaks.
- La inserción de anuncios que ahondaban en la sensación de descontrol.
- Los contactos reales entre personal del equipo de Trump y agentes rusos.

11. Chen, Adrian: «The agency», *The New York Times*, 2-6-2015 [https://www.nytimes.com/2015/06/07/magazine/the-agency.html; consultado el 4-1-2018]
12. Colas, Xavier: «La fábrica rusa de las mentiras (y no es broma, Cospedal)», El Mundo, 16-11-2017 [http://www.elmundo.es/cronica/2017/11/26/5a19c2f122601dfd678b45c4.html]

Aunque eran frecuentes en los países del este, en Europa occidental las campañas automatizadas se habían dado a pequeña escala y empezaron a preocupar solo a partir del referéndum para el Brexit (junio de 2016) y las elecciones de Francia y Alemania (mayo y septiembre de 2017, respectivamente). En España era frecuente que recurrieran a ellos partidos de todo el arco político, según Bots de Twitter. Por ejemplo, se halló una nebulosa que promocionaba a La Razón, el PP y la Familia Real, y hubo *bots* en las primarias del PSOE que enfrentaron a Pedro Sánchez y Susana Díaz. La atención hacia el fenómeno se disparó tras la celebración del referéndum catalán, detectándose entonces un impulso digital inusual a este asunto por parte de cuentas y medios rusos. El servicio EUvsDisinfo (https://euvsdisinfo.eu/), vinculado a la East Stratcom Task Force, una unidad contra la desinformación en el este de Europa creada por el Consejo Europeo, detectó gruesas noticias falsas sobre Cataluña. La Alianza para Asegurar la Democracia, entidad estadounidense, habló de un 2.000% de aumento de las menciones relacionadas con la cuestión entre cuentas favorables a El Kremlin el día previo al referéndum (aunque la metodología de estudio de esta asociación fue puesta en tela de juicio más tarde).

La suma de todos estos casos ha llevado a una preocupación extrema por cómo el mal uso de las redes sociales puede afectar a la democracia. Twitter, Facebook y Google han tenido que ofrecer explicaciones en el Congreso de Estados Unidos. Twitter y YouTube han limitado la publicidad y visibilidad de los medios rusos RT y Sputnik, señalados como «usuarios fuente». Europa y Estados Unidos se activan para protegerse mejor contra las amenazas digitales de todo tipo, incluidos los ciberataques.

Hay una tendencia a la securitización del discurso (abordar el problema principalmente desde la seguridad), y entre las medidas

que se anuncian se mezclan las que tienen que ver con control de la infoxicación (*bots*, perfiles falsos, bulos) y con la ciberguerra (robo de datos, inutilización de equipos informáticos). Todo ello forma parte de los nuevos modos de **guerra híbrida** o guerra asimétrica donde el dominio del campo informativo importa tanto como el del campo militar, pero tratar ambas dimensiones como conjunto inseparable puede conducir a errores y/o medidas censoras excesivas.

Sin querer minimizar la dimensión digital como forma de conflicto entre estados, que existe desde hace años y que debe ser conocida y gestionada por las autoridades, se recomienda seguir algunas pautas para no ser paradójicamente manipulado en temas de manipulación. La desinformación, y en particular la impulsada por grandes potencias, es un problema real, pero el miedo social o paranoia excesiva también. En los artículos que versen sobre pseudocampañas, en particular las atribuidas a gobiernos extranjeros concretos, es conveniente prestar atención a aspectos como: a) el **lenguaje** que dramatiza u oculta falta de pruebas mediante expresiones genéricas («los *bots* han podido afectar»; b) las **informaciones circulares**, en las que parece que los datos están corroborados porque los mencionan muchas fuentes, pero en realidad se citan unas a otras; c) la falta de método científico en los análisis; y d) la generalización: se habla de fábricas de trols rusas, en plural, pero se ha podido probar solo la actuación sistemática, maligna y políticamente inducida de una, IRA.[13] Como se ha visto, atribuir origen geográfico a las pseudocampañas puede ser difícil y más aún atribuir autoría intelectual y orquestación. El gobierno español denunció maniobras digitales rusas sobre el

