QUINTA
ASAMBLEA PLENARIA DE LA
RED MUNDIAL
DE JUSTICIA ELECTORAL

Nusa Dua, Bali, Indonesia
HÍBRIDO | HYBRID | HYBRIDE
9-11 • OCT
2022

Segunda versión del "Glosario: Medios Digitales y Elecciones"

Entregable del Observatorio de Redes Sociales

Quinta Asamblea Plenaria de la Red Mundial de Justicia Electoral (RMJE)

Coordinación general: Consejo del Observatorio de Redes Sociales

Diseño y coordinación: Secretaría Técnica de la RMJE

Coordinador Académico: Rafael Rubio, Profesor de Derecho Constitucional de la Universidad Complutense de Madrid

Global Network on Electoral Justice

BAWASLU
BADAN PENGAWAS PEMILIHAN UMUM

TRIBUNAL ELECTORAL
del Poder Judicial de la Federación

Índice

Introducción

Las redes sociales han transformado las **campañas electorales**. Su irrupción en la sociedad y, sobre todo, la generalización de su uso ha provocado cambios en la forma de difusión de la información y en las posibilidades de organización política, con especial importancia en el uso de **publicidad segmentada**, en los mecanismos de financiación, o la captación y organización de voluntarios.

No se trata de innovaciones exclusivas de la campaña electoral, sino que afectan a todo el proceso, desde la presentación de las candidaturas hasta la proclamación de electos. Las tecnologías de la información han permitido extender el ejercicio del derecho al voto (Brasil), facilitar su ejercicio mejorando la información con mecanismos como los **códigos QR o el uso de chatbots**, mejorar su transparencia y las posibilidades de control (Indonesia), aumentar la eficacia del sistema y la confianza en el mismo (ofreciendo resultados en un tiempo reducido que acorta los momentos de incertidumbre).

Durante este periodo electoral se hacen más visibles las amenazas tecnológicas, al tratarse de un momento especialmente intenso que afecta a la legitimidad de todo el sistema democrático y en el que la obligatoria apertura del sistema a la sociedad puede plantear ciertas debilidades. En el periodo electoral estas amenazas apuntan a la raíz de la base de la confianza en el sistema democrático, el proceso de elección de los representantes, que es de donde obtienen estos su legitimidad.

Por un lado, se han multiplicado las amenazas de ataques tecnológicos que buscan alterar o colapsar el sistema, de manera general o selectiva. El sistema electoral, incluso cuando se apoya en un grupo amplio de personas, depende de la tecnología en fases claves como la elaboración y distribución de los censos o la transmisión de los resultados y su puesta en común, dependencia que puede ser aún mayor en lugares en los que es necesario solicitar la inscripción al censo o, evidentemente, en sistemas que han incorporado el voto electrónico. En este campo se han denunciado ataques a los censos de localizaciones específicas, que buscaban excluir a determinados votantes del proceso o retrasar el ejercicio del voto provocando aglomeraciones que disuadieran selectivamente del ejercicio del mismo, o amenazas al sistema de recuento (Países Bajos). El ataque a las infraestructuras tecnológicas también puede afectar a la campaña electoral, con el robo de información privada (Estados Unidos en la campaña presidencial de 2016), los ataques DDoS[1] a las páginas webs o la utilización ilegal de bases de datos para hacer llegar mensajes a un grupo específico. El carácter global de estas amenazas ha provocado que se

[1] Los ataques por denegación de servicio distribuidos (DDoS) son un arma de ciberseguridad cuyo objetivo es interrumpir la actividad del servicio afectado o extorsionar a las empresas víctimas del ataque.

planteen distintos principios y estándares para proteger los procesos y los derechos implicados en los mismos[2].

También en las campañas electorales **internet** se ha convertido en un elemento diferenciador, cualquiera que participa en unas elecciones sabe que utilizar de manera innovadora la tecnología ofrece, al primero en hacerlo, una ventaja de partida. No se trata sólo de cambios cuantitativos que permiten obtener ventaja a aquellos que las adoptan con anterioridad, sino que supone cambios en elementos claves de todo el proceso electoral en lo que se refiere a sus canales, pero también a sus actores y sus tiempos. La **Web 2.0** (caracterizada por los **contenidos generados por los usuarios**) que permite a estos publicar post en formato audio, video o texto, y difundir este contenido gracias a otros usuarios, dotándole de **viralidad**, ha convertido a las compañías que ofrecen la conexión (**ISP**) y a los que ofrecen el software para realizar estas publicaciones (**intermediarios de internet**) en auténticos protagonistas de las campañas.

Es tal el protagonismo de la tecnología en estos procesos que hasta han caracterizado los sucesivos procesos electorales, al menos en las campañas presidenciales norteamericanas, que suelen ir por delante en la introducción de la tecnología. Así se ha venido hablando de las elecciones de Meetup (2004), de las redes sociales (2008), de la microsegmentación (2012), o de Twitter y la publicidad en Facebook (2016).

En recientes procesos electorales, durante la campaña, se han podido ver prácticas como: la capacidad de perfilar a los usuarios y adaptar la comunicación, pagada u orgánica, a estos perfiles (práctica popularizada por la empresa *Cambridge Analytica* en la campaña pro-Brexit en el referéndum sobre la permanencia del Reino Unido en la Unión Europea, celebrado en 2018); la interferencia de personas o grupos distintos de los partidos políticos, tanto desde dentro como desde el exterior del territorio en el que se celebran las elecciones, utilizando la compra de publicidad o a través de acciones coordinadas de *astroturfing*[3] (práctica denunciada, y demostrada, en las elecciones presidenciales norteamericanas de 2016 y 2020); la creación de perfiles falsos (bots automátizados o gestionados manualmente) para crear corrientes de opinión favorables (como en el referéndum sobre el aborto en Irlanda de 2018); o el uso de plataformas de comunicación interpersonal para distribuir masivamente mensajes de desinformación (en la que destaca el uso de *Whatssapp* que hizo en la campaña presidencial brasileña Jair Bolsonaro en 2018).[4]

---

[2] Venice Commission, Principles, for a fundamental rights-compliant use of digital technologies in electoral processes. Opinion 974/2019
[3] Anónimo. Confesiones de un bot ruso. Debate, 2022.
[4] Óscar Sánchez Muñoz, La regulación de las campañas en la era digital. Desinformación y microsegmentación en las redes sociales con fines electorales, CEPC (2020).

La percepción del aumento de los riesgos para la democracia en este periodo está provocando una evolución de las respuestas jurídicas que, inicialmente, buscaban dar una solución a los nuevos fenómenos aplicando la interpretación flexible de las normas existentes, con un fuerte componente de creación jurisprudencial y una dependencia importante de los operadores tecnológicos (Rubio, 2018). Ante la cantidad y la intensidad de las amenazas asistimos en la actualidad a un cambio de tendencia, un impulso normativo de limitación proactiva de determinadas prácticas y herramientas, en el ámbito de la desinformación, la segmentación y la publicidad política, estrechamente relacionadas entre sí, y en las que la tecnología tiene un protagonismo especial.

Existe una obligación positiva de asegurar las condiciones en las que el electorado puede formar y expresar libremente su opinión y elegir a sus representantes (**el derecho a votar y a ser votado**). La libertad de expresión (especialmente en el debate político) y las elecciones libres son derechos que se necesitan mutuamente. Así, resulta imprescindible adecuar el marco jurídico, en este nuevo contexto, para garantizar las condiciones para un entorno electoral equitativo. Lo que en el escenario digital implica una serie de dificultades añadidas para proteger la libertad y el secreto del voto, mantener a salvo la libertad de expresión y no perjudicar el principio de equidad. Para hacerlo, de momento, hemos de acudir a los principios generales que afectan a los periodos de campaña, como la veda electoral, o a la financiación de las campañas electorales y a su fiscalización, que se hace mucho más compleja.

En esta línea, familiarizar a los operadores jurídicos con los conceptos más habituales en este ámbito, así como con normativas y decisiones jurisdiccionales sobre la materia contribuye a lograr ir mejorando la respuesta ante esta amenaza creciente, que debe ser necesariamente hibrida y global. Este trabajo parte del Glosario: Medios digitales y elecciones del observatorio de redes social de la Red Mundial de Justicia Electoral y, sobre esa base, lo desarrolla ofreciendo una visión general e integrada de casos y conceptos que, para mayor claridad y facilidad de identificación, hemos señalado en letra negrita.

I. Vigilancia: ¿El origen de todos nuestros males?

Rodrigo Cetina Presuel
Profesor de Derecho
Universitat Pompeu Fabra Barcelona – Escuela de Administración
Facultad de Derecho Harvard
6odrigo.cetina@bsm.upf.edu

En los últimos años se ha hecho evidente que la manipulación política y los intentos de interferir indebidamente en los procesos electorales en todo el mundo se han convertido en algo habitual y que las redes sociales están en el centro de estas inquietudes. También es evidente que las plataformas de las redes sociales tienen un problema de desinformación y de información errónea. Y aunque la difusión de mentiras, información inexacta o perjudicial o los intentos de manipulación de la opinión pública no son nada nuevo, ha quedado claro que las plataformas de las redes sociales agravan los problemas relacionados con estos fenómenos en virtud de sus características (que no son en absoluto únicas, algunas se comparten con otras TIC y otros medios de comunicación): la difusión de la información no es jerárquica, se propaga con gran velocidad y a menudo de forma viral entre las redes de usuarios conectados, etc. Otras características más singulares (aunque también presentes en otros medios de Internet) son que los mensajes también pueden emitirse utilizando técnicas de *microtargeting* y personalización para difundir todo tipo de información a grupos de usuarios específicos y que hacen muy difícil averiguar qué grupos están expuestos a qué mensajes, (cámaras de eco, burbujas epistémicas), que la difusión de la información es algo más rápida que con otros y que la economía de los contenidos es también diferente.

Glosario

De todos los conceptos que deben ser considerados debemos referirnos en primer lugar a la vigilancia, ya que, como se dijo anteriormente, este concepto subyace a todas las lógicas que operan para dar lugar a los problemas que este trabajo explora en relación con la injerencia electoral.

La **vigilancia** (*surveillance* en inglés) es la recopilación y el procesamiento de información personal para su cuidado o control y que permite la identificación, el seguimiento y la categorización de personas o grupos de personas. Aunque las prácticas de vigilancia han existido desde hace mucho tiempo y el seguimiento sistematizado de poblaciones e individuos es una característica distintiva del Estado moderno (actividad conocida como vigilancia estatal), la vigilancia contemporánea añade otras dos características definitorias, es decir, que se trata de una vigilancia digital, definida como la recopilación y el procesamiento de datos personales computarizados; y que muchas empresas privadas basadas en Internet se dedican a

la vigilancia de sus usuarios para sus propios objetivos privados y no necesariamente por mandato gubernamental, un conjunto de actividades conocidas como vigilancia privada.

Además de definir la vigilancia, debemos necesariamente definir los temas relacionados, ya que el concepto de vigilancia se encuentra presente en las lógicas que operan en la mayoría de los problemas relacionados con la interferencia electoral y la manipulación política. Esto hace necesario, entonces, definir adecuadamente las diferentes subcategorías de vigilancia, junto con otros términos relacionados para crear una visión completa de los conceptos y una mejor comprensión de los mismos, juntos y separados.

Estos conceptos incluyen la **vigilancia estatal** (*state surveillance*) o las actividades de vigilancia llevadas a cabo por el Estado y en busca de objetivos gubernamentales. La vigilancia sistémica de poblaciones e individuos se ha convertido en una característica distintiva del Estado moderno. La **vigilancia privada** (*private surveillance*) se define como las actividades de vigilancia llevadas a cabo por entidades privadas que no forman parte del gobierno. Las empresas privadas basadas en Internet se dedican a la vigilancia digital de sus usuarios para sus propios objetivos privados y no necesariamente por mandato gubernamental, aunque puedan prestar servicios de vigilancia o suministrar tecnología de vigilancia a los gobiernos y sus organismos. También incluye la **vigilancia digital** (*digital surveillance)*, o la recopilación y el procesamiento de datos personales informatizados y que permiten la identificación, el seguimiento y la categorización de personas o grupos de personas, así como la vigilancia en línea (vigilancia de las redes sociales), que es cualquier actividad de vigilancia digital realizada en línea y en las plataformas dichas redes.

Para las empresas propietarias de las redes sociales, se trata de una práctica esencial en el centro de la monetización de sus actividades lucrativas. Para los gobiernos, Internet, y en particular las redes sociales, se han convertido en un espacio para la vigilancia de la ciudadanía con diversos objetivos políticos y electorales. También incluye los conceptos de **vigilancia digital privada-pública** (*private-public digital surveillance)*, que es la combinación de actividades y objetivos de vigilancia llevados a cabo por el Estado y por entidades privadas. A menudo, implica la dependencia de la tecnología de vigilancia privada para objetivos estatales que los gobiernos no podrían alcanzar por sí mismos. Otro concepto clave es la **vigilancia política digital** (*digital political surveillance**)***, que es el uso de las plataformas de las redes sociales para controlar a la ciudadanía, inhibir su acción política y silenciar la disidencia.

A su vez, tenemos otros conceptos que nos ayudan a pintar una imagen adecuada del estado actual de la vigilancia en línea, que son el **capitalismo de la vigilancia** (*surveillance capitalism)*, definido como una forma de capitalismo de la información en el que el sistema económico se centra en la recopilación de datos personales para

permitir la predicción y modificación del comportamiento humano para producir ingresos y lograr el control del mercado.[5] Otro concepto es el **instrumentalismo** (*instrumentarianism)*, que es la instrumentación y la instrumentalización del comportamiento humano con fines de modificación, predicción, monetización y control.[6] Tal y como lo define Zubboff, es un concepto íntimamente relacionado con el capitalismo de vigilancia.

La vigilancia privada activa por parte de las plataformas de las redes sociales las ha diferenciado de otros tipos de medios de comunicación. Esta capacidad sociotécnica de registrar y vigilar cada acción que un usuario realiza en línea no solo permite a las plataformas de las redes sociales construir complejos (aunque inexactos) perfiles de sus usuarios que, a su vez, les permiten separarlos en grupos y entregarles contenidos personalizados, sino que es también, en su gran mayoría, lo que subyace al modelo de negocio de las empresas de redes sociales. Se busca el beneficio a través de la vigilancia de los usuarios, la extracción y el tratamiento de sus datos personales y la venta de estos datos, de los perfiles de los usuarios o habilitando sistemas que les permitan vender publicidad personalizada (incluida la publicidad política dirigida) o servir contenidos personalizados, lo que tenga más probabilidades de mantener a un usuario comprometido y utilizando la plataforma, y a su vez extraer más información sobre ellos para monetizarla, y así sucesivamente.

