universidad de león

FACULTAD DE DERECHO
UNIVERSIDAD DE LEÓN
CURSO 2019/2020

LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN Y SU INJERENCIA EN LOS PROCESOS ELECTORALES

INFORMATION AND COMMUNICATION TECHNOLOGIES AND ITS INTERVENTION IN ELECTORAL PROCESSES

MÁSTER EN DERECHO DE LA CIBERSEGURIDAD Y ENTORNO DIGITAL

AUTOR/A: Dª. JULIETA ZANAZZI

TUTOR/A: DRA. Dª. MARÍA ESTHER SEÍJAS VILLADANGOS

AGRADECIMIENTOS

Agradezco a la Fundación Carolina, el INCIBE y la Universidad de León, por brindarme la beca que me dio la gran oportunidad de realizar el Máster en Derecho de la Ciberseguridad y Entorno Digital. A mi tutora la Dra. María Esther Seíjas Villadangos por su tiempo, valiosa ayuda y aporte de conocimientos.

DEDICATORIA

Quiero dedicar este trabajo a mis papás y hermana por siempre creer en mí y acompañarme en cada proyecto que emprendo. A Miguel y Luciano que me abrieron las puertas del maravilloso mundo del derecho y las tecnologías. A Lomb que sin su apoyo en el día a día no hubiera sido posible, y a la Tata que siempre estará presente en cada paso.

ABREVIATURAS

AEPD: Agencia Española de Protección de Datos

CDFUE: Carta de los Derechos Fundamentales de la Unión Europea

CE: Constitución Española.

CEDH: Convenio Europeo de Derechos Humanos

CIDH: Comisión Interamericana de Derechos Humanos

LOPDyGDD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

LOREG: Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General.

RAE: Real Academia Española.

RGPD: Reglamento General de Protección de Datos.

STC: Sentencia del Tribunal Constitucional

TICs: Tecnologías de la información y la comunicación.

TC: Tribunal Constitucional Español.

UE: Unión Europea.

ÍNDICE

RESUMEN

En este trabajo se hará un recorrido y análisis sobre las múltiples maneras en que las Tecnologías de la Información y la Comunicación pueden intervenir en las distintas etapas de los procesos electorales, haciendo foco en la manipulación del electorado a través de la desinformación y en la utilización de mecanismos de votación electrónica tanto presencial, como remota.

Las *fake news*, los bots políticos, los nuevos medios sociales, el voto electrónico y el voto por internet, son algunos de los elementos que se abordarán para evaluar como afectan en los principios democráticos y en la protección de la legalidad y legitimidad de los procesos.

Se estudiará el impacto de las TICs en su afectación al derecho al sufragio activo y pasivo, y cómo el principio de un voto universal, secreto, libre e igual se puede ver afectado.

Desde un enfoque jurídico se planteará el interrogante de la necesidad o no de una ley, y las consecuencias que traería aparejada la misma, analizando que elementos existen en el ordenamiento jurídico actual, que medidas a tomado la UE para luchar contra la desinformación y que derechos fundamentales se ven afectados por la injerencia de las TICs en el proceso y por la posible creación de una norma.

Para concluir se propondrá una solución desde las buenas prácticas y la educación en lo digital de la ciudadanía.

ABSTRACT

In this work, a tour and analysis will be made about the multiple ways in which Information and Communication Technologies can intervene in the different stages of the electoral processes, focusing on the manipulation of the electorate through misinformation and the use of e-voting mechanisms both in person and remotely.

Fake news, political bots, new social media, e-voting and voting though the internet, are some of the elements that will be addressed to assess how they affect democratic principles and the protection of the legality and legitimacy of processes.

The impact of ICTs on active and passive voting right will be studied, and how the principle of a universal, secret, free and equal vote can be affected.

From a legal perspective, the question will arise of whether or not a law is necessary, and the consequences that it would entail, analyzing what elements exist in the current legal system, what measures have been taken by the EU to combat disinformation and which fundamental rights are affected by the interference of ICTs in the process and by the possible creation of a standard.

To conclude, a solution will be proposed based on good practices and digital education for citizens.

PALABRAS CLAVE

Desinformación, procesos electorales, noticias falsas, voto electrónico, derechos fundamentales, democracia.

KEYWORDS

Misinformation, electoral process, *fake news,* e-voting, fundamental rights, democracy.

OBJETO DEL TRABAJO

Objetivo principal:

Las Tecnologías de la Información y Comunicación se han transformado en un elemento primordial en la sociedad de la información. Estamos inmersos en nuestra vida cotidiana en las grandes ventajas y facilidades que nos brinda la tecnología, y tanto el sector público como el privado lo saben, y se aprovechan de ello.

Como ciudadanos tenemos un rol cada vez más activo en los procesos electorales, y vemos cómo en los últimos años la tecnología ha ingresado en las diversas etapas de dicho proceso, siendo importante que desde el mundo académico y jurídico nos planteemos las consecuencias que conlleva frente a la democracia.

Es por eso, que el objetivo general de este trabajo es analizar como las TICs, intervienen en las distintas etapas del proceso electoral, haciendo especial hincapié en la desinformación y el condicionamiento del electorado. Así como también, en el respeto o no de los principios electorales democráticos que infiere el uso de algunas tecnologías, como por ejemplo el voto electrónico.

Se busca definir el rol del orden jurídico para regular y proteger los procesos democráticos, y las posibles soluciones para ello.

Objetivos específicos:

- Definir los diferentes momentos de un proceso electoral
- Distinguir y analizar el uso de las Tecnologías de la Información y la comunicación en cada uno de ellos.
- Calificar *fake news*, desinformación y posverdad
- Conceptualizar y analizar el sufragio secreto y libre.
- Analizar manipulación del electorado desde las TICs.
- Explicar el funcionamiento técnico de las distintas herramientas utilizadas para desinformar.
- Identificar casos de la realidad.
- Analizar el rol del derecho sobre los tópicos desarrollados.

- Identificar soluciones de buenas prácticas.

METODOLOGÍA

De acuerdo con el tema a tratar y los objetivos planteados, esta investigación utilizará un enfoque metodológico inductivo, haciendo énfasis en la búsqueda de hechos u objetivos concretos de la realidad -premisas particulares-, para a partir de ello obtener conclusiones generales.

Dentro de las etapas del método planteado en un primer paso se realizará la observación de los hechos y un análisis de la realidad.

Luego se clasificarán y estudiarán los hechos, a través de la investigación de cada situación tratando de extraer elementos comunes sobre los que sea posible sustentar una teoría con vocación generalista.

En una etapa posterior del análisis y estudio de las premisas particulares, podremos llegar como conclusión final, que de manera ascendente construimos abstracciones para lograr una descripción y formulación de premisas del tema que se está estudiando, la injerencia de las nuevas tecnologías en el ejercicio del derecho fundamental del sufragio activo.