13. Graham, David A.: «What Mueller's indictment reveals», Theatlantic.com, 16-2-2016 [https://www.theatlantic.com/politics/archive/2018/02/mueller-roadmap/553604/; visitado el 8-1-2018]

1-O y posteriormente hubo de aclarar que no tenía pruebas de injerencia directa de El Kremlin. Hay más pistas para evitar la «desinformación sobre la desinformación» en el artículo «Desde Rusia con *bots*» de Agenda Pública.[14]

Los efectos de estos fenómenos y sus cifras también deben ser considerados con rigor. Algún estudio revela por ejemplo el poder de Facebook para influir de modo real en la toma de decisiones electorales, pero hacen falta aún más análisis para determinar el impacto de las pseudocampañas y noticias falsas en la mente de los receptores y en su voto final. Al igual que la Teoría de la Aguja Hipodérmica fue desestimada hace años en su versión más ortodoxa (ahora se sabe que a la hora de tomar decisiones los ciudadanos se ven influenciados por diversas fuentes además de los medios), las redes son solo uno de los múltiples puntos de contacto que una persona puede tener con la actualidad. Su opinión se forma a partir de muchos focos.

Con respecto a los números las cifras son impactantes, en particular sobre Rusia. COMPROP hablaba en 2017 de notable automatización en este país (afectando al 45% de la actividad en Twitter).[15] No es el único afectado. Ya en 2015 había cuarenta estados con actividad de *bots* políticos, incluidas democracias como Estados Unidos, Reino Unido, Australia, Argentina o México, donde hay acusaciones frecuentes contra los llamados Peñabots, favorables al presidente Enrique Peña Nieto.[16] Servicios de inte-

14. Redondo, Myriam: «Desde Rusia con *bots*», Agenda Pública, 11-11-2017 [http://agendapublica.elperiodico.com/desde-rusia-bots/; consultado 4-1-2018]
15. Woolley, Samuel C.; Howard, Philip N.: *op. cit.*, pág. 4.
16. En México, la referencia en materia de *bots* es el activista Alberto Escorcia (@LoQueSigue_). Redondo, Myriam: *Política automatizada. Bots, trols y propaganda digital encubierta*, ACOP, Madrid, 2015 [http://www.globograma.es/propaganda-automatizada-bots-trols-y-desinformacion-internacional/; consultado el 4-1-208].

ligencia de los países más avanzados frecuentan las pseudocampañas hace tiempo. Estados Unidos puso en marcha una en 2011 para crear perfiles ficticios que impulsaran propaganda a su favor en Oriente Medio.[17] El uso más apabullante de la desinformación se da en China, donde según la estimación más fiable conocida el gobierno promueve cada año la publicación de unos 448 millones de comentarios «guiados» en redes sociales.

Es sin duda un problema, un reto, un desafío, pero el peso de estos números debe ponerse siempre en contexto. Cuando en enero de 2018 Twitter aumentó a 50.258 el número de cuentas problemáticas rusas detectadas, aclaró que representaban solo un 0,016% de todas las abiertas en su plataforma. La primera cifra suele pasar a los titulares; la segunda difícilmente se abre paso en los medios.[18]

En realidad, la desinformación global que se ha gestado en Internet no depende tanto de gobiernos oscuros como de grupos en los extremos del polarizado espectro ideológico actual. Estos pueden llegar a converger en temas comunes porque comparten un propósito, la desestabilización. En enero-febrero de 2017 se hizo viral un vídeo en el que un supuesto inmigrante golpeaba a una enfermera. En Francia lo difundió la extrema derecha criticando la cobertura sanitaria universal para extranjeros. En Turquía lo promovieron algunos críticos laicos del presidente Recep Tayyip Erdogan diciendo que estaba llenando el país de musulmanes para tener más votos. En realidad no era ni lo uno ni lo otro. Se trataba de un borracho ruso golpeando a una enfermera en un hospital del este de Rusia. Estos radicales de todo signo