La industria de la vigilancia digital privada ha crecido y se ha sofisticado desarrollando una tecnología que supera con creces las capacidades de vigilancia del Estado, los gobiernos han empezado a contratar servicios de vigilancia de entidades privadas y hacer uso de una tecnología que originalmente sirve para la vigilancia privada y que luego se reutiliza para la vigilancia estatal. La vigilancia privada y la pública se combinan para dar lugar a un enorme aparato de vigilancia empresarial-estatal. Una asociación público-privada.

Los intereses privados y los intereses públicos han hecho que la tecnología de vigilancia digital sea omnipresente. Las capacidades de vigilancia digital se han ampliado y sofisticado para abarcar a todo tipo de personas en todo tipo de lugares y situaciones. Como ya se ha dicho, la propia vigilancia privada se ha convertido en una parte muy importante de la industria digital, ya que permite obtener beneficios a través de la venta de datos y la venta de publicidad. La vigilancia privada digital de los usuarios se ha convertido en algo tan central en Internet tal y como la conocemos que algunas personas describen este modelo económico como un subconjunto del capitalismo, llamándolo capitalismo de la vigilancia.

[5] Zuboff, S. (2015). Big other: Surveillance Capitalism and the Prospects of an Information Civilization. Journal of Information Technology, 30(1), 75–89. https://doi.org/10.1057/jit.2015.5
[6]Zuboff, S. (2019). Surveillance Capitalism and the Challenge of Collective Action. New Labor Forum, 28(1), 10–29. https://doi.org/10.1177/1095796018819461, p. 20.

Sin embargo, la vigilancia no solo está en el centro del modelo de negocio de las plataformas de las redes sociales, sino que también puede estar en el centro de muchos de los males que asociamos a las redes sociales: invasiones de la privacidad, violación del derecho a la protección de los datos personales (que implica el control de los datos sobre uno mismo), difusión de discursos que incitan al odio, facilitar el abuso en línea, la difusión de contenidos dirigidos y publicidad dirigida (a veces con la intención de manipular o desinformar), y también puede ser una de las causas centrales del propio fenómeno de la desinformación en línea.

Esto se debe a que las plataformas de las redes sociales no basan su modelo de negocio en servir contenidos a sus usuarios ni en mantenerlos conectados, ni en ser el mejor medio posible para recibir las noticias, mantenerse bien informado o potenciar la opinión pública y el debate político. A pesar de lo que se pueda oír, la promoción de la libertad de expresión o de la libertad de prensa tampoco es fundamental en su forma de hacer negocios. La vigilancia de sus usuarios sí lo es.

Bajo la lógica del capitalismo de la vigilancia, las plataformas de las redes sociales tratan de proporcionar a los usuarios cualquier contenido que pueda hacer que sigan utilizando la plataforma, ya que el aumento de la actividad de los usuarios conduce a un aumento de la vigilancia del usuario o, en otras palabras, a un aumento de las oportunidades para vigilarlos y extraer datos que puedan convertirse en beneficios de una forma u otra.

Esto ha hecho que las plataformas de las redes sociales sean agnósticas en cuanto a la información. Eso significa que la principal preocupación de éstas es difundir cualquier información a cualquier usuario si puede mantenerlo comprometido y utilizando la plataforma, incluso si puede ser mala información o desinformación e independientemente de si el contenido es abusivo o manipulador. También significa que la creación de cámaras de eco mediante la distribución selectiva de información, mensajes o publicidad es una preocupación secundaria si mantiene a los usuarios comprometidos. En otras palabras, un modelo de negocio centrado en la vigilancia da a las plataformas un incentivo para ser lo más agnósticas posible con respecto a la información. Todo vale con tal de mantener la atención en las plataformas.

A través de la herramienta sociotécnica de la vigilancia, la información de calidad (pero también la de mala calidad) se considera solo una herramienta, un medio para otro fin, y no una preocupación central. Las plataformas de las redes sociales no son más que un conjunto de herramientas, un grupo de técnicas digitales para difundir mensajes y, en las manos equivocadas, pueden utilizarse para objetivos más nefastos que generen confusión electoral, estabilidad política y puedan socavar los procesos y las instituciones democráticas.

Las plataformas de las redes sociales ya no son ciegas a estos problemas y es cierto que, junto con los reguladores y la sociedad civil, están tomando medidas para mitigar los efectos negativos de la desinformación en línea, pero si dejaron que el problema se agravara y se convirtiera en algo sistémico, si no se dieron cuenta de que estaba ahí hasta que aparecieron los primeros relatos de injerencia electoral, de intentos de derribar las instituciones democráticas a través de la difusión de información falsa que condujo a una violencia política muy real, incluida la violencia de género y étnica, es porque abordarlos no estaba en el centro de su forma de operar, al menos no al principio.

Si bien es cierto que, tras verse envueltas en un escándalo tras otro y sufrir las consecuencias en materia de relaciones públicas y bajo una importante presión política y reguladora de los gobiernos para que actúen, las plataformas de las redes sociales han comenzado a realizar una supervisión más activa, filtrando y moderando los contenidos más nocivos, el hecho es que el resultado final ha sido negativo para las democracias y la ciudadanía de todo el mundo.

La vigilancia digital privada y pública y la vigilancia digital privada-pública conllevan riesgos específicos para la ciudadanía y ponen en peligro sus derechos y su bienestar. Algunos de estos riesgos socavan directamente la participación política y la vigilancia es la actividad subyacente a otras prácticas que también tienen efectos negativos para la democracia, como la difusión de desinformación, la manipulación política y la interferencia electoral.

De acuerdo con la Unión Europea, la vigilancia política en las redes sociales puede permitir a los gobiernos controlar a la ciudadanía, inhibir su acción política y silenciar la disidencia. La vigilancia de las redes sociales conduce a la pérdida de privacidad y autonomía, ya que socava la capacidad de juicio político de la ciudadanía y puede conducir a la desvinculación política, ya que la promoción de contenidos virales y el comportamiento adictivo en las redes sociales pueden distraer a la gente de la política.

A su vez, la personalización impulsada por la vigilancia encierra a la ciudadanía en burbujas informativas y afecta su capacidad para formarse opiniones, reduciendo su visión del mundo. La personalización también conduce a la fragmentación social y política, ya que la segmentación de la información y el compromiso reduce las oportunidades de diálogo político.

La personalización impulsada por la vigilancia también puede contribuir a la desinformación, ya que ayuda a distorsionar las opiniones y las preferencias mediante la difusión de información falsa en línea, y su difusión puede distorsionar los resultados electorales, socavando la integridad de las elecciones y afectando a los resultados electorales. La vigilancia también es clave para hacer posible la

desinformación automatizada, ya que las cuentas automatizadas pueden basarse en los perfiles de los usuarios para amplificar y exacerbar los efectos de la información falsa.

Es especialmente importante que estos conceptos se definan adecuadamente para poder comprenderlos mejor y contribuir a identificar adecuadamente aquellos usos indeseables de las técnicas y adoptar medidas para combatirlos. Esta contribución contiene la definición de varios de los conceptos mencionados, así como de otros relacionados, partiendo de un trabajo previo que ha dado lugar a un glosario de términos relacionados con el uso de la tecnología para interferir en las elecciones y la manipulación política en línea, así como a una clasificación que permite construir un mapa de términos relacionados.

Para complementar estas definiciones, también hemos realizado un análisis de la jurisprudencia y la legislación que aborda estos conceptos y, en el caso de este capítulo, específicamente el concepto y la actividad de la vigilancia. El objetivo de esto es arrojar información sobre lo que la ley y los tribunales tienen que decir al respecto, su definición legal y sus límites legales, incluyendo cómo la vigilancia en línea puede socavar los derechos fundamentales de la ciudadanía y si la ley reconoce adecuadamente que la vigilancia permite la manipulación política, la interferencia electoral y puede ser una amenaza para los procesos electorales y las instituciones democráticas, así como qué respuestas a sus efectos negativos existen en la ley.

Casos

En concreto, este trabajo incluye un análisis de varios casos revisados por la Junta Electoral Central (JEC). Todos estos casos están relacionados con las campañas electorales y tienen relación directa e indirecta con el uso de la vigilancia para emitir mensajes políticos y propaganda electoral, especialmente en el contexto del Reglamento General de Elecciones (LOREG). Se revisaron 28 casos e instrucciones que abarcan el periodo de 2011 a 2021, junto con otro caso relacionado que se remonta a 2006. Algunos de estos casos son solicitudes de aprobación, otros son consultas y otros son instrucciones emitidas en relación con la interpretación de las normas electorales y de campaña política, otros son quejas contra partidos políticos, políticos u organismos gubernamentales.

También se revisó una decisión del Tribunal Constitucional de España que aborda la constitucionalidad de algunas disposiciones de la ley electoral general relacionadas con la salvaguarda de los derechos fundamentales, incluido el derecho a la protección de los datos personales relacionados con las opiniones políticas, así como un caso ante el Tribunal Electoral de México que analizó la naturaleza de las redes sociales y la distribución de opiniones políticas y propaganda electoral a través de ellas, así

como otro caso del Consejo Nacional Electoral de Colombia que reflexiona de forma similar sobre la naturaleza de las redes sociales y sus capacidades tanto para dirigirse a los usuarios como para transmitir mensajes políticos y propaganda electoral a las masas.

Una valoración general de los casos analizados permite reflexionar sobre sus implicaciones para la vigilancia digital y lo que esto significa para los procesos electorales y el uso de las redes sociales de manera que se fortalezca, y no se obstaculice, el debate político, la elección política informada y los procesos políticos democráticos sólidos.

En el caso de España, basándose en los casos revisados, la Junta Electoral ha interpretado las leyes pertinentes relacionadas con las comunicaciones electorales para incluir todas las formas de comunicación en línea. Sin embargo, parece que la JEC no ha abordado directamente las implicaciones que la vigilancia, el *microtargeting* y la creación de perfiles en línea pueden tener con respecto a la forma en que los mensajes son entregados en línea y, por lo tanto, todavía tiene que lidiar más directamente con los requisitos tales como la transparencia o el control de los gastos de campaña en línea con el fin de garantizar elecciones libres y justas, ya que las redes sociales siguen siendo una herramienta central en las comunicaciones electorales modernas.

Sin embargo, el Tribunal Constitucional español anuló un artículo de la Ley Electoral española (art. 58 bis 1) que habría permitido a los partidos políticos recopilar y procesar datos personales relacionados con las opiniones políticas de la ciudadanía por no ofrecer suficientes garantías adecuadas a los derechos y datos de éstos y por no poder definir claramente qué interés público y constitucional pretendía perseguir. Esto tiene implicaciones fuertes y directas, particularmente para la vigilancia política en España y junto con la ley nacional de protección de datos y el Reglamento Europeo de Protección de Datos sirven como un marco fuerte para los derechos de protección de datos de la ciudadanía y en este caso, proporcionan fuertes elementos para la protección de datos como un instrumento de libertad de tener y expresar opiniones políticas garantizadas por la Constitución Española y en el marco europeo de protección de derechos fundamentales.

En el caso de México, está claro que, al menos en el caso revisado, el Tribunal Electoral no demostró suficiente sofisticación en su comprensión de cómo funciona el internet moderno, y particularmente cómo funcionan las redes sociales. El compromiso del Tribunal de poner un límite alto a la libertad de expresión, así como a la libertad de expresar la preferencia por uno u otro candidato político es loable, incluyendo la protección de esos derechos para los familiares de los candidatos políticos. Sin embargo, además de las referencias de que el Internet es diferente a otros medios de comunicación y de incluir una definición de *microtargeting*, e incluso

de *influencer*, no reconoce otros conceptos importantes como el marketing orgánico y la viralidad de las publicaciones y atribuye una "presunción de espontaneidad" a todas las publicaciones en las redes sociales que está en desacuerdo con la forma en que se utilizan las redes sociales para cualquier objetivo incluso tangencialmente relacionado con objetivos comerciales, políticos o electorales. El criterio de la autoridad electoral mexicana es que las redes sociales e Internet son tan diferentes de medios como la televisión o la radio que su ley electoral no debe aplicarse a las comunicaciones realizadas a través de medios online, lo que parece anticuado. En todo caso, esto puede ser una señal de que la ley electoral mexicana debería haber cambiado para incluir las comunicaciones electorales en línea con el fin de establecer adecuadamente las reglas del juego y mantener la ley electoral mexicana en sintonía con lo que otros países están haciendo.

Finalmente, el caso de Colombia es interesante por las razones opuestas, demuestra una comprensión más sofisticada de las redes sociales por parte del Consejo Nacional Electoral de ese país, al resolver sobre un caso de comunicaciones electorales realizadas fuera del período que permite la ley. Si bien el Consejo concedió que, según los criterios seguidos hasta entonces, la infracción no debía ser objeto de sanción, reconoce que tales criterios deben cambiar dada la naturaleza de Internet y señala que lo hará en el futuro. Es interesante que tenga en cuenta cómo se distribuyen de hecho las comunicaciones en internet, tanto permitiendo que los mensajes se dirijan directamente a grupos específicos de usuarios, como entendiendo que esos mensajes también pueden ponerse a disposición de grupos indeterminados de personas, y que a veces esa es precisamente la estrategia de quienes pretenden distribuir comunicaciones electorales en internet.

II. Desinformación

Vitor de Andrade Monteiro

Las mentiras, los rumores y los engaños nunca han sido ajenos a la política. De hecho, el disimulo y la falsedad son figuras que siempre han estado presentes en las disputas políticas y en el entorno del ambiente democrático. Algunos historiadores afirman que hasta el mismo contexto de lo que se ha conocido como el marco de la aparición de la democracia en Atenas conlleva algo de falso. Se sugiere que los motivos del heroico tiranicidio de Hiparco por parte de Harmodio y Aristógito, que dio lugar a la instauración de la democracia en Atenas unos años más tarde, tuvieron más que ver con razones pasionales y egoístas que con un noble espíritu democrático. A pesar de ello, la historia falsa ha triunfado y los amantes fueron reconocidos como los fundadores de la democracia, habiendo recibido tributos y sus descendientes obteniendo honores y privilegios.