En el proceso de trabajo se buscó conciliar dos ámbitos de conocimientos que normalmente se consideran ajenos o extraños, esto es el ámbito del derecho y el ámbito de las ingenierías tecnológicas.

Esto ha sido plasmado tanto en la búsqueda, análisis y estudio de la información, en el asesoramiento que se ha recibido de parte de un ingeniero en infotecnología, como también en las propuestas vertidas en el trabajo. Asimismo, se consultaron fuentes dentro de las ciencias sociales de la comunicación, buscando abordar el tema de manera interdisciplinar.

CAPÍTULO PRIMERO: TICs y DESINFORMACIÓN

"Las Tecnologías de Información y Comunicación (TIC) se han constituido en un elemento trascendental en nuestra sociedad, llamada ahora sociedad de la información" (E. TELLO LEAL, D. TELLO LEAL y SOSA REYNA, 2012:36). Podemos observar como todos los ámbitos de nuestra vida se ven afectados de una manera u otra por la tecnología, manifestándose principalmente en tres áreas: la información, las comunicaciones y la automatización (GARCÍA RODRIGUEZ, 2011).

Esa injerencia de las TICs comenzó a provocar cambios estructurales en nuestra sociedad, tal es así que hasta los procesos electorales se ven atravesados por las distintas herramientas tecnológicas.

La política, los ciudadanos, los medios de comunicación y demás agentes involucrados en el desarrollo del estado democrático, han ido utilizando los avances tecnológicos al servicio de los mismos, sin embargo, no todo se limita a beneficios y ventajas.

Gracias a internet, las TICs, y los nuevos modos de relacionaros y comunicarnos, aparecen fenómenos como las *fake news* y la posverdad, que permiten la aparición de campañas de desinformación con el fin de manipular al electorado y poner en jaque a los procesos democráticos.

En este primer capítulo, tendremos como objetivo contextualizar como las TICs pueden afectar en los procesos electorales, analizando y definiendo fenómenos como las *fake news* y la posverdad, y sus consecuencias en la desinformación. Asimismo, identificaremos el rol y la importancia de los nuevos medios sociales para las campañas de desinformación.

Por último, plantearemos los riesgos que surgen para la democracia como consecuencia de la aparición de estos nuevos fenómenos mencionados y la injerencia de las tecnologías en los procesos electorales. Se mencionará brevemente el caso de las elecciones en Estados Unidos en el 2016, como corolario de la aplicación del marco teórico y con el fin de demostrar la existencia en el mundo físico de lo que en este trabajo se expondrá.

1.1 Contextualizando los nuevos fenómenos

1.1.1.- La incursión de las TICs en el ámbito electoral

Cuando hablamos de las Tecnologías de la Información y la Comunicación, nos estamos refiriendo a un concepto asociado a la informática, entendidas como "… el conjunto de nuevos recursos, procedimientos y técnicas usadas en el procesamiento, almacenamiento y transmisión de información*"* (FERNÁNDEZ DELPECH, 2014:15).

Obviamente, los avances en el mundo de la tecnología también afectan a los procesos electorales, y la incorporación de internet al ámbito comunicacional ha adquirido incidencia convirtiéndose en un gran sistema de información, comunicación e incluso, como corolario de la injerencia de las TICs en el mundo electoral, de emisión de sufragio (GARCÍA RODRÍGUEZ, 2011).

La aplicación de las TICs por el Estado en las distintas etapas del proceso electoral genera cambios profundos en la manera en que las personas interactúan dentro de la sociedad, y el compromiso e interacción de los ciudadanos con los procesos. A raíz de dichos cambios surge el término Sociedad de la Información (TELLO LEAL et al., 2012).

En palabras de Fernández Delpech (2014:15-16): *"*La sociedad de la información… se refiere a la creciente capacidad tecnológica para almacenar informaciones y hacerlas circular cada vez de forma más rápida y con mayor difusión. Esa sociedad de la información surge como consecuencia de la implantación de las tecnologías de la información y comunicación (TICs) en las relaciones sociales, culturales y económicas de las comunidades…" sumándole a dicho concepto la implementación de las TICs en el ámbito político, en el desarrollo y ejercicio de nuestros derechos como ciudadanos de un estado, que se ve plasmado en el acto protagonista de la democracia representativa: la emisión del sufragio.

Ahora bien, se anhela que la sociedad de la información nos conduzca a la denominada sociedad del conocimiento, donde se espera que se produzca una apropiación crítica y selectiva de la información (FERNÁNDEZ DELPECH, 2014).

Estar inmersos en una sociedad informada, donde las TICs se aplican a los procesos electorales, implica mayor protagonismo del ciudadano. "Debido a las nuevas tecnologías

de la información y comunicación, y un cambio cultural-generacional, los ciudadanos-usuarios tienen el poder para crear valor, agregar intereses, producir sus medios de comunicación y, por ello, influir en asuntos públicos" (GARCÍA RODRÍGUEZ, 2011:11) Las tecnologías de la información han provocado una revolución en el ámbito de la configuración de la opinión pública (RUBIO NÚÑEZ, 2018).

Debemos aceptar que las TICs llegaron para quedarse y que las distintas etapas del proceso democrático se verán afectadas por una u otra tecnología. Como consecuencia de ello las legislaciones deben ser acordes para lograr una adaptación y modernización de los procesos, respetando los derechos fundamentales de cada Estado, vertiendo un especial enfoque, atención y cuidado respecto al ciudadano-usuario de las TICs, para evitar que su participación democrática se vea sesgada por terceros.

Al cobrar una mayor importancia el ciudadano dentro del proceso, ya no solo se dedica a emitir su voto, ahora también tiene más mecanismos para controlar la gestión institucional de los recursos, participar activamente, acceder a información más allá de la plasmada en los medios tradicionales y, ejercer el rol de informar y compartir la información que posee de manera masiva, gracias a que la tecnología le permite hacerlo libremente[1].