17. Fielding, Nick y Cobain, Ian: «Revealed: US spy operation that manipulates social media», *The Guardian*, 17-3-2011 [https://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks; consultado el 4-1-2018]
18. Twitter Public Policy: «Update on Twitter's review of teh 2016 U.S. election», 19-1-2018 [https://blog.twitter.com/official/en_us/topics/company/2018/2016-election-update.html; consultado el 20-1-2018]

hackean la atención de medios y ciudadanos con memes y virales atractivos que triunfan en un mercado sensacionalista. Entre ellos destaca la gran movilización de los partidarios de la extrema derecha, el supremacismo blanco y las teorías de la conspiración. En realidad, pueden compartir tácticas digitales con los activistas por los derechos humanos, pero las usan para poner en solfa sus creencias y su supuesta «corrección política».[19]

Hay bulos frecuentes contra los refugiados y una naturalización de los discursos de odio (contra determinadas religiones, contra las mujeres, contra los pobres –aporofobia–). También los intereses económicos tras el impulso a las llamadas noticias falsas son universales: estas se generan en lugares tan dispares como Macedonia y Estados Unidos. En definitiva, la información errónea y la desinformación están demasiado extendidas como para inscribirlas únicamente en un enfrentamiento de nueva Guerra Fría. Son cuestiones que debieran vincularse sobre todo a la necesidad de mayor alfabetización política, mediática y digital entre la ciudadanía, que debiera disponer siempre de conocimientos y recursos de verificación.

19. El vídeo del falso musulmán también llegó a España: *El País*: «La verdad detrás del bulo sobre la agresión de un musulmán en un centro médico», Elpais.com, 28-3-2017 [https://elpais.com/elpais/2017/03/27/hechos/1490618106_370724.html]. Sobre el impulso de la extrema derecha y otros grupos a la desinformación en Internet puede leerse: Marwick, Alice y Lewis, Rebecca: Media manipulation and disinformation online, Data&Society, 2017 [https://datasociety.net/output/media-manipulation-and-disinfo-online/].

Capítulo XII
Recursos y lecturas

Este capítulo presenta un listado de sitios web, expertos y lecturas destacadas para mantenerse actualizado en verificación digital. Seguro que hay más direcciones que añadir. Si se le ocurre alguna, contacte en redes con la autora.

1. Sitios web

1.1. En inglés/francés

FirstDraftNews.com (https://www.firstdraftnews.com), coalición internacional de referencia en verificación digital y lucha contra la desinformación | Bellingcat (https://bellingcat.com), expertos en geolocalización y verificación en conflictos bélicos | Storyful (https://storyful.com), pioneros en verificación digital; DFRLab (https://medium.com/dfrlab), laboratorio de The Atlantic Council activo en geolocalización y conflictos bélicos | Snopes (https://www.snopes.com), sitio decano en detección de bulos y leyendas urbanas (desde 1994) | The Computational Propaganda Project (COMPROP, http://comprop.oii.ox.ac.uk), dependiente de la Universidad de Oxford (OII), es uno de los centros más avanzados en el estudio de propaganda automatizada | OSoMe (https://osome.iuni.iu.edu), referente sobre difusión de información falsa en redes sociales y en detección de *bots* | Meedan (https://meedan.com),

verificación internacional y recursos para superar barreras idiomáticas; Eyewitness Media Hub (https://www.eyewitnessmediahub.com), con consejos para la gestión de material testimonial (*eyewitness media*) | The Observers (http://observers.france24.com), programa de televisión francesa y sitio web multilingüe destacado en materia de verificación | Les Décodeurs (http://decodeurs.blog.lemonde.fr), equipo de Le Monde dedicado a la verificación digital que dispone de recursos como el buscador Décodex | EU Disinformation Unit (https://euvsdisinfo.eu), unidad de la UE especializada en la verificación de propaganda digital procedente de Rusia y que afecta principalmente al este de Europa.