En la antigua Roma, expedientes desinformativos fueron utilizados por emperadores para buscar legitimidad y asegurar la estabilidad de su gobierno. Septimio Severo, aunque no tenía ningún vínculo familiar con su predecesor, Cómodo, que era hijo ilegítimo de Marco Aurelio, trató de crear una falsa relación con este famoso emperador, para que fuera aceptado por la población como el sucesor más legítimo. Como una parte considerable de la población romana no sabía leer y las noticias se reproducían principalmente a través de imágenes, ordenó la acuñación de monedas con su imagen debidamente retocada para presentar rasgos físicos similares a Marco Aurelio y fortalecer su aceptación por la población romana.

Dada esta antigua relación entre la mentira y la política, cabe preguntarse entonces por qué las discusiones sobre la mentira en la política han adquirido tanta proyección en la actualidad. ¿Por qué las ***fake news*** son objeto de tantos debates y preocupaciones para los organismos electorales? En otras palabras, si la falsedad siempre ha existido en la política, ¿por qué sigue siendo importante discutir la **desinformación**?

La búsqueda de respuestas a estas preguntas parece pasar por dos puntos. Uno de ellos es el fenómeno de la **posverdad**, y su impacto en la comprensión de la mentira (¡y de la verdad!) en la actualidad; el otro es la llegada de las plataformas digitales y toda la revolución que ha provocado en el campo de la comunicación que se deriva de ella. Aunque el alcance del presente trabajo no permite un análisis en profundidad de cada uno de los puntos mencionados, el desarrollo del tema central de este escrito requiere un paso, aunque sea breve, por ellos.

El término **posverdad** se presenta como una expresión de efecto que sirve para captar un panorama de los tiempos actuales. Representa el declive de la racionalidad, la ofuscación de los hechos, la superación de la realidad comprable por una lógica

guiada por la emoción, por la creencia y por la subjetividad. En los tiempos de la posverdad, los hechos objetivos y verificables tienen menos influencia en la **opinión pública** que las creencias individuales. Mejor dicho, no hay hechos, sino interpretaciones sobre los hechos. Es la victoria de la *doxa* sobre la *episteme*, de la opinión sobre el conocimiento. Un estudio científico metodológicamente correcto y contrastado por la comunidad académica pasa a tener el mismo peso que una opinión legal.

La liquidez de los tiempos actuales no permite reflexiones exhaustivas - y tediosas - y las conclusiones parecen seguir esta dinámica, favoreciendo la horizontalidad. Es el triunfo del hígado sobre el cerebro, de lo aparentemente simple sobre lo honestamente complejo. En este escenario, la búsqueda de la verdad ha sido sustituida por la construcción de una versión de los hechos que aporte satisfacción y ofrezca protección frente a la dureza de la realidad. Esa reclusión en la subjetividad dirige el pensamiento hacia un ambiente acogedor, que ofrece opiniones que refuerzan las convicciones preexistentes, aunque estén fundadas en el vacío. Es el entorno perfecto para el desarrollo de **metarrelatos**, **teorías conspirativas** y **realidades alternativas** de diversos tipos, todo lo cual colabora a la devaluación de la verdad como elemento para la toma de decisiones políticas.

A este alejamiento de la idea de verdad se suma el impacto de las nuevas tecnologías en el **ecosistema de la información**. Con el crecimiento vertiginoso de la comunicación por medios digitales y su inserción cada vez más profunda en la sociedad, se han producido cambios significativos y de diversas índoles. La informalidad con la que se desarrolla la comunicación en el entorno digital, aunque democratiza el derecho a opinar, ha acabado potenciando los efectos de la posverdad, ya que ha posibilitado una competencia relativamente equilibrada entre los hechos científicamente probados y los textos periodísticos profesionales, de un lado, con las opiniones sin fundamento y la resignificación de hechos, de otro. Esto resulta aún más impactante ante el inmenso volumen de contenidos que se producen cada minuto en las redes sociales.

Por otro lado, el modelo de negocio de las plataformas digitales fomenta la amplificación de la desinformación, ya que se basa en la capitalización de la atención y de la participación de los usuarios. La información falsa se difunde mucho más rápido, más lejos y más profundamente que la información verdadera, y por lo tanto genera más beneficios. Los efectos nocivos de la desinformación se observan en diversos contextos de la vida en sociedad, desde las decisiones sobre cuestiones relacionadas con problemas económicos y de salud pública, en la evaluación de las políticas de drogas, en cuestiones religiosas, etc. Sin embargo, es el contexto político el que parece ser más susceptible a la influencia de la **información manipulada**, habiéndose comprobado que la información falsa sobre este tema se difunde significativamente más rápido, más lejos, más profundamente y más ampliamente que

otras relativas al terrorismo, los desastres naturales, la ciencia y las leyendas urbanas (VOSOUGHI et al., 2018).

La desinformación degrada el terreno en el que se construye el diálogo, fomentando el uso de la fuerza como medio para resolver las divergencias. La democracia pierde espacio ya que su existencia depende de la circulación libre y sin obstáculos de las ideas (STENGEL, 2020). Los **desórdenes informativos** minan el derecho a participar en el proceso electoral de forma consciente e informada, lo que se traduce en un déficit de legitimidad en el resultado de las elecciones y en un daño a la normalidad del proceso electoral.

Más que ofrecer resultados válidos que se correspondan con la realidad, el proceso electoral, para lograr su principal objetivo, necesita transmitir la sensación de validez y legitimidad. Como la mujer del César, no basta con que la justicia electoral actúe bien, sino que es necesario transmitir al votante la percepción de que el proceso electoral se desarrolló dentro de la normalidad y extrajo la verdadera voluntad del electorado. La misión institucional de la justicia electoral requiere, por lo tanto, la producción de confianza y es precisamente en este punto donde se han centrado los mercaderes de la desinformación.

Se ha identificado una tendencia preocupante por la que el **desorden informativo** en el contexto electoral está dirigido a atacar la integridad del proceso electoral y a las autoridades vinculadas al organismo electoral competente para su realización. Esta estrategia, constantemente asociada a algún tipo de **populismo digital** (BRUZZONE, 2021), ha sido identificada en varios países del mundo, como lo ejemplifican las últimas elecciones presidenciales de Estados Unidos, el voto del Brexit, las elecciones brasileñas de 2018 y 2020, las elecciones presidenciales de México, Hungría y Perú.

Estos artificios perniciosos tienden a impactar en la credibilidad de las instituciones involucradas en el proceso y generan descrédito en los resultados obtenidos en las elecciones. Este escenario abre la puerta a movimientos pro-ruptura (como en el caso de **Myanmar)** y a levantamientos populares seguidos de violencia y muerte (como en **Kenia** y **Costa de Marfil**). Además, la propia existencia del organismo electoral puede verse afectada por los efectos de la desinformación, ya que la pérdida de reputación abre el camino a reacciones legislativas (como la pérdida de competencias por parte del organismo electoral) y a la intensificación de los ataques dirigidos a la asfixia institucional (como la reducción de los presupuestos, las prerrogativas funcionales y el personal). Un ejemplo llamativo es el caso del **Instituto Nacional Electoral de México**, que, tras ser víctima de varias noticias desinformativas, fue propuesto su supresión por el presidente de la república, Andrés Manuel López Obrador.

Los impactos de la desinformación se pueden hacer más sentidos con la utilización de **estrategias de automación de perfiles** en redes sociales, permitiendo que las informaciones manipuladas sean difundidas por ***bots*** con apariencia humana para promover determinados posts, amplificación de publicaciones de fuentes de baja

credibilidad y las menciones a usuarios influyentes en esas publicaciones. Con ese comportamiento los *bots* desempeñan un papel destacado en la producción del efecto viral de la desinformación.

Glosario

Una adecuada comprensión del fenómeno de la desinformación exige la familiaridad con algunos conceptos que traducen características importantes sobre los desórdenes informativas. En principio, la propia definición de lo que esta inserto en el concepto de desinformación es algo que demanda una atención detenida. Para algunos autores, como Wardle y Derakhshan (2017), la desinformación es una de las nociones que están incluidas en la idea de desórdenes informativas. Para ellos, hay que distinguir los mensajes que son verdaderas de las que son falsas, y aun las que son creadas con la intención de causar daños, de las que no son. Así, los desórdenes informativas constituyen un conjunto que incluye las figuras de la a) **información errónea** (***misinformation***), que es la que se produce sin la intención que causas perjuicios, pero que tiene contenido falso ; b) **desinformación** ***(disinformation),*** que son los contenidos creados deliberadamente para causar daños; y c) **malinformación (*malinformation*),** que es la información basada en la realidad, pero que es utilizada con la intención de causar daño a alguien, a una organización o a un Estado (Wardle y Derakhshan, 2017).

A pesar de la larga utilización de la expresión ***fake news*** por la media, su empleo no es recomendado para la definición del fenómeno de la desinformación, una vez que no permite una clara delimitación de su objecto ni tampoco la correcta comprensión del problema. Explico, primeramente, si observa que la expresión *fake news* ha sido utilizada como un arma que es dirigida a los oponentes por su propia condición de enemigo, y no contra informaciones por elles presentadas. Además, como ha sido visto, por veces los desórdenes informativos incluyen informaciones que en su origen no son *fakes,* como en el caso de la malinformación. También se percibe que la propia idea de noticia está ligada a algo basado en la verdad, lo que torna la expresión *fake news* un oxímoron.

Otro concepto importante para la comprensión del fenómeno es lo de ***Information Operations*** o ***Influence Operations***, que consisten en una serie de técnicas de guerra utilizadas para obtener informaciones, influenciar y desestabilizar el proceso de tomada de decisión del adversario. Las prácticas desinformativas humanas por veces se promueven de manera ordenada, por empresas que se dedican a crear y administrar perfiles para producir ***post*** y ***likes*** para estimular determinada narrativa. Esas empresas son conocidas como **haciendas de contenidos o de clicks (*content* o *click farms***). La figura de los ***trolls*** también es particularmente presente en la desinformación y consiste en usuarios de plataformas digitales que buscan, de manera deliberada, amenazar, provocar, intimidar y ofender para causar distracción

o discordia. Sus acciones pueden ser insoladas o de forma ordenada con otros actores. Por veces su actuación es promovida por empresas dedicas a esas finalidades y que actúan en la misma manera que la haciendas de cliques, y por eso son conocidas como ***troll farms***.

En la actividad desinformativa son muchas las maneras de crear narrativas y una de las más sofisticadas son las ***Deep fakes***, que consisten en la manipulación de imágenes y videos por medio de inteligencia artificial para combinar aspectos reales con otros fabricados buscando crear contenido ultra realista en que personas digan o hagan cosas que no pasaran, creando confusión en el destinatario. La desinformación suele se beneficiar de prácticas reprehensibles para obtener más resultados. El ***phishing*** es una de ellas y se basa en ataques dirigidos por *hackers* para obtener datos personales de usuarios.

Casos

A pesar de la desinformación no ser algo nuevo en la sociedad, su impacto en los procesos electorales ahora recibe más atención de los organismos electorales. En este texto se incluyen diversos casos juzgados por la Junta Central Electoral española (JEC), por el Tribunal Superior Electoral de Brasil (TSE) y de Argentina que demuestran las formas como las cortes electorales están haciendo frente a el fenómeno de la desinformación por medio de las plataformas digitales en el proceso electoral. En la secuencia se presentan algunos de esos casos además de documentos que tratan sobre los retos del enfrentamiento a la desinformación.

La desinformación afecta la capacidad del elector elegir su candidato basado en informaciones veraces e ideas que corresponden a la realidad. Así, el acceso a la información correcta, transparente y accesible es requisito para la efectiva libertad. Para la **Cámara Nacional Electoral Argentina**, en la **Acordada Extraordinaria 66/18**, cuanta más información, imparcialidad y libertad en el proceso electoral, mayor será la calidad de la democracia. La Cámara registró los impactos en la amplificación de la desinformación de los ***trolls*** (“comentaristas pagos que utilizan perfiles falsos”) y de los ***bots*** (“perfiles simulados con determinados momentos de intensa actividad en línea, seguidos de largos períodos de inactividad”). Para la institución, para si alcanzar algún éxito en la compleja tarea de contrarrestar la manipulación informativa es necesario “tiempo, recursos y creatividad”, empezando por una especial atención para la educación mediática. Después de desarrollar un análisis del fenómeno en varios contextos electorales, la Cámara pasó a adoptar una serie de medidas dirigidas a regulación de la participación de participantes de la disputada electoral en las elecciones, tales como la divulgación de los resultados del monitoreo de redes sociales y propaganda y la creación de registro de cuentas de redes sociales y de sitios *web* oficiales de los candidatos, agrupaciones políticas y máximas autoridades electorales.

En el **Fallo 3010/02, la Cámara Nacional Electoral Argentina** reiteró la importancia del acceso a la información para el ejercicio del derecho de votar, a que se llamó de "voto informado". La relevancia del **acceso a información** para la **orden democrática** ha sido destacada en el **Parecer Consultivo OC-5/85** de la Corte Interamericana de Derechos Humanos, que registró que la libertad de expresión es condición para que la sociedad tome sus decisiones de manera informada. La conclusión de la Corte es que una sociedad no es libre se no está bien informada, y, evidentemente, la calidad de la información es esencial para la efectiva libertad.

Una importante iniciativa desarrollada por la Cámara Nacional Electoral Argentina para preservar la calidad del debate democrático en las plataformas digitales es el **Compromiso Ético Digital**. Ese documento tiene en cuenta la creciente preocupación con la manipulación de informaciones en las redes digitales y en el entorno digital y su impacto en la democracia. EL Compromiso menciona la referida **Acordada 66/18** para registrar la conveniencia de promover la educación digital para mejorar el manejo de la información política electoral en el entorno digital. Al adherir al compromiso las entidades asumen el compromiso de promover, "la honestidad del debate democrático en las próximas elecciones nacionales, de modo de contribuir a mitigar los efectos negativos de la divulgación de contenido falso y demás tácticas de desinformación en redes sociales y otros entornos digitales". A su tiempo, las plataformas digital adherentes declaran que "reconocen la complejidad y la tensión que puede existir durante el proceso electoral con la difusión o proliferación de información inexacta o noticias falsas, y acuerdan, dentro del marco de sus posibilidades y herramientas, colaborar con las autoridades competentes en este proceso respetando los valores democráticos y la libertad de expresión". Diversas plataformas digitales adherirán al compromiso, como Google, Twitter, Facebook, Whatsapp, Kwai y Tik Tok.