1.1.2.- Fake News y Posverdad

El 2016 fue un año clave en el cual se produjeron tres acontecimientos donde las TICs, sobre todo las redes sociales y el nuevo marketing político estratégico para comunicar y establecer lo que es verdadero y lo que es falso, modificaron la percepción del poder de las tecnologías para influir en procesos de toma de decisiones en un estado. El resultado del referéndum de salida del Reino Unido de la Unión Europea (*Brexit*), la victoria de Donald Trump en las elecciones de Estados Unidos y el resultado del primer referéndum para el proceso de paz

[1] Lo que se conoce comúnmente como periodismo ciudadano. Cada vez más los medios tradicionales les brindan espacios a los diferentes usuarios para que informen sobre acontecimientos de interés donde el ciudadano tiene contacto directo por encontrarse en el lugar del hecho, por ejemplo, o ser protagonista. Asimismo, las redes sociales y su inmediatez hacen que luego en los canales oficiales y/o tradicionales de notica se utilice como fuente de información tuits, comentarios o publicaciones tomadas de las redes al momento de acontecer algún evento de relevancia. Asimismo, gracias a Internet los ciudadanos se han ido convirtiendo en los verdaderos protagonistas del proceso electoral. El acceso a múltiples fuentes de información y la posibilidad de utilizar nuevos canales en apoyo de uno u otro candidato los convierte en agentes destacados en el proceso electoral (RUBIO y JOVE, 2006)

en Colombia (TUÑON NAVARRO, OLEART y BOUZA GARCÍA, 2019), fueron determinantes para que los estados comenzaran a entender que aquello que veíamos lejano y sucedía en el ciberespacio no quedaba solo allí, sino que tenia consecuencias muy reales en el mundo físico.

Compañías como Google, Facebook y Twitter fueron convocadas a comparecer ante el Comité de inteligencia del Congreso de los Estados Unidos, por un motivo meramente político y relacionado con la investigación sobre las injerencias de Rusia en las elecciones presidenciales del año 2016. Se sospechaba que a través de estas plataformas tecnológicas gran cantidad de estadounidenses habían sido expuestos a información falsa (*Fake News*) generada por Rusia con el fin de provocar la discordia en la sociedad norteamericana y favorecer la candidatura de Donald Trump (RUBIO NÚÑEZ, 2018).

Asimismo, se habían detectado el uso de tácticas similares durante el referéndum convocado en el Reino Unido, donde los británicos decidían sobre su permanencia o no en la Unión Europea (RUBIO NÚÑEZ, 2018).

En los ejemplos en mención, observamos que internet y las redes sociales han tenido un papel relevante para la generalización de estas prácticas, lo cual ha generado en los estados distintas reacciones y preocupación respecto a los peligros que presupone para la democracia (TUÑON NAVARRO et.al., 2019).

Por ello, términos como posverdad, *fake news* y desinformación han ganado protagonismo en discursos políticos, trabajos académicos, análisis periodísticos e incluso en ámbitos legislativos.

El Diccionario de Oxford escogió "posverdad" como la palabra del año 2016. Expresión que se refiere a que los hechos objetivos y reales tienen menos credibilidad o influencia que los sentimientos y creencias de los individuos al momento de formular una opinión pública o determinar una postura (DE CASTRO RUANO, 2018).

En otras palabras, estamos hablando de distorsión de la realidad de manera deliberada donde los hechos ya no son tan relevantes y prevalecen los sentimientos o creencias personales que se generan sobre los hechos en sí mismos.

Respecto a las *Fake News*, no existe unificación doctrinaria sobre el concepto del término[2] pero podríamos definirlas como *"*...aquel contenido que, tomando la apariencia de ser legítimo, busca manipular, en mayor o menor medida, a la opinión pública" (ROMERO RODRIGUEZ, VALLE RAZO y TOUKOUMIDIS, 2018:270). Es un concepto amplio que abarca las distintas formas que pueden tomar este tipo de noticas falsas. Tal es la importancia del término que en el año 2017 el diccionario británico Collins eligió *Fake News* como palabra del año *"*describiéndolas como información falsa, a menudo sensacionalista, diseminada bajo la apariencia de noticia*"* (RODRÍGUEZ-FERNÁNDEZ, 2019:1715).

Aunque en el plano teórico se distinguen las *fake news* de la posverdad, en la práctica es habitual que se utilicen ambas palabras como caras de una misma moneda.

Como se puede apreciar, el impacto de la información falsa, de la manipulación del lector apelando a sentimientos y creencias, y las graves consecuencias que ello trae aparejado para un estado, como se mencionara ut supra respecto a los acontecimientos ocurridos en el año 2016, llevó a que la Comisión Europea comience a interesarse en estos tópicos, preocupados más que nada, por la injerencia de estos fenómenos en los procesos democráticos y una posible manipulación del electorado.

Luego de analizar y estudiar los términos *fake news* y posverdad, la UE se decidió que la acepción correcta para denominar lo que estaba ocurriendo, era desinformación.

Por ello, cuando hablamos de desinformación debemos entender como "aquella información verificablemente falsa o engañosa que, de forma acumulativa, se crea, presenta y divulga con fines lucrativos o para engañar deliberadamente a la población y puede causar un perjuicio público, entendido como amenazas contra los procesos democráticos políticos y de elaboración de políticas, así como contra los bienes públicos, como la protección de la salud, el medio ambiente o la seguridad de los ciudadanos de la UE" (COMISIÓN EUROPEA, 2018:1).

[2] Pero si encontramos coincidencias respecto de los elementos de las mismas. Ellos son: la estética adoptando formatos idénticos tanto en contenido como en la apariencia a los de los medios convencionales y digitales; la narrativa porque los contenidos son redactados como géneros periodísticos y, por último, la manipulación: las *fake news* esconden siempre la intención de manipular a la opinión pública. (ROMERO RODRÍGUEZ et.al., 2018)

Por lo expuesto, más allá del término que utilicemos, estamos frente al uso de la mentira como técnica para persuadir y manipular al lector, bajo la apariencia de una noticia o información verdadera, lo cual trasladado al ámbito político puede ser grave. Es decir, en un Estado democrático el elector debe obtener toda la información necesaria, lo más objetiva posible, para poder formular su decisión a la hora de ejercer su voto y gracias a las TICs agentes externos fácilmente logran presentar los datos de manera tal que inducen al ciudadano a pensar como dicho agente quiere que lo haga.

1.1.3.- Nuevos medios sociales

Los medios de comunicación son espacios que contribuyen a definir la agenda política, jugando un rol central a la hora de informar y combatir la desinformación (TUÑON NAVARRO et.al., 2019).

Según la RAE un medio de comunicación es un "Instrumento de transmisión pública de información, como emisora de radio, televisión, periódicos, internet, etc." (REAL ACADEMIA ESPAÑOLA, 2014).

Hasta finales del siglo pasado, los medios de comunicación tradicionales eran los encargados de crear y transmitir mensajes que marcaban la agenda política ejerciendo el papel de mediadores en el proceso de conformación de la opinión pública (CENTRO CRIPTOLÓGICO NACIONAL [CCN], 2019).

Con los medios tecnológicos a disposición, la aparición de Internet y las redes sociales, se crean nuevos canales para obtener información haciendo que los medios tradicionales tengan que adaptarse al mundo digital.

Nos encontramos con la aparición de los denominados nuevos medios sociales que toman cada vez más protagonismo, aunque continúen conviviendo e incluso influenciando a los medios tradicionales, tales como, prensa, radio, tv (DE CASTRO RUANO, 2018).