1.2. En español

Es.FirstDraftNews.com (https://es.FirstDraftNews.com), textos de Firstdraftnews.com traducidos al español | Maldita.es (https://www.maldita.es), comunidad que recopila bulos y permite conversar sobre ellos | VOST Spain (http://www.vost.es), especialistas en información de emergencias | La Lupa MSUR (http://msur.es/lupa), sección de la publicación MSUR centrada en engaños sobre el mundo árabe | Hechos (https://elpais.com/agr/hechos), sección de El País centrada en bulos y verificación | El Tragabulos (https://www.facebook.com/eltragabulos), página de Facebook de Verne | El Cazabulos (http://www.eldiario.es/autores/el_cazabulos), sección de Eldiario.es contra los bulos | Esta noticia es falsa (http://facebook.com/groups/esta.noticia.es.falsa), grupo de Facebook especializado en bulos de América Latina | StopFake.org.es (https://www.stopfake.org/es/), sección en español del portal ucraniano contra bulos.

2. Herramientas

Bellingcat's digital forensic tools (http://bit.ly/2w1Xq1z) | Eoghan mac Suibhne (https://start.me/p/Wrrzk0/tools) | OSINT Framework (http://www.osintframework.com) | Verification handbook's tools (http://verificationhandbook.com/book/chapter10.php) | Julia Bayer (https://start.me/p/ZGAzN7/verification-toolset)

3. Twitter

3.1. En inglés/francés

First Draft News (@firstdraftnews) | Craig Silverman (@craigsilverman) | Claire Wardle (@cward1e) | Elliot Higgins (@EliotHiggins) | Tom Trewinard @tom_el_rumi | Aric Toler (@arictoler) | Henk van Ess (@henkvaness) | Paul Myers (@PaulMyersBBC) | Cristoph Koettl (@ckoettl) | Andy Carvin @acarvin | Julia Bayer (@bayer_julia) | Truthy (@truthyatindiana) | Political bots (@polbots) | Les Décodeurs (@decodeurs) | Les Observateurs (@observateurs) | EU Mythbusters (@EUvsDisinfo) | Stop Fake (@StopFakingNews)

3.2. En español

VOST Spain (@vostSPAIN) | Maldito Bulo (@malditobulo) | Maldita.es (@maldita_es) | El Cazabulos (@elcazabulos) | Josu Mezo (@malaprensa)

4. Recursos propios

Direcciones de la autora con información sobre verificación digital

Twitter @globograma

Globograma.com: Verificación en periodismo internacional http://www.globograma.es/verificacion-periodismo-internacional/

Lista «Verification» en @globograma: https://twitter.com/globograma/lists/verification

Diigo Globograma «Verification» (lecturas): https://www.diigo.com/profile/globograma/verification

Diigo Globograma «Verification-tools» (recursos): https://www.diigo.com/profile/globograma/verification-tools

Diigo Globograma «Verification-images» (herramientas de verificación de imagen): https://www.diigo.com/profile/globograma/verification-images

Diigo Globograma «Verification-videos» (herramientas de verificación de vídeos): https://www.diigo.com/profile/globograma/verification-videos

5. Lecturas / audiovisuales

Álvarez, Yolanda: «Guerra a la mentira». *En Portada*, Madrid: RTVE, 30-1-2017 [http://www.rtve.es/alacarta/videos/en-portada/portada-64/3892038/]

Carvin, Andy: *Distant witness. Social media, the Arab Spring and a journalism revolution*, Amazon.com, enero de 2013 [https://www.amazon.com/Distant-Witness-Andy-Carvin/dp/1939293022; consultado el 4-1-2018]

Marwick, Alice y Lewis, Rebecca: *Media manipulation and disinformation online*, Data&Society Research Institute, Nueva York, 15-5-2017. [https://datasociety.net/output/media-manipulation-and-disinfo-online/; consultado el 4-1-2018]

Nolan, Markham: *How to separate fact and fiction online*, Charla TED, noviembre 2012 [https://www.ted.com/talks/markham_nolan_how_to_separate_fact_and_fiction_online; consultado el 4-1-2018]

Ostrovsky, Simon*:* «Selfie soldiers. Russia checks in to Ukraine», Vice, 2015 [https://www.youtube.com/watch?v=2zssIFN2mso; consultado el 4-1-2018]

Silverman, Craig: *Regret the error. How media mistakes pollute the Press and imperil free speech*, Union Square Press, 2007 [https://www.amazon.com/Regret-Error-Mistakes-Pollute-Imperil/dp/B008SLF90E; consultado el 4-1-2018]

Silverman, Craig (ed.): *Manual de verificación*, European Journalism Centre, 2014 [http://verificationhandbook.com/book_es/; consultado el 2-1-2018].