Las **plataformas sociales** poseen especial relevancia en las comunicaciones en la contemporaneidad. En ese sentido la **Junta Electoral Central de España**, al juzgar el **expediente 293/1215, en el Acuerdo 146/2021**, ha reconocido la predominancia de las redes sociales en la sociedad actual, entendiendo que su utilización se muestra casi imprescindible para candidatos y formaciones electorales. En vista de eso, el comportamiento de las redes sociales ante las partes no puede ser considerado un irrelevante político. De hecho, la actuación de las plataformas debe observar lo principio de igualdad, no pudendo servir como herramienta de desequilibrio del juego político. Delante de esa constatación, se observa que pueden surgir obligaciones que van allá de las contenidas en sus contratos de uso. Así, para la Junta, la sanción aplicada por Twitter, de suspensión de funciones del perfil de un partido electoral, por cuenta del incumplimiento de sus términos de uso fue razonable fase a el comportamiento de la agremiación.

En Brasil, a pesar de la espantosa amplitud que la desinformación ha alcanzado en el escenario político, son poco los casos en que la temática ha sido debatida en la corte superior electoral. En dos importantes casos el TSE ha debatido sobre la posibilidad de aplicar sanción de perdida de mandato por cuenta de la **difusión de desinformación** por los candidatos y de la **utilización de envío en masa** por medio de la aplicación Whatsapp.

El **caso Franceschini** se ocupa de la **difusión de desinformación contra el proceso electoral a través de las redes sociales** el día de las elecciones. En resumen, un diputado hizo una transmisión en vivo el día de las elecciones, y antes de su cierre, afirmando que tenían urnas fraudulentas y que tenía información oficial sobre el fraude. El TSE consideró que había motivos suficientes para la destitución, al considerar que había habido abuso de poder mediático. Según los datos expresados en la sentencia, la emisión en directo fue transmitida en vivo, antes del término de las votaciones (en 07/10/2018), a más de 70.000 personas (en 12/11/2018, tenía más de 105.000 comentarios, 400.000 compartidos y seis millones de visualizaciones). Entre los discursos pronunciados en la ocasión ha sido dicho que las “urnas son adulteradas” y que había documentos de la Justicia Electoral reconociendo esa afirmación. El Supremo Tribunal Federal de Brasil (STF), al ser cuestionado, confirmó la constitucionalidad de la decisión del TSE.

La cuestión de la utilización de **envíos en masa** por medio de la aplicación Whatsapp fue el objeto del **caso Bolsonaro/Mourão**. En el juzgado la candidatura presidencial fue absuelta por falta de pruebas sólidas de la acusación de abuso de poder económico y uso indebido de los medios de comunicación. Aunque el caso concreto no se ha impuesto ninguna sanción, el caso merece importancia pues en el fallo se estableció la siguiente tesis: “la utilización de aplicaciones digitales de mensajería instantánea para promover comunicados masivos que contengan desinformación y falsedades en perjuicio de los adversarios y en beneficio de un candidato puede constituir abuso de poder económico y utilización indebida de los medios de comunicación, de conformidad con el **artículo 22 de la LC 64/1990 (la Ley de Inelegibilidad),** en función de la gravedad real de la conducta, que se examinará en cada caso”.

El fenómeno de la desinformación trae nuevos contornos a la dimensión del derecho a libertad de expresión. Es que, aunque el derecho a **libertad de expresión** ocupe una posición central en el entorno democrático, la propia existencia de la democracia requiere la protección de otros derechos constitucionales que pueden verse socavados por el ejercicio arbitrario de la libertad de expresión, especialmente con el empleo de desórdenes informativas. En el **Plano de Acción Conjunto Contra la Desinformación,** la **Comisión Europea y el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad** consignan que el derecho de participar de manera libre, justa e informada de los procesos políticos es cada vez más desafiado por la difusión deliberada a gran escala, y la difusión sistemática de

desinformación y exigen determinación política y respuestas coordenadas. La **Convención Americana de Derechos Humanos, en su artículo 13**, prevé el derecho a la libertad de expresión y de pensamiento. La cuestión ha sido tratada en la Corte IDH en los casos **Olmedo Bustos y otros (2001), Álvarez Ramos vs Venezuela (2019), Urrutia Laubraeaux vs Chile (2020).** Para la Corte IDH hay una dupla dimensión que debe ser considerada en la libertad de expresión: la social e la individual.

Manifestando preocupación y atención con el fenómeno de la desinformación y su implementación con el propósito de **confundir y afectar los derechos a toma de decisiones** basada en informaciones veraces, que son derechos impactados por la libertad de expresión, el Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión, la Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), el Relator Especial de la OEA para la Libertad de Expresión y la Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP), han publicado **Declaración Conjunta Sobre Libertad De Expresión Y "Noticias Falsas" ("Fake News"), Desinformación Y Propaganda** en que se buscan presentar las características y estándares sobre desinformación, destacando la necesidad de garantizar un entorno posible para la libertad de expresión.

La **Comisión de Venecia**, en el informe "**El impacto del desorden informativo (desinformación) en las elecciones"**, resaltó que la internet cambió la manera como los electores reciben mensajes políticos y que ese cambio puede tornar posible que falsa informaciones se difundan en una escala sin precedentes.

Los casos y los estudios arriba presentados son apenas algunos ejemplos de cómo las cortes electorales han encarado los retos de la desinformación en las campañas electorales y de las dificultades para su enfrentamiento.

III. Microsegmentación y Personalización: de la Injerencia Electoral a la Manipulación Política

Leyre Burguera Ameave
Profesora de Derecho Constitucional
Facultad de Derecho
Universidad Nacional de Educación a Distancia (UNED)
lburguera@der.uned.es

Toda campaña electoral destinada al éxito requiere del conocimiento preciso de quienes son los destinatarios finales del mensaje político. El análisis de los intereses e inquietudes de los electores arrojan claridad para configurar una comunicación electoral efectiva.

Este propósito ha estado siempre presente en la organización de las campañas electorales (a través de encuestas, grupos de discusión, etc.) pero es quizás ahora, con la eclosión del *big data*, cuando somos más conscientes de su potencialidad y de los riesgos que comporta.

Glosario

Existen diferentes estrategias que se utilizan actualmente para influir en los mensajes políticos a través de la desinformación o la manipulación con el objetivo de avanzar en ciertos objetivos políticos, incluido el socavamiento del desarrollo normal de los procesos electorales democráticos. Entre ellas, merece especial atención el uso de técnicas de ***microtargeting*** y personalización de mensajes para diseñar y elaborar la comunicación electoral.

La manipulación política y los intentos de interferir indebidamente en los procesos electorales a través de estas dos técnicas se están dando en todo el mundo desde hace más de una década. Casos paradigmáticos como la campaña de Obama de 2012 o las elecciones parlamentarias indias de 2014, son tan sólo dos ejemplos iniciales que, posteriormente, encontraron en el Reino Unido (referéndum del Bréxit), Francia (elecciones de 2017) o EEUU (campañas de Donald Trump o Hillary Clinton en 2016) un mayor impacto.

Esta situación se debe, en parte, a la expansión del uso de las redes sociales y a que la labor de recogida y análisis de los datos albergados en estas herramientas se ha ido profesionalizando y sofisticando con el paso del tiempo. Por eso, las redes sociales han estado en el centro de las preocupaciones sobre la publicidad electoral dirigida a grupos específicos de usuarios y la falta de transparencia del proceso.

La **microsegmentación** y la personalización del mensaje electoral obedecen a una inercia comunicativa que no tiene por qué concebirse como negativa pues podría favorecer la motivación e implicación política, aumentando la participación de los electores en los procesos electorales.

Ahora bien, su diseño y empleo por parte de los partidos políticos no suele obedecer a esa cándida intencionalidad, al contrario, tratan de mejorar la recaudación de fondos (en los países con financiación de campañas fundamentalmente privada) y movilizar al electorado hasta extremos que pueden llegar a fomentar campañas negativas, polarizando y fragmentando al propio electorado. Además, facilitan la injerencia y el socavamiento de la privacidad y el derecho a la protección de datos personales, así como la creación de las llamadas cámaras de eco y burbujas epistémicas.

Al tratar en el texto los riesgos potenciales de estas dos herramientas, se hará referencia, específicamente, al uso del *big data* y la inteligencia artificial en este campo. La recopilación y tratamiento de datos por parte de las organizaciones políticas con fines de comunicación política junto con el uso de las técnicas modernas antes citadas han generado un amplio debate y preocupación respecto a los límites que deben aplicarse, entre los que se encuentra el derecho a la protección de datos de carácter personal.

Los problemas y desafíos que se van a plantear tienen que ver, principalmente, con dos cuestiones interconectadas: la obtención de los datos necesarios para el diseño de las actuales “campañas guiadas por los datos” en relación con el respeto a la normativa relativa a la protección de datos de carácter personal y la determinación de los usos de esos datos puesta en conexión con las cada vez más frecuentes estrategias organizadas de desinformación. A todo ello, cabría añadir: las vulnerabilidades de las estructuras tecnológicas y sus modelos de negocio, la variedad de dispositivos que permiten la obtención de datos, el desarrollo de la inteligencia artificial, la sujeción normativa de las empresas tecnológicas, etc.

Ahora bien, en el caso específico de la **microsegmentación**, los riesgos asociados a su uso que se van a tratar son: la manipulación política ya que esta técnica disminuye la capacidad crítica de los ciudadanos; y la distorsión del proceso electoral puesto que puede cambiar las reglas y normas de un modo explícito.

En el caso de la **personalización**, los riesgos asociados a su empleo tendrán que ver con la configuración de una limitada visión del mundo ya que individualizan la información que recibe el ciudadano, reduciendo su cosmovisión y retroalimentándola en una suerte de burbuja informativa. De este modo, la capacidad del ciudadano de formarse opiniones y ser capaz de entender o comprender al que piensa diferente, se ve claramente constreñida. En consecuencia, produce una fragmentación social y

política reduciendo la capacidad de diálogo de la sociedad en la que se inserta esta técnica.

En definitiva, preocupaciones que se han ido incrementado, al hacerse públicos determinados casos de tratamiento ilícito de datos personales para influir en la opinión política de los votantes (un caso paradigmático es el de *Cambridge Analytica*), y que ha dado lugar a que, determinados países hayan regulado las cuestiones aquí señaladas, de manera más o menos restrictiva. Es el caso, por ejemplo, de la Autoridad Italiana de Protección de Datos (Garante para la *Protezione dei Dati Personali*) que el 6 de marzo de 2014, emitió su documento «*Provvedimento in materia de trattamento di dati presso i partiti politici e di esonero dall´informativa per fini di propaganda elettorale*». En noviembre de 2016 lo hizo la Autoridad francesa (*Commission Nationale de l'Informatique et des Libertés*) con, entre otros, el título «*Communication politique: quelles sont les règles pourl' utilisation des données issues des réseaux sociaux?*». Y en abril de 2017 la Autoridad británica (*Information Commissioner´s Office*) aprobó su «*Guidance on political campaigning*». Asimismo, el Supervisor Europeo de Protección de Datos emitió el 18 de marzo de 2018 su Opinión 3/2018 sobre «manipulación online y datos personales («EDPS *Opinion on online manipulation and personal data*») y la Comisión Europea, ante la proximidad de las elecciones al Parlamento Europeo de 2019, el 12 de septiembre de 2018 aprobó su guía sobre la aplicación de la normativa europea de protección de datos en el contexto electoral («*Commission guidance on theapplication of Union data protection law in the electoral context*»).

Asimismo, en este texto se van a incluir menciones a los dos principales conceptos antes mencionados: microtargeting y personalización de la política, así como también señalar, la importancia de examinar otros conceptos relacionados, directa o indirectamente, con las dos cuestiones planteadas en esta contribución. De ahí que se atienda, en el trabajo a nociones o ideas como: Web 2.0, red social, perfil, neuromarketing, burbuja epistémica, cámara de eco, *Big data, deep fake, deep learning, datamining, bots*, etc.

De todos los conceptos que hay que tener en cuenta, debemos referirnos en primer lugar al **microtargeting,** también llamado “focalización de audiencia”, “microfocalización” o “microsegmentación” que es definido como la técnica de mercadotecnia que consiste en dirigir mensajes diseñados a medida de las características personales de los destinatarios con el fin de influir en su comportamiento como consumidores. Se trata de dirigir mensajes diseñados a medida a partir de los datos recopilados sobre cada persona en particular, combinados con datos recolectados en otros niveles, con el fin de influir en su posicionamiento político y en su comportamiento electoral.

En cambio, la **personalización de la comunicación** es el uso que se hace de esa estrategia de recolección de datos y que favorece un desequilibrio de poder entre la ciudadanía y los grupos que controlan esos datos ya que abre la puerta a la manipulación informativa y la polarización política.

Casos

Para complementar el significado y aplicación de los términos abordados, se realizará un análisis de la normativa vigente y la jurisprudencia de especial relevancia.

En el plano legislativo, se han dado pasos significativos como la Ley nº 19.884 de 2017 promulgada en Chile, que regula en su art. 2, la propaganda electoral pagada o la Ley electoral de 1993, promulgada en Nueva Zelanda, sección 3ª, que estima que las opiniones políticas personales no son publicidad electoral. También se va a analizar dos códigos electorales, ambos de 2014, que regulan estos términos (microsegmentación y personalización) pero desde distintas problemáticas. En el caso del código electoral de Georgia, su artículo 51.11, incide en estas cuestiones al afectar a los requisitos de los sondeos de opinión pública. Por su parte, el código electoral de Japón, en su artículo 235.5, trata la utilización de nombre falso, castigando con multa o prisión las posibles infracciones.