"Los nuevos medios sociales se valen de las posibilidades digitales de acceso a la información y constituyen un nuevo espacio de información y comunicación generado, distribuido y compartido a través de las redes sociales de internet en sus múltiples expresiones y formas: blogs, páginas webs, apps para móviles y tabletas, wikis, chats, redes

sociales como Facebook, Twitter, Instagram, LinkedIn, etc." (DE CASTRO RUANO, 2018:3).

Existen numerosas diferencias entre los nuevos medios y los tradicionales. La más importante de destacar, y que nos interesa dentro del ámbito de la desinformación, es que los nuevos medios permiten que cualquier usuario se convierta en un potencial informador, democratizando la autoría de contenidos y superando la intermediación tradicional de los medios convencionales. No se necesita ser profesional de la comunicación para publicar contenidos, si no que cualquiera puede generarlos (DE CASTRO RUANO, 2018).

A priori podríamos pensar que estos nuevos medios son una oportunidad única para la libertad de información, la libertad de prensa, democratizar contenidos y permitir que la mayor cantidad de personas conozcan la verdad de los acontecimientos cotidianos. Sin embargo, "…en las redes sociales no hay filtros, que sí existen en los medios de comunicación tradicionales o convencionales; filtros que, a decir verdad, no garantizan la objetividad absoluta ni eliminan totalmente la manipulación, como bien sabemos; pero al menos, aminoran la posibilidad de la mentira más burda, no se ocultan en fuentes desconocidas de dudosa legitimidad, sabemos qué intereses defienden, podemos exigirles rendición de cuentas y, en última instancia, dejar de comprarlos o escucharlos si sentimos que nos engañan..." (DE CASTRO RUANO, 2018: 3-4).

Los nuevos medios sociales, se caracterizan por publicar de manera casi simultánea a cuando surge el hecho, se aceleran los procesos de publicación y distribución del contenido, es decir, permiten acceder a la información desde cualquier lugar y en cualquier momento (DE CASTRO RUANO,2018). "Pero estos nuevos medios y esta forma de acceder a la información facilitan también la aparición de *fake news*, la propagación de bulos y la generalización de noticias de difícil o imposible verificación" (DE CASTRO RUANO, 2018:4).

"Según datos de la Asociación para la Investigación de Medios de Comunicación (AIMC), el principal uso que los ciudadanos españoles hacen de Internet es para la lectura de noticias de actualidad, así lo manifestó el 84,6 por ciento de las personas encuestadas entre octubre y diciembre de 2017" (CCN, 2019:9)

El ciudadano aprovecha las bondades de las TICs, para mantenerse actualizado e informarse, sin embargo, si no se realiza una apreciación crítica y racional de la información que se obtiene, se convierte en el eslabón estratégico de las campañas de desinformación.

Ello teniendo en cuenta que las redes sociales y los medios tecnológicos a disposición, acentúan la dimensión comunitaria de los procesos informativos, es decir, que las noticias se procesan y se valoran, en el interior de comunidades digitales afines, ideológica y socialmente (DE CASTRO RUANO, 2018).

Creemos con más facilidad aquello que nos gusta, intentamos que la búsqueda de la verdad no nos estropee nuestros sentimientos, nuestras creencias e ideologías (DE CASTRO RUANO, 2018).

Los erróneos hábitos de consumo de la información, el compartir sin contrastar la misma, el dejarse llevar por los sentimientos o creencias tomando como verosímil lo que recibimos sin analizar de manera objetiva las fuentes, si se trata de hechos reales o no, que expectativas sociales hay sobre tal acontecimiento, y la tecnología a disposición, tornan un ambiente propicio para la construcción de la falsedad.

La Comisión Europea llevó a cabo una encuesta denominada Eurobarómetro con el fin de explorar la conciencia y las actitudes de la ciudadanía sobre la existencia de noticias falsas y la desinformación en línea. La encuesta se realizó entre el 7 y el 9 de febrero de 2018 en los 28 Estados miembros de la Unión, encuestando alrededor de 26.000 ciudadanos de diferentes grupos sociales y demográficos (EUROPEAN COMMISSION,2018).

Las cuestiones más relevantes que se extraen es que “la mayoría de los encuestados dice encontrar una noticia falsa por lo menos una vez a la semana (incluso, el 37% afirma encontrar una cada día o «casi cada día»). Por cierto, la proporción más elevada se encuentra entre los encuestados en España (un 78% de ellos afirma encontrar noticias falsas por lo menos una vez a la semana)” (DE CASTRO RUANO, 2018:8). Asimismo “la mayoría de los encuestados confía menos en las noticias de fuentes de información digitales que en las que provienen de los medios tradicionales (la radio es el que ofrece más credibilidad: 70%; luego la TV: 66%; y los medios impresos: 63%)” (DE CASTRO RUANO, 2018:8).

“En resumen, el Eurobarómetro indica un importante grado de desconfianza en los medios; aunque la mayoría al menos tiende a creer en los medios tradicionales (radio, TV y prensa escrita) y menos en los digitales. Vemos también que las noticias falsas son percibidas como una realidad cotidiana en la ciudadanía” (DE CASTRO RUANO, 2018:8).

Las campañas de desinformación se aprovechan de la crisis de confianza en los medios, para implantarse y extenderse con facilidad y generar inestabilidad en las opiniones públicas (CCN, 2019).

Los nuevos medios sociales, como se expresará, permiten una participación activa de los ciudadanos a la hora de recibir, apreciar y compartir la información, pero también posibilitan que las campañas de desinformación y las *fake news* se propaguen fácilmente cumpliendo el objetivo de modificar la opinión pública y manipular a gusto de cada campaña las creencias de quien recibe dicha información.

Si bien como evidenció el Eurobarómetro ya referido, existe conciencia por parte de los ciudadanos del problema que acarrea la desinformación, “ un porcentaje del 83% afirmó que las *fake news* representan un peligro para la democracia” (DE CASTRO RUANO, 2018), sin embargo, la campañas de manipulación como se apreció en el referéndum de salida del Reino Unido de la Unión Europea (Brexit) o en la victoria de Donald Trump en las elecciones de Estados Unidos (TUÑON NAVARRO et.al., 2019) tienen éxito y por eso, debemos prestarles atención y cuestionarnos el rol del derecho ante tal fenómeno.

1.2 Democracia en peligro

La democracia funciona mejor, si la ciudadanía está informada y se involucra en los temas de interés público, el derecho a la información cobra especial relevancia en los procesos electorales (MEIXUEIRO NÁJERA, 2017).

“Todo el edificio democrático se apoya sobre la opinión pública, opinión que para ser tal debería ser verdaderamente autónoma…, y sobre esta opinión pública impacta especialmente la verdad” (RUBIO NÚÑEZ, 2018:218).