Silverman, Craig; Tsubaki, Rina (eds.): *The verification handbook for investigative reporting*, EJC, 2015 [http://verificationhandbook.com/book2/chapter1.php; consultado el 2-1-2018]

Wardle, Claire y Derakhshan, Hossein: Toward an interdisciplinary framework for research and policy making, Council of Europe report, 2017-09 [https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c; consultado el 10-1-2018]

Wardle, Claire: *Social newsgathering. A collection of storyful blog posts*, Storyful, 2013 [https://itunes.apple.com/us/book/social-newsgathering/id596436867?mt=13; consultado el 4-1-2018]

Woolley, Samuel C.; Howard Philip N.: *Computational propaganda worldwide The Computational Propaganda Project*, University

of Oxford, working paper No 2017.11, noviembre de 2011 [http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf; consultado el 4-1-2018]

MYRIAM REDONDO

VERIFICACIÓN DIGITAL PARA PERIODISTAS

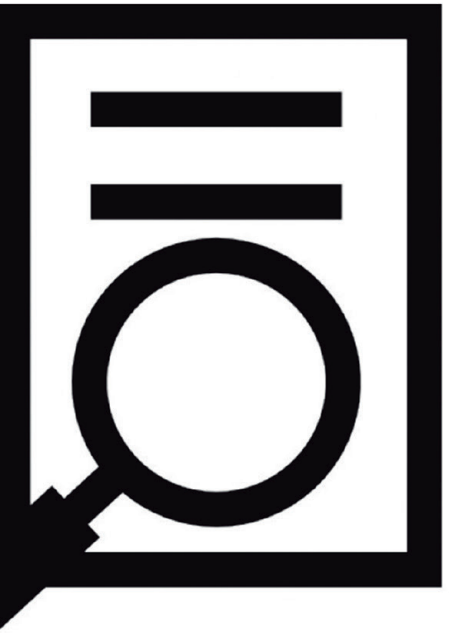
MANUAL CONTRA BULOS Y DESINFORMACIÓN INTERNACIONAL

COMUNICACIÓN

Bulos, errores, noticias falsas, *bots*, posverdad. Comprobar la fiabilidad de las informaciones en las redes sociales es un reto mayor que nunca. Este manual ofrece técnicas y recursos gratuitos para la verificación digital de informaciones, imágenes e individuos. Está pensado para periodistas, estudiantes de periodismo, interesados por la inteligencia de fuentes abiertas (OSINT) y ciudadanos concienciados sobre la desinformación internacional. ¿Quién lo afirma? ¿Qué retoques tiene la fotografía? ¿Cuándo se tomó? ¿Dónde se grabó el vídeo? ¿Por qué se difundió? Son las 5W de la profesión llevadas a Internet, además de una explicación sobre cómo se expande la mentira en línea.

Con este libro aprenderás sobre:

✓ verificación digital; ✓ redes sociales; ✓ herramientas digitales; ✓ bulos; ✓ *bots*; ✓ mentira; ✓ desinformación; ✓ propaganda; ✓ OSINT; ✓ noticias falsas; ✓ manipulación; ✓ posverdad; ✓ estrategias de búsqueda; ✓ credibilidad; ✓ fuentes de información; ✓ comunicación internacional; ✓ *fact-checking*; ✓ información de emergencias; ✓ periodismo de investigación; ✓ periodismo internacional



Myriam Redondo

Periodista y profesora universitaria, es experta en comunicación digital y relaciones internacionales, con especial atención a los contenidos generados por usuarios, la propaganda automatizada y la desinformación en Internet.

EDITORIAL UOC