En el plano jurisprudencial, merece la pena destacar, entre otras, la sentencia 76/2019, de 22 de mayo de 2019 del Tribunal Constitucional español que resuelve el recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo respecto del apartado primero del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del régimen electoral general, incorporado por la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. En ese artículo 58 bis, se exponía que: “1. La recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas”. La indeterminación de la expresión “garantías adecuadas” fue decisiva para que este tribunal estimase la nulidad del precepto legal que posibilitaba la recopilación por los partidos políticos de datos personales relativos a las opiniones políticas de los ciudadanos. Previamente, la Agencia Española de Protección de Datos (AEPD), había emitido la Circular 1/2019, de 7 de marzo, en la que interpretaba el nuevo artículo, fijaba algunos criterios y trataba de establecer algunas garantías. No era suficiente para la envergadura de la polémica planteada en cuanto a la posibilidad de elaborar perfiles ideológicos al servicio de la personalización del mensaje electoral.

Asimismo, también resultará relevante examinar, entre otras, la sentencia de tres de septiembre de dos mil veintiuno, del Tribunal Electoral del Poder Judicial de la

Federación (TEPJF) de México, que estudia un caso de campaña negativa, llegando a afirmar que: “si bien el debate político tiene una protección reforzada, no se debe generar confusión en el electorado o la ciudadanía con la propaganda político-electoral, puesto que ello tiene un impacto negativo en la formación de una opinión consciente e informada para el ejercicio del derecho al voto, lo cual podría generar un efecto vicioso respecto de la configuración del propio sistema político nacional”. Por tanto, el impacto de la desinformación llevada a cabo a través de técnicas concretas de obtención de información y manipulación será el trasfondo que nos haga percibir la envergadura del problema.

También en el caso español, se revisa la doctrina de la Junta Electoral Central (JEC), a partir de la Instrucción dada en 2007 que viene a equiparar los instrumentos o mecanismos comunicativos tradicionales con las nuevas herramientas, sin tener en cuenta su potencialidad. De ahí que, anclada en una normativa con perspectiva ciertamente analógica, no sea capaz de abordar con eficacia e inmediatez, muchos de los retos que se le presentan en cada convocatoria electoral. En esa senda, se analizará, como ejemplo, la Instrucción 1/2021, de la Junta Electoral Central, de 13 de mayo, sobre la difusión de propaganda electoral mediante envíos en los que no sea identificado nominativamente su destinatario (BOE núm. 119, de 19 de mayo de 2021), que viene a interpretar el artículo 39.3 de la Ley Orgánica del Régimen Electoral General (LOREG), modificado por la Disposición Final Tercera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que introduce el derecho de los electores a oponerse a su inclusión en las copias del censo electoral que se faciliten a los representantes de las candidaturas para realizar envíos postales de propaganda electoral.

Con carácter general, y en relación a los términos analizados, son significativos los casos en los que se desestiman las denuncias interpuestas ante la JEC por entender que no incurre en ninguna prohibición la participación en redes sociales (siempre que no suponga ningún tipo de contratación comercial para su realización). La frontera entre publicidad (encubierta o no) e información es difusa, especialmente, cuando se hace mención al ámbito de internet. Se revisan y estudian los acuerdos que abarcan el periodo 2005-2022.

IV. La intervención de terceros en campaña

Rafael Rubio Núñez
Universidad Complutense, Madrid
rafa.rubio@der.ucm.es

La generalización de las tecnologías de información y comunicación (**TICS**) ha transformado la naturaleza de las **campañas electorales**, que han pasado de ser una propuesta comunicativa concentrada en el tiempo, protagonizada por los candidatos y los medios de comunicación, a convertirse en una propuesta comunicativa donde terceros tienen la capacidad de influir de manera directa y eficaz en el resultado final. Este tipo de influencias no son nuevas, y ya existían a través de donaciones y de la participación de los actores públicos en campaña, pero ahora se añaden nuevos sujetos, especialmente los particulares sin una adscripción al partido político o al candidato.

De ahí que, como consecuencia de la generalización del uso de la tecnología en las elecciones se produzca el incremento de la participación de terceros en campaña y su impacto. Aunque, inicialmente, no se trata de un problema propiamente tecnológico, con la tecnología adquiere una nueva dimensión. Tradicionalmente la participación de actores ajenos al proceso electoral en las campañas electorales se vinculaba casi exclusivamente a la financiación de las campañas electorales por parte de terceros, ya sea contribuyendo con la campaña oficial u organizando campañas sobre temas específicos, con ánimo de influir en la agenda de los candidatos. A estas formas de participación de particulares y grupos de la sociedad civil deberíamos añadir también la intervención de funcionarios del gobierno (que deberían permanecer neutrales en el proceso) o de los medios de comunicación (cuyo papel se ha venido regulando de manera cada vez más exhaustiva), que aunque son objeto de regulación desde hace tiempo, ven su papel modificado como consecuencia de la tecnología.

La aparición de estos nuevos actores, o la transformación del papel de algunos de los actores tradicionales sin una vinculación directa con las candidaturas plantea nuevos interrogantes a la regulación existente. Es necesario ofrecer respuesta jurídica a nuevas situaciones como la actuación de los particulares, o las organizaciones sociales que impacta a la elección, la posibilidad del anonimato; el papel de actores extranjeros en los procesos electorales; el uso de *bots* que pueden amenazar la equidad de la contienda electoral.

Si, como sostenía Sartori (1993:76-77), "(l)a autonomía de la opinión pública (…) entra en crisis, al menos en una crisis de vulnerabilidad, con la aparición de la radio, y más aún con la televisión", con las nuevas tecnologías de la información, el concepto de opinión pública se

transforma radicalmente, convertida en un *puzzle* de opiniones de grupo, sin aparente relación entre sí, lo que hace imposible el diálogo que es la esencia de la idea misma de la conformación de la opinión pública.

Glosario y casos

Tradicionalmente se ha considerado la participación en campañas de medios de comunicación, candidatos, partidos políticos y autoridades. Todos los demás actores políticos se entendían ajenos a la misma, o irrelevantes en su actuación. La irrupción de las tecnologías de la comunicación altera el terreno de juego y la adaptación de estos actores les otorgan un papel diferente.

En primer lugar, destaca por su abundancia el uso que las autoridades y organismos públicos están haciendo de estas plataformas en campaña. Al aumentar la frecuencia de su comunicación y las formas de difusión de sus actuaciones pueden desequilibrar con más frecuencia, e incidencia, de manera directa y en el momento de mayor impacto, la contienda electoral, tanto a través de publicaciones como de la contratación de publicidad, afectando a la equidad del proceso, con riesgo de malversación de fondos públicos.

Sobre este punto, quizás el más habitual pero también el menos novedoso al ser previo a internet, se han manifestado organismos electorales como la JEC o el TEPJF. Por un lado resulta interesante ver como en México el TEPJF (SUP-RAP-288/2009, SUP-RAP-318/2012) ha extendido a dirigentes, afiliados, militantes y simpatizantes de los partidos políticos las obligaciones constitucionales en torno de la propaganda política y electoral en materias como la obligación de abstenerse en el debate político y electoral de denigrar a las instituciones y partidos así como de calumniar a las personas a “cualquier lectura en el sentido de que esa obligación sólo constriñe a los partidos políticos resulta inaceptable”.

Por otro lado, más numeroso, estaría la prohibición de las campañas de logros en actos públicos difundidos por la web o publicaciones electorales en las cuentas y páginas oficiales de ayuntamientos, ministerios o la presidencia (JEC entre otras: **196/2011; 206/2011; 459/2015; 601/2015; 166/2016; 212/2016; 293/841; 293/842; 293/863; 293/864; 293/869; 293/880; 293/882; 293/891; 293/892; 293/898; 293//901**). Este también es un fenómeno habitual en México, donde desde un comienzo se plantea la obligación de neutralidad de las autoridades, también en las redes sociales, (**SUP-RAP-57/2010; SUP-RAP 105/2014**) y donde la actuación del presidente López-Obrador ha sido objeto de especial atención por parte del **TEPJF (SUP-REP-139/2019 y acumulados; SUP-REP-142/2019; SUP-REP-185/2020; SUP-REP-193/2021; SUP-REP-312/2021 y acumulados; SUP-REP-382/2021 y acumulados**).

Algo similar ocurre con los medios de comunicación, cuya definición se difumina, hasta perder el monopolio de la información electoral. Como anticipaba Cotino (2008) hace ya 15 años "(l)os tradicionales medios de comunicación de masas bien dejan de ser un pilar básico en el sistema democrático o bien, y cuanto menos, dejan de ser el único pilar básico. El edificio democrático se sostiene con muchos otros "pilares" en la red". La extensión a estos de la protección y las obligaciones de las que gozan los medios de comunicación se está replanteando con el surgimiento de "medios" exprés, o "pseudomedios", que aprovechando las facilidades de internet para crear sitios web *adhoc* y dotarles de la apariencia de un medio de comunicación.

Estas plataformas informativas, que aparecen y desaparecen según el calendario electoral, se apoyan en un espacio en la web, con la única intención de revestirse de la apariencia de fiabilidad de la que gozan los medios de comunicación para reforzar la credibilidad de determinadas informaciones, distribuidas habitualmente a través de las redes sociales con la participación de redes coordinadas de activistas y *bots*, lo que les permite distribuir información política distorsionada con la "garantía" de ser considerados medios de comunicación. Muchos de estos "pseudomedios" que difícilmente cumplen con los estándares habituales de rigor, necesarios para el ejercicio de la profesión periodística, se convierten en las fuentes de información más distribuidas durante la campaña, como ocurrió con la campaña presidencial norteamericana de 2016, con medios creados y gestionados desde un pequeño pueblo de Macedonia, Veles (Peirano, 2019) o las elecciones presidenciales francesas del año 2017, donde medios como *Sputnik* o *Russia Today*, tras crear una versión en francés para las elecciones, se colaron entre los más consultados durante todo el proceso, con más de 2 millones de interacciones en un mes. Un fenómeno particular, habitualmente relacionado con los medios, es la publicación de información no permitida en determinados periodos como los resultados antes del cierre de las urnas o las encuestas, días o incluso semanas antes de la elección. Así ocurrió en **Costa Rica (ST. Corte Suprema, 2018**), donde para difundir resultados de encuestas hay que estar autorizado.

Junto a la transformación del papel de los actores tradicionales, la aplicación de la tecnología a las campañas electorales permite, como hemos visto, la aparición de nuevos actores que pueden influir en la campaña e incrementa su impacto. Como señalaba Clift ya en (2007) "algunos individuos y grupos informales pueden utilizar internet para influir en los resultados electorales, de manera independiente de los partidos". Como hemos visto, hoy difundir información a favor en contra de una opción política, sin vinculación con las campañas oficiales, con mayores índices de audiencia e impacto está al alcance de muchos. Cualquiera puede publicar un mensaje de apoyo o crítica en sus redes sociales, re difundir mensajes oficiales de campaña o incluso pedir el voto a sus seguidores…. pero hoy estas actividades pueden influir en los resultados de las elecciones. Aumenta así la descentralización de las campañas

electorales, que se parecen cada vez más a un intercambio donde muchos emisores comunican con muchos receptores en diferentes plataformas sociales.

De ahí que, junto a los candidatos, los partidos políticos y los medios de comunicación, los "sospechosos habituales" de la regulación electoral vigente, sea necesario prestar atención al papel de organizaciones e individuos sin una vinculación formal con las candidaturas y al papel de las plataformas en las que estos individuos difunden información relacionada con la campaña. Estos nuevos actores pueden ser reales, como los *influencers* que, de manera voluntaria o lucrativa han comenzado a utilizar sus redes para apoyar determinadas candidaturas políticas, o creadas de manera artificial por organizaciones estatales como el *Internet Research Agency* ruso (IRA) que, durante la campaña presidencial norteamericana de 2016, creo decenas de grupos para promover la inestabilidad del proceso. Una muestra de 6 de ellos realizada por Jonathan Albrighth (*Tow Center for Digital Journalism*) señala a la generación de más de 340 millones de interacciones durante el proceso (Peirano, 2019).

El **derecho al voto (a votar y ser votado)** guarda una relación directa con la campaña electoral que, en términos jurídicos, se desenvuelve en un continuo equilibrio entre la **libertad de expresión y de asociación**, derecho que se ve reforzado en el ámbito político y especialmente en la campaña electoral, y la equidad de la campaña. Así lo señala la Corte IDH (2004, párrafo 88), "(E)l ejercicio de los derechos políticos y la libertad de pensamiento y de expresión se encuentran íntimamente ligados y se fortalecen entre sí", pero no podemos obviar que esta participación de terceros, amparada en el ejercicio de sus derechos fundamentales, puede afectar a la **equidad** en la contienda, que pretende que los candidatos tengan oportunidades semejantes, y afecta por tanto a otros derechos fundamentales como el derecho de sufragio. La inequidad está estrechamente relacionada con la **libertad del sufragio**, asumiendo que una mayor exposición de una candidatura condiciona la participación libre del elector, y con la autenticidad del mismo, evitando interferencias que distorsionen la voluntad ciudadana; en el caso, dotando de certeza sobre el origen, destino y límite de los recursos empleados en las campañas políticas, para evitar que las opciones políticas obtengan ventajas indebidas.

El **derecho al voto** exige una intervención activa para asegurar las condiciones en las que el electorado puede formar y expresar libremente su opinión y elegir a sus representantes. La libertad de expresión (especialmente en el debate político) y las elecciones libres son derechos que se necesitan mutuamente, pero no hay duda que, en ocasiones, la equidad electoral puede entrar en conflicto con la libertad de expresión de terceros. Así, resulta imprescindible adecuar el marco jurídico a las obligaciones legales en materia de libertad de expresión con las nuevas dinámicas de campaña electoral. En este nuevo contexto garantizar las condiciones para un entorno de campaña equitativo en el escenario digital implica una serie de dificultades

añadidas, que permitan mantener a salvo la libertad de expresión sin perjudicar el principio de equidad.

De esta manera, la regla general ha sido considerar estas actividades de particulares durante la campaña electoral como ejercicio de la **libertad de expresión**, entendiendo este comportamiento como una conducta espontanea, libre e individual, amparado en la dificultad que estos particulares tienen para incidir de manera decisiva y, en el caso que esta capacidad exista, la legitimidad de su actuación pública. El problema se plantea en casos donde se pueden plantear dudas sobre la espontaneidad de estas actuaciones, con **interferencias** tanto en el plano interno como por parte **de actores extranjeros**. Estas actividades pueden detectarse de manera clara cuando existe un pago por estas intervenciones y con más dudas cuando existen formas de actuación coordinada que pudiera implicar relación con la campaña, afectando a la **limpieza y equidad de la elección**.