En este epígrafe abordaremos la trascendencia de las nuevas tecnologías en referencia al punto sobre el que pivota las democracias actuales, los procesos electorales.

1.2.1.- Planteamiento general sobre los riesgos de las democracias actuales

La deliberación pública se convierte en el instrumento para lograr acuerdos y un equilibrio, teniendo en cuenta la subjetividad de la verdad. Ante el debate político lo importante es vencer, ya no pasa por convencer, y se busca que el mensaje llegue al mayor número posible de personas (RUBIO NÚÑEZ, 2018).

Es por ello que como analizáramos anteriormente, los medios ocupan un lugar fundamental en el proceso democrático[3] y los agentes políticos convierten a la comunicación en un concurso por la construcción de relatos, tornándose un arma para lograr la victoria política sobre la oposición. De esta manera, nos encontramos en una forma de guerra, donde la información es la clave para alcanzar y mantener el poder (RUBIO NÚÑEZ, 2018).

Las TICs facilitan el acceso a la información, permitiendo que la participación de los distintos grupos de la ciudadanía aumente, en especial aquellos que normalmente como los jóvenes, no demuestran tanto interés en temas relacionados con la democracia (MEIXUEIRO NÁJERA, 2017).

Las redes sociales, los blogs, los medios digitales permiten una participación más activa de la ciudadanía en asuntos políticos, nos brindan el espacio para expresarnos libremente y hasta nos convierten en emisores de noticias dando como resultado la democratización de la información.

Sin embargo, las bondades de las TICs generan un terreno propicio para la desinformación, permitiendo que circulen noticias no verificadas o información falsa que pretende parecer verdadera (MEIXUEIRO NÁJERA, 2017).

La manipulación de la información acarrea efectos negativos en la cohesión social y la estabilidad política (ESTRATEGIA DE SEGURIDAD NACIONAL, 2017).

"La teoría política suele describir a la democracia como un sistema de gobierno frágil, que debe ser permanentemente protegido de múltiples peligros. Uno de ellos son las

[3] Tal como lo expresa Rubio Núñez (2018:218) "La comunicación no es algo accesorio…, sino que forma parte esencial de la democracia." y por ello la importancia que amerita.

interferencias ejercidas por actores ajenos a la comunidad que ostenta la soberanía, con el propósito de inclinar los resultados del proceso político hacia un resultado que favorezca sus intereses" (TORRES SORIANO, 2017).

Como venimos apreciando en este trabajo, las técnicas de la comunicación y las tecnologías de la información permiten la manipulación de sentimientos, comportamientos y formas de pensar, generando que la opinión pública sufra las consecuencias de la desinformación (RUBIO NÚÑEZ, 2018), afectando directamente las decisiones de los electores, poniendo al proceso democrático en peligro.

El ciberespacio es cada vez más utilizado para cometer ataques que alteren los intereses de un Estado, teniendo como objetivo manipular el funcionamiento de unos de los principales elementos de la democracia liberal que es la opinión pública. De obtener éxito los ciberataques de este tipo, los daños afectarían la naturaleza y razón de ser de un sistema de gobierno basado en la democracia (CCN, 2019).

"Las estrategias de desinformación inciden no solo en la capacidad de distribución, sino también en el tiempo de la misma, la sentimentalización de las decisiones políticas, la fragmentación de la opinión pública, la creación de esferas públicas paralelas, y su consiguiente polarización, la ausencia de referencias informativas válidas y la creación de un clima de sospecha general que pone en cuestión el papel de la verdad y pone en peligro la democracia, más allá de los periodos electorales" (RUBIO NUÑEZ, 2018:227).

Según el informe "*The Crisis of social media*" realizado por *Freedom House* (2019) podemos encontrar tres formas distintas de interferencia electoral digital: por un lado se encuentran las medidas informativas en las cuales las discusiones en línea se manipulan subrepticiamente a favor del gobierno o partidos particulares; por el otro las medidas tecnológicas, que se utilizan para restringir el acceso a las fuentes de noticias, herramientas de comunicación y en algunos casos extremos el acceso a todo el internet; y por último las medidas legales, que las autoridades aplican para castigar a los opositores y enfriar la expresión política.

"El ciudadano mejor informado será capaz de tomar las mejores decisiones para su gobernanza" (CCN, 2019:15), pero si la información que obtiene ha sido manipulada, y la esencia de sus pensamientos y decisiones son el resultado de una campaña de

desinformación, todo el proceso democrático se encuentra viciado, poniendo en jaque los pilares de un Estado-Nación moderno con peligrosas consecuencias para la democracia liberal.

1.2.2.- Caso Real: Elecciones en EE.UU 2016

El ciberespacio se transformó en un nuevo dominio donde proyectar el poder estatal, proporcionando a las operaciones y campañas de influencia un ambiente propicio para su desarrollo (TORRES SORIANO, 2017).

Asimismo, el uso de Internet como fuente de información, la crisis económica y de confianza de los medios tradicionales y la multiplicación de nuevos medios sociales generarán el ambiente perfecto para las campañas de desinformación (TORRES SORIANO, 2017).

El termino *fake news* como ya mencionáramos, ha tomado protagonismo después de la campaña electoral de las elecciones presidenciales de Estados Unidos de 2016 (LÓPEZ BORRULL, VIVES GRÀCIA y BADELL, 2018).

Tanto las autoridades judiciales como el propio congreso de los Estados Unidos analizan si hubo una injerencia de países extranjeros, especialmente Rusia, que alimentó debates políticos y sociales para aumentar las diferencias ideológicas sociales y erosionar la cohesión interna del país de manera maliciosa (CCN, 2019).

"Estados Unidos era a finales de 2016 una sociedad altamente polarizada en torno a diferentes brechas relacionadas con la raza, la respuesta al terrorismo yihadista, los efectos de la crisis económica, o la propia identidad del país frente al mestizaje sociocultural provocado por la inmigración de origen principalmente latino" (TORRES SORIANO, 2017:7), dándose las condiciones idóneas para que tuvieran éxitos las operaciones de influencia.

Aprovechándose de la polarización social, los portales de *fake news* y sus bots en redes sociales hicieron emerger noticias difamatorias sobre Hillary Clinton, información falsa destinada a adjudicarle frases, acciones delictivas y pensamientos en pos de disuadir al electorado seguidor de la candidata demócrata y favorecer la candidatura de Donald Trump (RUBIO NÚÑEZ, 2018).

Según Twitter, la gente en Estados Unidos tuiteó mil millones de veces sobre las elecciones durante la campaña (THOMPSON, 2016).