La generalización de la **web 2.0**, con la extensión del **contenido generado por el usu**ario (blog **post**, videos, fotos…) facilita la participación de particulares con capacidad de influencia (***influencer***). Aunque tampoco es algo nuevo. En *Time, Inc. V. Firestone*, 424 U.S. 448 (1976), la Corte Suprema señala como figura pública a aquellos que gocen de especial relevancia en la percepción de la sociedad; capacidad para ejercer influencia y persuasión en la discusión de asuntos de interés público y desarrollen una participación activa en la discusión de controversias públicas específicas con el propósito de inclinar la balanza en la resolución de las cuestiones implicadas.

Esta capacidad de influencia amenaza así la regla general, especialmente cuando se generaliza y se extiende el número de personas a las que se supone capacidad de influencia en las redes sociales, o realizan estas conductas fuera de ellas, amplificando sus efectos a través de estos canales (**SUP-REC-1874/2021 y SUP-REC-1876/2021 y acumulados**), especialmente cuando lo hacen de manera retribuida y coordinada a través de **campañas de influencia**. En esta línea se han manifestado distintos organismos electorales, muy especialmente el INE y el TEPJF respecto a la prohibición de este tipo de campañas de apoyo durante la veda electoral, con motivo de campañas de apoyo al partido verde en las elecciones de 2015 y 2021, durante la veda electoral, y sobre la obligación de reportar los gastos realizados en esta materia, a efectos de transparencia y de calcular el tope electoral (**SUP-REP-542/2015 y acumulado y SUP-RAP-172/2021**), al tratarse de acciones coordinadas y en las que se demostró el pago a algunos de los participantes.

También **el ST. Tribunal Regional Electoral, Río de Janeiro, 2018** obligó a la retirada de los posts publicados por unos ***bloggers*** señalando su deseo de postulación de un candidato determinado antes del inicio de la campaña electoral. Merece la pena destacar otras tres sentencias **del TEPJF (SUP-REC-00887-2018 y**

SUP-RAP-180/2021 y acumulados[7] **y SUP-REC 143/2021**) en las que se abre la puerta a que este tipo de terceros puedan realizar apoyos específicos siempre que no reciban ningún tipo de remuneración a cambio, estableciendo una suerte de presunción de espontaneidad.

En este contexto surgen también comportamientos inauténticos como forma de influencia electoral de nuevos actores. Estos se basan, en gran medida en el **anonimato**, facilitado por la tecnología. Desde el anonimato, los terceros que estamos estudiando podrían llevar a cabo campañas, que aprovecharían la libertad de no estar sometidos a la regulación electoral para traspasar las reglas de la campaña electoral tanto en la parte de contenido, con campañas negativas, o la publicación de información no permitida en tiempo de veda, evitando la fiscalización que ya hemos señalado cuando estas actuaciones corren a cargo de personas con capacidad de influencia demostrada. Este anonimato dificulta la identificación, hasta hacerla imposible, abre la puerta a la **suplantación de identidad** y plantea una complejidad adicional para el control y la imputación de responsabilidades ante la infracción de las prohibiciones establecidas.

Así, es necesario identificar a los sujetos que realizan actividades con repercusión electoral como la creación de páginas informativas que divulgan información falsa sobre candidatos o contratan publicidad política en campaña. Se plantea así la transparencia sobre la persona o el grupo que lo está financiando, y la forma de hacerlo. Encontramos algunos ejemplos de este tipo de campañas, y la respuesta ofrecida por los organismos electorales, en la decisión de la **JEC de España (688/2019)** sobre la campaña promovida, supuestamente por personas que fingían ser sus simpatizantes para desincentivar el voto a las candidaturas rivales, o la **Sentencia del Tribunal de Sao Paulo (2015)** por la que Twitter debía proporcionar al candidato datos de los usuarios que le difamaron en dicha red social, en la misma línea que la sentencia del **Tribunal Supremo de Illinois (2015) y,** de manera documentada y sistemática**, el *Report On The Investigation Into Russian Interference In The 2016 Presidential Election* del Departamento de Justicia de los Estados Unidos. Sin embargo, en otros casos como la plataforma "Voto útil",** que proporcionaba herramientas para identificar a la opción política con mayores probabilidades de vencer a los candidatos de Morena en las elecciones federales del 6 de junio de 2021, al ofrecer información pública y no existir ningún tipo de vinculación se consideró ajustada a la normatividad electoral **(SUP-REP-319/2021)**.

Muy relacionado con el anonimato se encuentra la utilización masiva de ***bots***, cuentas "falsas", anónimas y automatizadas, que se presentan en las redes como un usuario

[7] https://www.te.gob.mx/sentenciasHTML/convertir/expediente/SUP-REC-00887-2018 y https://www.te.gob.mx/EE/SUP/2021/RAP/180/SUP_2021_RAP_180-1083242.pdf

más con el objetivo de aumentar el volumen de distribución de determinada información, buscando que esta parezca mayoritaria, creando de manera artificial una corriente de opinión, de aceptación o rechazo a determinadas ideas o personas (Sánchez Muñoz 2020: 34-40). Aunque las plataformas los tienen en su punto de mira y actúan de manera habitual para eliminarlos de la arena pública la facilidad para crearlos y gestionarlos a través de mecanismos de inteligencia artificial ha planteado una auténtica guerra tecnológica, a la que los Estados asisten como meros espectadores, mientras las decisiones de las plataformas, habitualmente sin un procedimiento ni claro ni garantista, pueden poner en jaque los derechos fundamentales de particulares implicados, que ven como sus cuentas son eliminadas, sin poder hacer nada para evitarlo o recuperarlas. Otro tipo de amenaza en esta línea es la de los ***trolls***, que desde sus cuentas personales, el anonimato o el uso de cuentas falsas, contaminan la conversación en la red, llegando en ocasiones a la amenaza o la violencia física, muchas veces a través de campañas coordinadas de comportamiento no auténtico.

La compra de **publicidad política** (***electionering*)** en las redes también puede plantear problemas relacionados con su contratación por parte de terceros. Existen países como **Albania** que prohíben la contratación de publicidad electoral a aquellos sujetos que no participen en las elecciones (**Código Electoral de 2012, art. 84**) o **Canadá** que distingue la publicidad de la opinión personal expresada en redes (**Ley Electoral, sección 319**) pero esta prohibición no es universal, y siempre existe, además, la posibilidad de contratar publicidad en tiempo electoral con intención electoral, aunque no se identifique como tal. Si, en el caso de campañas de apoyo a una candidatura no hay duda sobre la aportación en especie, y la necesidad de contabilizarla como tal, el problema se complica cuando se trata de campañas de ataque a otros candidatos como las sucedidas en Colombia durante la última campaña presidencial, o de publicidad temática, que no se identifican directamente con ninguna candidatura.

En estos casos se plantean nuevos conflictos relacionados con la coordinación, o falta de esta, de estas actuaciones con la campaña oficial, o con el sometimiento de estas campañas publicitarias a los plazos electorales que restringen la publicidad a tiempo de campaña oficial y prohíben la misma en periodos de veda o reflexión electoral. Esta compra afecta a terceros ajenos a la campaña (***Report On The Investigation Into Russian Interference In The 2016 Presidential Election*** **del Departamento de Justicia de los Estados Unidos, JEC de España (688/2019)** ***o Recurso em Representação*** **nº 060147858** y el ***Agravo Regimental em Recurso Especial Eleitoral*** **nº 060505606** resueltos por el **Tribunal Superior Electoral de Brasil**. También a la compra de publicidad de medios o pseudomedios de comunicación, que fingen publicitar su contenido para tratar de influir en la campaña (**Costa Rica, XX**) y también a la compra por parte de entidades gubernamentales, que de esta manera intervienen de manera impropia en la campaña.

La actuación de terceros durante la campaña también afecta a las decisiones de las plataformas, cuando de manera coordinada con los organismos electorales o por propia iniciativa, adoptan decisiones que restringen esta libertad de expresión como el cierre o la suspensión de cuentas, o la eliminación de contenidos determinados, sin un procedimiento conocido previamente, lo que abre la puerta al abuso y la arbitrariedad, especialmente cuando estas decisiones se adoptan de manera automatizada por algoritmos opacos. Estas actuaciones, a las que muchas veces los Estados asisten como espectadores, se adoptan sin las garantías necesarias para proteger los derechos afectados como si el tratarse de empresas privadas les eximiera del respeto a los derechos fundamentales. Para garantizarlos estas decisiones deberían ser adoptadas, al menos en periodo electoral, por los organismos electorales o al menos realizarse a través de un procedimiento claro, transparente y sin discriminación en el que exista la posibilidad de recurrir la decisión, e incluso la obligación de dar respuesta motivada a la misma, susceptible de ser sometido a posteriori al control de una autoridad judicial.

Actualmente se da la paradoja que al tratarse de particulares estos cierres no se consideran materia electoral, y no gozan de la protección de los organismos electorales cuya actuación se limita a casos de cuentas relacionadas con los partidos y los candidatos como el cierre de la cuenta oficial en Twitter del partido político Vox durante las elecciones catalanas (2021) o la eliminación de los canales de WhatsApp de todos los partidos políticos en las elecciones generales de abril de 2019. En el caso de la contratación de publicidad de terceros, ante la ausencia de una regulación clara, las plataformas optaron inicialmente por etiquetar como política, la publicidad de esta naturaleza, y ofrecer información sobre las personas que han pagado esa publicidad (para que los organismos electorales puedan considerar estos pagos como contribuciones a la campaña e incluirlos en los informes y aplicarlos al techo de gasto). En algunos países las propias plataformas han terminado por prohibir la contratación de publicidad electoral a cualquier actor que no forme parte oficialmente de la campaña (partidos y candidatos) a los que exigen una identificación especial.

Además, es importante señalar que todas las conductas señaladas anteriormente pueden realizarse desde dentro o desde fuera del espacio donde se celebran las elecciones. Se trata de la actuación de individuos, grupos, o incluso medios de comunicación, situados «virtualmente» fuera de nuestras fronteras, que desde su “extraterritorialidad” pueden llevar a cabo acciones no permitidas destinadas a influir en el proceso electoral (**campañas de interferencia**). Este fenómeno, que se puso de manifiesto de manera evidente por primera vez en la campaña presidencial norteamericana de 2016, con la demostrada injerencia rusa, se ha ido acrecentando desde entonces (Oxford 16 en adelante), y plantea retos a la regulación existente con la compra de publicidad en las plataformas digitales durante la jornada de reflexión (veda electoral), o la publicación de información electoral, como el resultado de los

sondeos a pie de urna, durante la misma jornada electoral, algo habitualmente prohibido.

Estas campañas también aprovechan su anonimato para promover acciones de ***astroturfing*** desde perfiles falsos, mucho más difíciles de controlar. Aunque las plataformas han comenzado a tomar medidas para evitar estas injerencias externas este tipo de intervención plantea nuevos problemas de control, prueba y adopción de medidas y se plantea cada vez con más fuerza la prohibición de cualquier tipo de acción con contenido electoral desde el extranjero (identificada o anónima, legal o ilegal) para lo que resulta imprescindible la colaboración de las plataformas.

Conclusiones

Todo lo anterior plantea un debate sobre el papel de ciudadanos y grupos en la campaña electoral y el establecimiento de obligaciones y límites a sus actividades, en lo que se refiere a la petición del voto (campañas no oficiales), críticas a partidos o candidatos (campañas negativas), envío de información no solicitada a sus contactos o contratación de publicidad en apoyo o en detrimento de una opción determinada..., ya que más allá del ejercicio legítimo de la libertad de expresión estas nuevas posibilidades de participación en la campaña abren la puerta a nuevas estrategias de partidos y candidatos, que pueden apoyarse en terceros para llevar a cabo acciones que por su contenido, por el momento que se realizan o por su coste, no pueden ejecutar en nombre propio. Además, se abre otra posibilidad a que grupos independientes de partidos y candidatos, sin ninguna conexión, quieran incidir en los resultados en ejercicio legítimo de su libertad de expresión, en defensa de sus ideas y/o intereses, algo que, realizado a gran escala, puede afectar a la equidad en la campaña y crear una zona de sombra en la regulación electoral existente.

Hasta la fecha, la respuesta está centrada en el control financiero, indispensable para garantizar la equidad. En periodo electoral, para garantizar la igualdad de oportunidades entre las fuerzas políticas, los gastos de la campaña electoral se establecen límites de gasto, y se exige una mayor transparencia de esta financiación obligando a los actores implicados a proporcionar información sobre los gastos de campaña durante las elecciones, mejorando la eficacia de la supervisión de la fiscalización de las campañas electorales y estableciendo sanciones para los incumplimientos en esta materia que pueden van desde la exclusión de una candidatura, la anulación de la elección, hasta la pérdida total o parcial de la financiación pública. Al incluir dentro de esta fiscalización las actuaciones de terceros, que han sido objeto de pago o que se consideran realizadas por una expectativa futura, se trata de igualar el terreno de juego, no sin dificultades, como veremos más adelante.

De ahí que sea necesario definir de forma clara la respuesta de las autoridades electorales ante la actuación de terceros en los procesos electorales en un momento en el que pueden ser determinantes, ofreciendo un marco jurídico adecuado.

V. Discurso del odio y violencia política de género

Ignacio Álvarez Rodríguez
Profesor Contratado Doctor de Derecho Constitucional
Facultad de Derecho
Universidad Complutense de Madrid
ialvarez1@ucm.es

Es importante llegar a un consenso académico mínimo en torno al objeto de estudio, pues los expertos señalan que es demasiado amplio. Nos basamos en tres instituciones que han elaborado documentos de trabajo esclarecedores sobre el particular Una es el *National Democratic Institute*. Otra es el *Observatorio de Reformas Políticas en América Latina (1978-2021)*, adscrito al Instituto de Investigaciones Jurídicas (IIJ-UNAM) y a la Organización de los Estados Americanos. La tercera es el *Instituto Nacional Electoral de México*.

Glosario

Para explorar el encaje jurídico de la llamada violencia política de género (VPG) durante la campaña electoral es necesario emplear una serie de términos técnicos tal que vienen recogidos en el Glosario.

En primer término, destaca la ***ciberdelincuencia***, también llamada en ocasiones *cibercrimen*, noción que comprende toda actividad delictiva o ilegal que se realiza a través de Internet. Por poner algunos ejemplos, dentro de ella se engloba el *phishing*, el uso indebido de información personal, diferentes formas de piratería informática, el discurso de odio y la incitación al terrorismo, e incluso la distribución de pornografía infantil y de prácticas sexuales con menores. Este tipo de delitos tienen lugar respecto de todos los dispositivos digitales, incluidos ordenadores, tabletas y teléfonos inteligentes que están conectados a la Internet.

En segundo término, debemos destacar la ***desinformación de género***, esto es, el uso de información falsa para confundir o engañar mediante la manipulación del género como una divisoria social fundamental para atacar a las mujeres y/o influir en los resultados políticos.

En tercer lugar, destaca el concepto de ***discurso de odio***, que cubre muchas formas de expresiones o ataques que difunden, incitan, promueven o justifican el odio, la violencia y la discriminación contra una persona o grupo de personas por las más variadas razones. También abarca el discurso polarizador que promueve la intolerancia, el odio y la incitación a la violencia mediante referencias explícitas o indirectas a la raza, el origen nacional o étnico, la religión, el género, la orientación sexual, la edad o la discapacidad u otras agrupaciones inmutables, generalmente con

el objetivo de generar una diferencia tangible en una institución, organización o sociedad.

En cuarto lugar, tenemos los llamados ***trolls*** de Internet. Los trolls son usuarios humanos que intencionalmente acosan, provocan o intimidan a otros, a menudo para distraer y sembrar la confusión o la discordia. Los trolls pueden actuar como individuos y, en este sentido, comparten muchas características de quienes ejercen el discurso de odio en formatos analógicos. También cabe que actúen mediante comportamientos coordinados con otros trolls.

En quinto lugar, debemos resaltar la ***violencia en la Red contra la mujer dedicada a la política***, definida como todas las formas de agresión, coerción e intimidación de mujeres en el ciberespacio simplemente porque son mujeres. También se le conoce como ciberviolencia contra la mujer. El fenómeno se exacerba al hacerse en Internet porque las candidatas políticamente activas enfrentan diversas amenazas de otros candidatos, partidos y/o ciudadanos.

Normativa internacional y nacional

Existe cierto respaldo internacional a la persecución de conductas violentas contra las mujeres en política, tanto desde el Derecho Internacional Universal (Organización de Naciones Unidas) como desde el Derecho Internacional Regional (Unión Europea, Consejo de Europa, Organización de Estados Americanos).

Otro tanto puede decirse de varios países a nivel individual, aunque el apoyo es más parco y, cuando se produce, bastante vago e impreciso. Algunos gozan de legislación específica en la materia o han intentado aprobar iniciativas de este porte (Chile, Argentina, Alemania, Bolivia, Bosnia Brasil, Ecuador, El Salvador, México, Panamá, Paraguay) y otros tienen legislación no específica pero aplicable a tales supuestos gracias a la tipificación penal del discurso del odio (España).

Ejemplos de Constituciones:

1. Propuesta de Texto Constitucional para Chile, 2022 (rechazado en referéndum en septiembre del mismo año), artículo 27: “1. Todas las mujeres, las niñas, las adolescentes y las personas de las diversidades y disidencias sexuales y de género tienen derecho a una vida libre de violencia de género en todas sus manifestaciones, tanto en el ámbito público como en el privado, sea que provenga de particulares, instituciones o agentes del Estado. 2. El Estado deberá adoptar las medidas necesarias para erradicar todo tipo de violencia de género y los patrones socioculturales que la posibilitan, actuando con la debida diligencia para prevenirla, investigarla y sancionarla, así como brindar atención, protección y reparación integral a las víctimas, considerando especialmente las situaciones de vulnerabilidad en que puedan hallarse”.

2. Constitución de Ecuador: artículo 50.7: “El Estado adoptará las medidas que aseguren (…) protección frente a la influencia de programas o mensajes nocivos que se difundan a través de cualquier medio, que promuevan la violencia, la discriminación racial o de género, o la adopción de falsos valores”.
3. Constitución de Kenia, artículo 33.2: “El derecho a la libertad de expresión no se extiende a las siguientes manifestaciones: a. Propaganda para la guerra, b. Incitación a la violencia, c. Discursos de odio, o d. Proselitismo del odio que i. Constituya una incitación contra una etnia, una humillación de otros o una instigación a causar daños, o ii. Esté basada en algún motivo de discriminación especificado o contemplado en el apartado 4 del artículo 27” (donde se incluye el sexo).

Ejemplos de Legislación:

1. Alemania: Ley de 2017 que obliga a las plataformas a retirar contenidos potencialmente delictivos en menos de 24 horas. La misma ley adicionalmente obliga a eliminar el discurso “obviamente ilegal”, también en plazo de 24 horas, a contar desde que se realiza la denuncia.
2. Argentina: Ley de 2019 que castiga específicamente la VPG, incluyendo sanciones tales como la advertencia previa, la comunicación de los hechos al lugar de trabajo del “agresor”, o la “asistencia obligatoria a programas reflexivos, educativos o terapéuticos tendentes a la modificación de conductas violentas”.
3. Bosnia-Herzegovina: Ley de 2006 que prohíbe del uso de cualquier lenguaje, fotos, símbolos, audios o videos que inciten a violencia o difundan odio.
4. España:
    - Ley Orgánica 1/2015, de 30 de marzo, de modificación del Código Penal: castiga penalmente el discurso del odio.
    - Ley 15/2022, de 12 de julio, Integral para la Igualdad de Trato y la No Discriminación: conmina a los poderes públicos a prevenir y fomentar la denuncia de cualquier tipo de violencia y de discurso del odio.

Casos relevantes

Dentro de los casos existentes, podemos diferenciar entre aquellos que han dado pie a pronunciamientos en vía administrativa y pronunciamientos en vía judicial.

Pronunciamiento en vía administrativa

1. España: denuncia realizada por el partido político *Plataforma per Catalunya (PxC)* en 2015, contra un colectivo autoproclamado "antifascista", por publicar en Internet que aquel defendía ideología nacionalsocialista y fascista. Los hechos, a juicios de la formación, constituían delito electoral. La Junta Electoral Central, en el Acuerdo 196/2015, de 13 de mayo, comunicó que, de conformidad con el artículo 151 de la LOREG, corresponde a los tribunales ordinarios -y no a la Junta Electoral Central- determinar la existencia y autoría de los presuntos delitos a los que se refería la formación.
2. México:
    a. TEPJF, Sentencia SUP-REP-70/2021: las quejas por VPG deben ser tramitadas en instancia por los órganos electorales administrativos (UTCE-INE).
    b. TEPJF, Sentencia SUP-REP-158/2020: confirma que las UTCE-INE son competentes para tramitar denuncias por VPG y recuerda que debe mediar nexo causal entre la alegación de presunta VPG y la competencia material de tales órganos.

Pronunciamiento en vía judicial

Se han detectado decenas de casos donde los altos tribunales de un mismo país (México) se han pronunciado específicamente sobre la VPG. Los pronunciamientos tienden a proteger a la mujer, siempre que los hechos y las pruebas así lo permitan, jurídicamente hablando, aunque en otras sentencias los tribunales han decantado la balanza en contra. Esto debería inducir a reflexión, pues demuestra que transformar la ideología política en Derecho no siempre da resultado.

Bosquejo de casos (todos TEPJF):

1. Sentencia SUP-REC-91/2020, donde se ventila el asunto de la licitud de una lista negra de personas que cometen VPG. El Tribunal entiende que dicha lista es constitucional en la medida en que encuentra justificación en el deber de las administraciones públicas de erradicar la VPG. La minoría discrepante emite un duro voto particular donde achaca a sus colegas realizar "una política judicial inquisitorial inadecuada".
2. Sentencia SUP-REC-61/2020, donde se distingue entre los llamados actos de violencia política de los actos de VPG y añade que si existe denuncia de VPG se debe notificar personalmente a los involucrados (a todos) en un plazo máximo de 48 horas.

3. Sentencia SUP-JDC-156/2019, donde se obliga a la administración electoral a que reevalúe una denuncia por VPG en contra de una servidora pública que en instancia no obtuvo resarcimiento.
4. Sentencia SUP-REC-594/2019, donde se pone en relación la VPG frente a la inviolabilidad parlamentaria. La decisión de fondo dictamina que las expresiones presuntas violentas están cubiertas a la vez que correspondería al Congreso sancionarlas. Un voto particular recuerda que la inviolabilidad parlamentaria es asunto de constitucionalidad, no de legalidad.
5. Sentencia SUP-REC-1388/2018, donde se estudia la VPG vertida en varios videos de Facebook, se da la razón a la demandante y se incluye en el fallo una serie de medidas para resarcir a la víctima (publicar en prensa que ha sido sometida a VPG y elaborar un protocolo por la administración pública competente para prevenir y erradicar estas conductas).
6. Sentencia SUP-REC-531/2018, que confirma la licitud de la anulación de una candidatura electoral por concurrir expresiones de VPG.

Casos señeros:

1. TEPJF: Sentencia SUP-REP-140/2020. VPG en su modalidad de violencia digital. Una candidata presenta una queja por las expresiones utilizadas en un video de Facebook. La Sala Especializada entendió que efectivamente tal violencia sucedió, incluso aunque la legislación nacional de aquel momento no sancionara la misma, pues diversas normas internacionales, de Derecho Comparado e incluso jurisprudenciales sí lo hacían. La minoría de la Sala Superior discrepa del parecer mayoritario por su vaguedad e imprecisión.
2. TEPJF: Sentencia SUP-JDC 111/2019, de 3 de julio. Da la razón al hombre denunciado. Este había colgado en Twitter un video y un artículo criticando la gestión de la dirigente, cosa que también publicó en diversos portales periodísticos. Las palabras exactas fueron: (la dirigente) “desestabiliza y divide al partido”; excluye de la candidatura a personas como él por ser “críticos de ese gobierno tramposo”; que “divide a MORENA -el partido- y que deje la presidencia”; la compara con Luis XIV y dice que “perdió la brújula”.
3. TEPJF: Sentencia SUP-REP27/2019. Candidata denuncia por VPG a hombres que difunden una entrevista en redes sociales que no la deja -estima ella- en buen lugar. Funda su demanda en que el ataque se produce “por el mero hecho de ser mujer”. Se sanciona a un hombre con más de ocho mil dólares pero la Sala Superior la anula porque se vulneró su derecho a un juicio justo.
4. TEPJF: Sentencia SUP-REP-623/2018. Candidato difunde un video en redes sociales donde se tilda a otra candidata de “Bruja de Blancanieves” y de que, de votarla, se estaría votando en verdad a su marido. La Sala Regional Especializada entendió que los estereotipos son discriminatorios y, en

consecuencia, constituyen VPG, extremo que confirma la Sala Superior por "subordinar y minimizar las capacidades de la candidata para la vida política".

5. TEPJF: Sentencia SUP-REP-617/2018. Candidata denuncia por VPG contra otro candidato porque en una discusión pública en Facebook este le dijo: "te enseñé cómo se debe trabajar; pobrecita das risa y lástima; infeliz y frustrada". En primera instancia, la Sala Especializada reputa tales expresiones como VPG. Sin embargo, en segunda instancia la Sala Superior tumba dicha decisión por entender que las frases no constituían ilícito alguno, atendiendo tanto a lo dicho como al contexto donde se dijo, amén de la trayectoria en su día conjunta de ambos, que finalizó con cajas destempladas.
6. TEPJF; Sentencia SUP-REP-121/2018 y Sentencia SUP-REP-142/2018. Candidata denuncia a ciudadano por manifestaciones vertidas en Facebook y en un blog que podían constituir VPG. El órgano electoral dicta medidas cautelares y ordena al ciudadano su retirada. Ante la negativa de este, le multa, recurrida ante la jurisdicción que dicta las resoluciones referidas, por entender que se vulnera su derecho a la libertad de expresión. La Sala Superior confirma los criterios del INE y niega la razón al demandante.
7. TEPJF; Sentencia SUP-JDC-383/2017. Candidata denuncia ser sometida a VPG por las siguientes expresiones vertidas en redes sociales (sobre todo, Twitter): "¿Delfina es nombre propio? ¿O así le dicen por como la trata quien la nombró y es su jefe?". Segunda expresión: "Títere". Tercera expresión: "Desastre de gestión como presidenta municipal". Cuarta expresión: "Lamentable que un titiritero quiera gobernar el Estado de México". La Sala Superior del TEPJF sentenció que las manifestaciones no constituyen VPG ni estaban dirigidas a la demandante por ser mujer ni le afectaban de forma desproporcionada. Aunque los actos fueran ofensivos, continúa la resolución, eso no significa que sea violencia política contra alguien. Además, añade el Tribunal, en los procesos electorales los candidatos deben tener más tolerancia a las críticas desabridas, duras o fuertes pues existe un interés general mayor que es el que satisface la libertad de expresión y, especialmente en este caso, la libertad de información.

Conclusiones críticas

Es sintomático y revelador que no sepamos siquiera cómo llamar a esta "violencia": de género, VPG, violencia en política contra las mujeres, violencia contra las mujeres políticas por razón de género. Relacionado estrechamente con tal diagnóstico, se plantean dos problemas adicionales. Por un lado, nadie sabe qué es de veras, desde la perspectiva jurídica, dicha violencia, pero sí sabemos que las democracias constitucionales ya están y estaban equipadas con un arsenal normativo (también penal) para combatir según qué cosas.

Si con VPG se quiere decir prohibir cualesquiera malos tratos, erradicar la violencia física o, en definitiva, evitar o intentar resarcir de cualquier tipo de menoscabo intolerable jurídicamente hablando para con las mujeres (y hombres) el concepto resulta inoperante porque tales conductas -y otras tantas- estaban ya convenientemente recogidas y castigadas. Además, recordemos que la convivencia humana en libertad siempre conlleva molestias y ruidos que provocan fricciones, desacuerdos, manifestaciones subidas de tono, y demás condiciones derivadas del *zoon politikon*. Si con el concepto no solo no se pretende "nombrar" una realidad sino construir una *ad hoc*, donde se tenga en burbujas a las mujeres, se las trate como seres permanentemente necesitados de tutela y protección, y se parta de la presunción de que las palabras pueden herir igual que las acciones, la violencia política por razón de género perpetuará lo que desea combatir, amén de poner en la picota, sin solución de continuidad, a quienes dice querer proteger a toda costa.