Los abogados de Google, Facebook y Twitter testificaron ante el Comité de inteligencia del Congreso de los Estados Unidos respecto a la investigación sobre las injerencias de Rusia en las elecciones presidenciales (RUBIO NÚÑEZ, 2018) que "hasta 126 millones de usuarios de Facebook podrían haber visualizado contenido producido y difundido por agentes rusos. Por su parte, Twitter declaró que había descubierto 2.752 cuentas controladas por rusos, y que más de 36.000 bots rusos produjeron 1,4 millones de tuits durante las elecciones. Finalmente, Google reveló que había encontrado en Youtube 1.108 videos con 43 horas de contenido relacionado con la injerencia rusa" (PUIG, 2017).

Las elecciones presidenciales en Estados Unidos en el 2016 es un claro ejemplo del poder de las campañas de desinformación en el ciberespacio. Entendiendo que el punto de partida para el éxito de las mismas es la existencia de una fractura social que permite que la manipulación surta efecto (TORRES SORIANO, 2017).

Con ayuda de las TICs se replican a millones de personas las *fake news* y de esa manera se manipula al electorado para que la elección del voto a realizar, se base en la información falsa intencionada que ha recibido durante todo el proceso, y que lo llevará a elegir al candidato que el organizador de la campaña de influencia deseaba.

No podemos afirmar con certeza si las campañas de desinformación que se produjeron en Estados Unidos fueron originarias de Rusia, pero lo que sí es una realidad es que tantas acusaciones graves, información - tanto verdadero como falsa - sobre la vida privada de los candidatos, afectó enormemente a la concepción que tenia el electorado de cada uno de ellos.

Lo cierto es que la candidata Clinton fue la más perjudicada, las campañas contra ella fueron brutales y las acusaciones gravísimas, "…cuentas anónimas en Facebook y medios de comunicación de escasa credibilidad comenzaron a difundir la noticia de que la candidata demócrata a la presidencia de Estados Unidos, Hillary Clinton, formaba parte de una red de explotación sexual de menores que tenia su sede en una conocida pizzería de Washington D.C. Estas informaciones se difundieron a gran velocidad y miles de ciudadanos le dieron credibilidad. De hecho, apenas un mes después de la publicación de esta noticia, un

ciudadano estadounidense entró armado al restaurante y comenzó a disparar con la intención de liberar a los presuntos niños explotados sexualmente"(CCN, 2019:20).

Este es un claro ejemplo de cómo algo que se viralizó en las redes sociales producto de una campaña de desinformación, tuvo consecuencias reales muy graves, demostrando que el electorado cree en la información que se le presenta.

Otro evento relacionado con la candidata demócrata fue el descubrimiento sobre que su equipo electoral había sido *hackeado* consiguiendo ingresar a sus correos electrónicos, servidores, obtener documentación y demás información privada. Ello llevo a que el FBI, el Congreso y un juzgado federal intervinieran, con el fin de investigar a los supuestos autores de los delitos informáticos que se sospechaban era grupos rusos, y determinar si hubo una interferencia con estas acciones en las elecciones.

Por ende, más allá de la dificultades que presentan los delitos informáticos y las maniobras de desinformación para atribuir el origen de las mismas, y por lo tanto lograr su persecución, no podemos desconocer el efecto real que presentan sobre el electorado y eso fue uno de los principales perjuicios sufridos por la candidata Clinton en las elecciones en Estados Unidos que la habrían llevado a perder las elecciones.

CAPÍTULO SEGUNDO: ETAPAS DEL PROCESO ELECTORAL Y LAS TICS

La utilización de nuevas tecnologías en la organización, planificación y ejecución de procesos electorales es una decisión que debe acompañarse con un análisis por parte del Estado respecto a la necesidad de la aplicación de herramientas tecnológicas, los costos y beneficios que acarrean (ORGANIZACIÓN DE LOS ESTADOS AMERICANOS [OEA], 2014), así como también, lo imperativo de educar a la población y a los partidos políticos sobre el uso de las TICs a implementar y su debida difusión.

"El régimen electoral está determinado por los elementos que configuran el sistema y el proceso electoral a través de los cuales se ejerce el derecho de sufragio. La celebración de unas elecciones y el ejercicio del derecho a votar y ser votado requieren la puesta en marcha de unos procedimientos y garantías, la intervención de unas instituciones y la configuración de un sistema electoral que transforme los votos obtenidos en escaños, todo lo cual constituye el régimen electoral" (CASTELLÁ ANDREU, 2018:98).

En los procesos electorales lo que se busca es que se respete y concrete los que las constituciones definen respecto al voto, esto es que sea: universal, libre, igual, directo y secreto (CASTELLÁ ANDREU, 2018), características que se replican en las constituciones de Estados que pregonan una democracia representativa[4].

De las características mencionadas, debemos hacer especial énfasis en dos de ellas: libre y secreto, ya que son las que más se podrían ver vulneradas gracias a la implementación de las TICs.

Que el voto sea libre implica que se cumplan con ciertas garantías antes, durante y después de las elecciones. Por ende, como hemos ido reflexionado en este trabajo, las campañas de desinformación infieren especialmente en la elección libre que debemos realizar de nuestro

[4]Tomando como ejemplo Argentina y España, podemos apreciar que en la Constitución de la Nación Argentina el articulo 37 garantiza el pleno ejercicio de los derechos políticos respetando el principio de la soberanía popular y determinando que el sufragio es universal, igual, secreto y obligatorio. Asimismo, en la Constitución Española en su articulo 68 se replica las características de universal, igual, secreto y obligatorio, sumándole la concepción de libre, que aunque en el régimen Argentino no se manifieste de manera explícita surge de la interpretación sistemática de la norma. En resumen, las Constituciones de los distintos estados le otorgan importancia a cómo debe llevarse a cabo el sufragio, y por ende, en el proceso electoral deben respetarse las características del mismo, aun con mayor énfasis cuando se aplican herramientas tecnológicas y/o automatizadas.

voto, ya que, se nos manipula e influye para que creamos lo que el dueño de la campaña desea.

Asimismo, se deben generar las condiciones óptimas para que se pueda ejercer con libertad el sufragio, evitando el día de las elecciones que se realice propaganda electoral y/o exista alguna manipulación técnica del sistema que se utilice para ejercer el voto. Y por supuesto es indispensable que, durante todo el proceso, se garantice la supervisión de las elecciones por una administración independiente del Gobierno (CASTELLÁ ANDREU, 2018).

Respecto al carácter secreto del voto la norma española, por ejemplo, estipula una serie de mecanismos para que no se pueda conocer contra la voluntad del votante su decisión, y así es que se utilizan cabinas electorales, papeleta dentro del sobre y urnas selladas (CASTELLÁ ANDREU, 2018), sin embargo, debemos reflexionar en cómo proteger el secreto si lo que se utilizara es una herramienta y/o dispositivo electrónico, teniendo que adaptar las normas a ello.