Por otro lado, la libertad de expresión como derecho fundamental, aun con los límites pertinentes, debe prevalecer. Nunca podemos olvidarlo: mientras que la libre expresión es un derecho basilar que irradia todos los demás y encuentra acomodo en la mejor tradición constitucionalista, el discurso del odio es una noción lábil y brumosa creada a golpe de sentencia que, en la versión que aquí hemos estudiado -la VPG- no se muestra muy operativa. Tanto menos cuando se blande en contextos político-electorales donde se está luchando a brazo partido por el poder. Agotando el razonamiento libertario, cierto grado de expresión "fuerte" siempre se dará, puesto que con la libertad de expresión queremos convencer a otros de la bondad de lo nuestro, queremos provocar el choque de pensamientos. VPG se parece mucho a decir: dennos un cheque en blanco que nosotras (algunas, pocas, las *elegidas*) nos encargaremos de administrar su montante.

Esta cuestión de la VPG depende mucho de la zona, del país, de los sistemas constitucionales (si es que hay), de la regulación y respeto por las normas electorales, de los sistemas jurídicos, en fin, de tantas variables que se hace difícil extractar reglas generales, más allá de esta: los denunciados son hombres y las presuntas víctimas, mujeres. Con mentalidades así se traslada la idea, por poner un ejemplo lacerante, de que los hombres caídos en la lucha contra el narco, cuentan menos, mucho menos, que el de las mujeres caídas en la misma contienda, problema real porque todavía existen valientes de los dos sexos que desafían el terror cotidiano que impone.

Cabe añadir que el género es un concepto abstruso, confuso, abigarrado, que no pone de acuerdo a nadie en torno a él, antes al contrario, ni siquiera quienes defienden su vigencia y legitimidad. Unas dicen que hay que hacerlo central y otras dicen que hay que destruirlo. Unos dicen que gracias al género se destruirán las discriminaciones de género y otros hablan incluso de *borrar* el sexo, como si atacar la naturaleza biológica más elemental del ser humano fuera algo de lo que se puede salir indemne (ya lo dijo Macbeth: "los actos contra la naturaleza engendran disturbios contra la naturaleza").

VI. Moderación en el Espacio Digital durante el Periodo Electoral

María Garrote
Facultad de Derecho, Universidad Complutense de Madrid
magarrot@ucm.es

La función de moderación de las plataformas digitales durante el período electoral es, como hemos visto, uno de los nodos de la respuesta frente a las amenazas tecnológicas en campaña electoral. De ahí la necesidad de incidir en los riesgos que puede generar esta función que, sin embargo, es absolutamente necesaria.

Los procedimientos internos de moderación de contenido constituyen un avance muy importante en la lucha contra la desinformación o la difusión descontrolada de publicidad de contenido político o de mensajes políticos extremos. Sin embargo, estos procedimientos internos generan desconfianza y no están exentos de riesgos. Podemos identificar tres grandes amenazas en la función de moderación: Primero, pueden convertirse en medidas de censura política. La moderación de las redes sociales amenaza la libertad de expresión y facilita un control sobre la opinión pública. No es fácil identificar qué contenidos son inapropiados, tanto por el fondo como por la forma en que se difunden, y en período electoral se debe extremar el respeto a la libertad de expresión y garantizar en todo momento la igualdad de oportunidades. En segundo lugar, las plataformas digitales utilizan algoritmos para detectar contenidos inapropiados que pueden estar sesgados. Este sesgo algorítmico incrementa los errores (que pueden tener graves e irreversibles repercusiones en la competición electoral), reducen la transparencia y automatizan el sesgo humano. Por último, las decisiones de las plataformas de social media se desenvuelven en un marco ajeno al control democrático. El problema fundamental es que se deja en manos de compañías privadas la regulación de los contenidos que se publican en redes sociales, en aplicación de unas normas que no tienen origen democrático y mediante unos mecanismos técnicos (basados en algoritmos) poco transparentes (Sánchez, 2020:119).

Glosario

La **función de moderación** podría definirse como la actividad que realizan las compañías tecnológicas propietarias de plataformas digitales o redes sociales con el fin de controlar los contenidos publicados por los usuarios y que puede implicar incluso la retirada de esos contenidos o la suspensión de las cuentas de los usuarios. Esta actividad de control por parte de las compañías afecta a dos principios

fundamentales que deben presidir todo proceso electoral: la libertad de expresión y la igualdad de oportunidades de los contenientes.

Para comprender el alcance de esta función y los riesgos que puede conllevar es necesario hacer referencia a una serie de términos técnicos que se encuentran relacionados con esa actividad.

En primer lugar, debemos mencionar los *algoritmos*, que son intensamente utilizados por las plataformas digitales y redes sociales para, entre otras cosas, compilar y seleccionar el contenido que ven los usuarios.

Los **algoritmos** son un conjunto finito de reglas formales (operaciones lógicas, instrucciones) que permiten a una computadora obtener un resultado a partir de elementos de entrada. Estas reglas pueden ser objeto de un proceso de ejecución automatizado y contar con modelos diseñados a través de aprendizaje automático. El *aprendizaje automático* hace posible construir un modelo matemático para permitir que una computadora tome decisiones o predicciones sin intervención humana en función de los datos, que incluyen una gran cantidad de variables que no se conocen de antemano. Por otra parte, el **aprendizaje supervisado** es una forma de aprendizaje automático que no funciona de forma independiente, sino que requiere intervención humana. Los datos se presentan en la máquina y el proceso es guiado por una persona mientras la computadora trabaja hacia un resultado específico. Mediante, por ejemplo, el etiquetado de contenido, el aprendizaje automático guiado generará un resultado esperado.

La utilización intensiva y frecuente de algoritmos nos lleva a otro concepto, el **sesgo algorítmico**: Tecnologías que no contemplan toda la gama de ideas disponibles y presentan errores repetibles en el resultado de un sistema informático, privilegiando un resultado sobre otro. Un algoritmo puede "programar" un software para que no admita una gama completa de entradas, sino solo un espectro más pequeño. Este sesgo se encuentra en los resultados de los motores de búsqueda y en las plataformas de redes sociales. Este concepto está ligado a la inteligencia artificial, y también puede describirse como manipulación digital de las elecciones cuando un intermediario utiliza una presentación selectiva de la información para favorecer su agenda, en lugar de la de los usuarios, que en este caso son los votantes.

La ***tecnología de comunicaciones digitales*** es el entorno en el que se va a desenvolver la función de moderación. Se trata del diseño y construcción de tecnología de comunicaciones que transmite información en forma digital. Son herramientas digitales que permiten que dos o más personas se comuniquen entre sí. En este sentido, la **alfabetización digital** (alfabetización informática, mediática o informacional) se refiere a las habilidades complementarias y entrelazadas, tanto técnicas como sociales, que las personas deben emplear cuando utilizan la

comunicación basada en Internet (incluidos hipertexto, imágenes, audio y video) para consumir y crear mensajes en una variedad de contextos académicos, cívicos y culturales. Es la alfabetización de las prácticas digitales emergentes, donde los estudiantes competentes deben desempeñarse igual de bien en la comunicación cara a cara y en la impresa, como nuevas herramientas en línea. Los conceptos relacionados son la alfabetización informática, la alfabetización en tecnologías de la información y la comunicación (TIC), la alfabetización informacional, la alfabetización mediática, las nuevas alfabetizaciones y las multialfabetizaciones.

En la comunicación digital nos encontramos con el fenómeno de las "**cámaras de eco"** *-echo chambers-* En general, el término "cámaras de eco" ilustra las formas en que los cuellos de botella o silos de datos restringen las opciones disponibles para personas o máquinas. En las redes sociales y otras plataformas interactivas, donde las tecnologías a menudo seleccionan fragmentos de datos de una fuente general de acuerdo con heurísticas o algoritmos de aprendizaje, los usuarios pueden ver un *feed* de redes sociales que se convierte en una "cámara de eco" de ideas similares o comunes. Una cámara de eco también se puede definir como una situación en la que las personas solo escuchan opiniones de un tipo o similares a las suyas. Esto significa que otras voces han sido activamente excluidas y desacreditadas. Se ha llevado a los miembros de las cámaras de eco a desconfiar sistemáticamente de todas las fuentes externas. En las burbujas epistémicas, no se escuchan otras voces, mientras que, en las cámaras de eco, otras voces se socavan activamente.

El **Internet de las cosas** *(IoT) e*s el hecho de conectar cualquier dispositivo con un interruptor de encendido y apagado a Internet (y/o entre sí). Esto incluye todo, desde teléfonos móviles, auriculares, dispositivos portátiles e incluso lavadoras, etc. Esto también se aplica a los componentes de las máquinas. El *IoT* es una red gigante de "cosas" conectadas (que también incluye a las personas). La relación es entre personas-personas, personas-cosas y cosas-cosas. Puede usarse o abusarse para cambiar el discurso político en línea, al acceder y almacenar cantidades considerables de datos personales o usuarios de dispositivos, y afectar el compromiso cívico en línea o en la política. Así, las *botnets* de *IoT* son una red de dispositivos conectados a *IoT* que están infectados con malware o controlados por actores malintencionados.

Garantizar la igualdad de condiciones electorales debe ser una prioridad en cualquier actividad de control o moderación en la comunicación digital. Una competencia justa que asegure que cada partido y candidato reciba un trato justo y se le proporcionen exactamente las mismas oportunidades y recursos financieros, independientemente de su tamaño y popularidad, asegurándoles la misma oportunidad de presentar su caso ante los votantes. Con la digitalización de la política, este término se puede utilizar en relación con el discurso político en línea, el uso de las redes sociales de los candidatos más ricos, etc. Directamente relacionado con ello está el concepto de **neutralidad de la red***,* que subraya que los proveedores de servicios de Internet

deben tratar todos los datos por igual. Los proveedores de servicios no pueden priorizar ningún dato.

Casos

Iniciativas de regulación

Desde hace unos años se han planteado varias iniciativas reguladoras que, entre otras medidas, tratan de establecer una serie de garantías en la actividad de moderación de las plataformas digitales. En el ámbito estatal, Alemania aprobó una ley sobre aplicación de la ley en las redes sociales (2017) que contiene una serie de medidas para mejorar la efectividad de las leyes y regula el procedimiento de remoción de contenidos, que no ha estado exento de críticas. Además, el *Tratado interestatal sobre medios* (2020) incide en la responsabilidad de los intermediarios de internet e impone unas reglas para la función de moderación.

En el ámbito europeo, destaca el *Código de conducta sobre desinformación* acordado por la Comisión europea en 2018 -a partir del informe emitido por un Grupo de Expertos de Alto Nivel sobre *fake news* y desinformación online- que apuesta por la autorregulación (el documento fue firmado por Facebook, Google, Twitter, Mozilla y Microsoft) y traslada a las compañías la responsabilidad de intervenir en los contenidos mediante un control que puede ser más rápido y eficaz que el realizado por las autoridades públicas. También en 2018 la Comisión y el Alto Representante para los Asuntos Exteriores y la Política de Seguridad aprobaron conjuntamente el *Plan de Acción contra la desinformación,* uno de cuyos pilares se refiere a la movilización del sector privado mediante la adhesión y cumplimiento del *Código de conducta.*

En el seno del Consejo de Europa, *la Recomendación del Comité de Ministros sobre el papel y la responsabilidad de los intermediarios de internet* de 2018 reafirma la obligación de que cualquier decisión sobre eliminación de contenidos debe estar respaldada por una autoridad judicial o por una autoridad independiente, sometida en última instancia a revisión judicial, así como otras garantías en el proceso de retirada de contenidos. La Comisión de Venecia ha recopilado muchas iniciativas en dos documentos que resultan imprescindibles: un informe sobre *Tecnologías digitales y elecciones* (2019) y los *Principios para un uso conforme a los derechos fundamentales de tecnologías digitales en procesos electorales* (2020).

Casos relevantes

Existen varios precedentes judiciales y administrativos que han abordado directa o indirectamente cuestiones relativas a la moderación de los contenidos en la comunicación digital.

Resulta muy interesante el Acuerdo de la Junta electoral Central de España que resuelve la reclamación contra Twitter por la suspensión de la cuenta del partido político VOX en esa red social estando convocadas las elecciones al Parlamento de Cataluña de 14 de febrero de 2021.La suspensión de la cuenta, motivada por la publicación de un mensaje que contravenía la política relativa a conductas de incitación al odio, fue considerada legítima y proporcionada. Dicho acuerdo fue ratificado por el Tribunal Supremo en su sentencia 246/2022, de 28 de febrero.

El Tribunal Superior de Elecciones de Costa Rica el 6 de febrero de 2022 resolvió cautelarmente 63 casos en los cuales ordenó la remoción de contenido de redes sociales -durante el periodo de veda electoral -por vulnerar la legislación electoral en Costa Rica sobre prohibición de propaganda electoral. Todos los contenidos eran publicitarios y estaban alojados en la biblioteca de anuncios. Se procede a “ordenar a Meta Platforms, Inc. que proceda de inmediato con la remoción del espacio publicitario”.

El Tribunal Electoral del Poder Judicial de la Federación de México ha resuelto varios casos sobre la publicación de mensajes de personas no candidatas en redes sociales durante la veda electoral y se han considerado propaganda electoral (los más recientes, SUP-REP-319/2021. SUP-RAP-0172-2021 SRE-JE-0106-2021-Acuerdo 1)

En Brasil también se han dictado resoluciones relevantes en este ámbito. La decisión del Tribunal Superior Electoral de mayo de 2019 (Recurso Especial Eleitoral nº 13351) indica que los mensajes enviados a través de la aplicación Whatsapp no están abiertos al público, como sí lo están los albergados en redes sociales como Facebook e Instagram. La comunicación es de carácter privado y se restringe a los interlocutores o a un grupo limitado de personas, lo que justifica, aplicando el canon de proporcionalidad en sentido estricto, la prevalencia de la libertad de expresión. Esta línea interpretativa se refuerza en la decisión de abril de 2020 (Recurso em Representação nº 060147858) en la que afirma que la realización de propaganda electoral en el perfil de una persona jurídica en la red social Facebook viola los arts. 57-B y 57-C de la Ley 9.504/97 y conlleva la imposición de una multa.