Por lo expuesto, en este capítulo se dividirá el proceso electoral en tres etapas: la precampaña y campaña electoral, el momento de celebración de elecciones y proclamación de electos y por último, la postcampaña.

Siguiendo esta línea se identificará en cada etapa como puede influir la utilización de las tecnologías en ellas, reflexionando sobre el conflicto que se puede generar para la democracia.

2.1 Precampaña y Campaña electoral

En esta etapa vamos a encontrarnos, por un lado, con "la presentación y proclamación de candidaturas por los partidos, coaliciones y agrupaciones de electores…" (CASTELLÁ ANDREU, 2018:100), así como también todas las funciones necesarias para la preparación y organización del evento electoral (OEA, 2014). Y por el otro, la campaña electoral propiamente dicha en la que los candidatos llevan a cabo actividades orientadas a la

captación del voto, realizando campañas institucionales de tipo informativo…" (CASTELLÁ ANDREU, 2018).[5]

Mediante actos de difusión, publicidad, presentación de planes, proyectos y debates los candidatos buscan captar la voluntad política del electorado, siempre dentro de un clima de tolerancia democrática (CÓDIGO ELECTORAL NACIONAL ARGENTINO, 1883).

2.1.1.- Marketing Político y el uso de la desinformación para manipular al electorado

En las campañas electorales los candidatos y sus estructuras políticas retoman el contacto con los ciudadanos en búsqueda de lograr la confianza del votante. En sus comienzos, la comunicación política seguía un modelo vertical donde el político centralizaba y controlaba el mensaje, y el rol de los electores era completamente pasivo, reducido a recibir y asimilar esa información, siendo su única reacción la emisión del voto (RUBIO, 2010).

Este modelo de comunicación ha ido transformándose desde la irrupción de las TICs e internet. Los ciudadanos se han convertido en los principales protagonistas de la campaña electoral, ya que, de ellos dependerá que el candidato alcance popularidad, reciba financiación y de que la campaña se viralice (RUBIO, 2010).

Lo que se busca en una campaña[6] es atraer la atención del público para provocar en él una determinada percepción que luego condicionará su comportamiento. La transmisión de información no depende sólo del emisor y el contenido de la misma, sino que depende sobre todo de la recepción que de la información hace el usuario (RUBIO NÚÑEZ, 2018).

Desde la irrupción de internet y con el crecimiento de las herramientas tecnológicas al servicio de la comunicación, las TICs se transformaron en uno de los pilares fundamentales

[5] En el caso de España, la campaña electoral conforme lo determina la LOREG dura entre 15 y 21 días y finaliza a las cero horas del día anterior a la votación, dicho día tiene lugar la jornada de reflexión (CASTELLÁ ANDREU, 2018). En Argentina conforme al articulo 64 bis del Código Electoral Nacional *"*La campaña electoral se inicia cincuenta (50) días antes de la fecha de las elecciones generales y finaliza cuarenta y ocho (48) horas antes del inicio de los comicios*"*. Los plazos varían según cada Estado, pero la finalidad es la misma: captar la voluntad política del electorado.

[6] Es menester destacar que las cuatro funciones esenciales que se persiguen en la campaña electoral son la información, la financiación, la interacción y la movilización e integración de la misma. Por ende, cuando se planea la estrategia de la campaña, las tecnologías son aliadas para lograr las funciones mencionadas, siendo indispensable un planteamiento online de la comunicación política a realizarse (RUBIO, 2010).

de la construcción de las estrategias electorales, siendo las redes sociales las principales protagonistas.

Los usuarios comparten, muestran y publican en las redes sociales todo tipo de información sobre ellos, como el estado civil, lugar de residencia, edad, creencias políticas y religiosas, tipo de estudios, *curriculum* profesional, lugar de trabajo, correo electrónico, entre otros. Además de toda la información otorgada directamente por el ciudadano, también se puede cruzar con otras redes imágenes, videos, cantidad y tipos de usuarios "amigos", grupos de pertenencias y aplicaciones que utiliza regularmente (CALDEVILLA DOMÍNGUEZ, 2010).

Con toda esa información al alcance, y la gestión de grandes cantidades de datos podemos ir definiendo el perfil del electorado al que se dirige la campaña, clasificándolo según su nivel socioeconómico, cultural, zonas de residencia, preferencias, etcétera, (CALDEVILLA DOMÍNGUEZ, 2010) contando como resultado con una base de datos organizada y abundante que permita una integración completa de cada uno de los sujetos involucrados.

El objetivo es que el mensaje político llegue de manera eficaz a la ciudadanía, entonces a mayor número de personas a las cuales tenemos acceso, con incontable información obtenida de cada uno de ellos, más cerca del éxito estará nuestra campaña y se logrará que llegue el mensaje que deseamos, ampliando exponencialmente el número de comunicaciones eficaces hacia los posibles votantes (RUBIO, 2010).

Pero tal como hemos analizado en el capítulo anterior la tecnología puede afectar de manera negativa a la democracia, y el momento del proceso democrático dónde más se percibe esta afectación es en la campaña electoral (RUBIO NÚÑEZ, 2018).

Ello es así conforme a que, las bondades mencionadas sobre la aplicación de la tecnología en esta etapa del proceso electoral también son utilizadas para lograrse campañas de desinformación exitosas, siendo el arma infalible de las mismas las ya mencionadas *fake news*.

Las *fake news*[7] que se incluyen en las campañas de desinformación desorientan y engañan a los ciudadanos, provocando que cambien de postura en asuntos importantes, así como también pueden reforzar ideas y prejuicios, convirtiéndolo en un agente electoral partícipe de la campaña activamente. Es decir, si el ciudadano está en contra de un candidato y se encuentra en alguna red social una información o fotografía que lo ridiculice o culpe de algún hecho, compartirá o comentará dicha noticia con el fin de que mayor cantidad de personas accedan a la misma (LÓPEZ AGUIRRE, ACOSTA VALVERDE y ESTRADA GARCÍA, 2019).

Como se mencionaba previamente las grandes bases de datos, bien alimentadas con información actualizada y cruzada entre todas las redes sociales y demás sitios que se tiene simple acceso a través de internet, permite dividir a los electores según sus preferencias políticas y creencias, pudiendo realizarse una campaña de desinformación dirigida, acorde al receptor del mensaje, con grandes probabilidades de éxito en la manipulación (ya sea afirmando la elección o ayudando a definirla) de su decisión respecto al candidato electoral.

Por ende, las nuevas tecnologías facilitan el conocimiento más profundo del electorado y torna más accesible su manipulación. Así, las comunicaciones se vuelven personalizadas y la influencia en la opinión pública consigue realizarse con éxito, (CALDEVILLA DOMÍNGUEZ, 2010), poniendo en jaque la libre decisión que debe realizar el electorado sobre su voto.

[7] Nos podemos encontrar con distintos tipos o características de las *fake news*, la forma de presentación de las mismas se adapta a cada campaña de desinformación. Sin embargo, los rasgos comunes y que se aprecian con regularidad corresponden a noticias que se presentan como periodísticas sobre un hecho que jamás ocurrió, pero se distribuyen, y ello genera confusión y engaño en el lector. También aparecen noticias con información verdadera pero expuesta fuera de contexto, es decir, el protagonista no dijo lo que se interpretó en la nota publicada. Son noticias sensacionalistas, buscan generar emociones en el lector que lo lleven a actuar sin pensar en la veracidad o no de lo que está leyendo. Se utilizan titulares para llamar la atención, y quien recibe no lee el cuerpo del mensaje, que en realidad no coincide o dice lo contrario al titulo de la nota. No se citan o son de dudosa procedencia las fuentes, nombres de personas involucradas en el supuesto hecho, ni se dan pruebas o evidencias de declaraciones, por lo tanto, no es posible o se torna difícil comprobar su veracidad. Algo que se usa mucho en el contexto electoral es el uso de fotografías antiguas o de otros países o zonas geográficas y se las hace pasar como actuales y/o propias del lugar donde se publican. El uso de nuevos medios sociales, portales o cuentas de redes sociales de reciente creación y sin un claro origen también forma parte de las *fake news*. Con un nivel más experto en tecnologías, se publican videos o imágenes manipuladas o alteradas y se realizan montajes, logrando que el candidato o el protagonista de la notica diga y haga lo que el artífice de la campaña desea (LÓPEZ AGUIRRE et.al., 2019).

2.1.2.- La tecnología detrás de la desinformación: algoritmos y bots a la orden del día

Como venimos analizando en este trabajo los beneficios que conlleva el uso de las TICs en los distintos ámbitos de nuestra vida, también se utilizan para mejorar y ampliar los métodos para desinformar y manipular a los usuarios (OFICINA DE SEGURIDAD DEL INTERNAUTA [OSI], 2020).

Las campañas de desinformación no lograrían su objetivo de manipular a la opinión pública de manera exitosa, si no contaran con tantas herramientas tecnologías que permiten la viralización del contenido de manera automática y rápida.

La mayoría de los usuarios con los que nos encontramos en el ciberespacio no son personas reales, la información que observamos en sus perfiles no coinciden con la de una persona humana identificable en otras fuentes (CCN, 2019).

Esto es posible gracias a que las redes sociales y las plataformas digitales de comunicación social permiten que se creen cuentas anónimas y que se utilice software para la automatización y gestión de esos perfiles, permitiendo que se puedan lanzar campañas de desinformación que alcancen un gran volumen y difusión en redes sociales (CCN, 2019).

Los "bots políticos" se encuentran entre las últimas herramientas de los equipos de campañas digitales, ya que esta tecnología juega un papel determinante en la dirección del sentimiento público y la manipulación de las opiniones del electorado (HOWARD, WOOLLEY & CALO, 2018).

Los "bots[8] políticos" son scripts automatizados diseñados para influir en la opinión pública a través de cuentas usuarios que han sido equipadas con las funciones o el software

[8] El termino *bot* "viene de "robot". Es un programa informático cuya función es realizar tareas automatizadas a través de Internet, generalmente funciones simples que requieren de cierta repetición. Los comandos pueden estar programados en el bot o ejecutarse mediante scripts, para que se lleven a cabo cuando se aplican ciertos criterios. El bot también puede recibir instrucciones en forma dinámica conectándose a uno o más servidores de Comando y Control" (WE LIVE SECURITY, 2020). Asimismo, es menester conocer el termino *Botnet* que surge de la "Combinación de las palabras "robot" y "network". Es un grupo de equipos infectados por códigos maliciosos que se comunican entre sí y/o con su servidor(es) de Comando y Control, controlados por un atacante de modo transparente al usuario, disponiendo de sus recursos para que trabajen de forma conjunta y distribuida. Cada sistema infectado (zombi) interpreta y ejecuta las órdenes emitidas" (WE LIVE SECURITY, 2020).

adecuado, para automatizar la interacción con otras cuentas sobre política. Estos algoritmos[9] analizan la información y toman decisiones generando contenido e interactuando con usuarios humanos en los distintos sitios webs (HOWARD, et. al., 2018).

Otra manera de utilizar a los *"*bots políticos" es para aumentar el número de seguidores y fingir una mayor popularidad en los perfiles de las redes sociales de los candidatos y agentes políticos (HOWARD, et. al., 2018).

"Los algoritmos que utilizan las nuevas plataformas de comunicación digital, como las redes sociales, se han convertido en aliados involuntarios de las campañas de desinformación" (CCN, 2019:30), ya que las tecnologías implementadas están diseñadas para que el usuario reciba e interactúe únicamente con mensajes que se alinee con sus ideas y sentimientos, ofreciendo información de sus preferencias políticas, más allá de la veracidad y calidad del contenido (CCN, 2019).

Como podemos apreciar la comunicación política automatizada implica la creación y transmisión en forma masiva de contenido político importante a través de redes sociales y demás medios de comunicación digital, generando preocupación y riesgos para un proceso electoral justo y transparente (HOWARD, et. al., 2018), ya que gracias a las bondades de las tecnologías la viralización de información falsa y la manipulación de la opinión pública se torna cada vez más sencillo.

Es menester resaltar una nueva tecnología que se está utilizando para acompañar las *fake news* y tornar cada vez más creíbles las campañas de desinformación, se denominada *deepfakes.*

Cuando hablamos de *deepfakes*[10] nos referimos a "vídeos manipulados para hacer creer a los usuarios que los ven, que una determinada persona, tanto si es anónima como si es personaje

---

[9] "Un algoritmo es un conjunto ordenado y finito de operaciones que permite hallar la solución de un problema. Está definido por instrucciones o reglas bien definidas, ordenadas y finitas que permiten realizar una actividad. Dado un estado inicial, una entrada y una secuencia de pasos sucesivos, se llega a un estado final y se obtiene una solución" (MARTÍNEZ LADRÓN DE GUEVARA, 2013:7)

[10] *"*La palabra *deepfake* es un término combinado de *deep learning* y *fake*, es decir: *Deep learning* o aprendizaje profundo hace referencia a una de las ramas de la inteligencia artificial. *Fake* o falso, hace referencia a la elaboración de falacias en la red, del mismo modo que las *fake news*" (OSI, 2020).

público, realiza declaraciones o acciones que nunca ocurrieron. Para la creación de dichos vídeos, se utilizan herramientas o programas dotados de tecnología de inteligencia artificial que permiten el intercambio de rostros en imágenes y la modificación de la voz" (OSI, 2020).

Lo peligroso de esta tecnología es la facilidad para crear este tipo de videos, ya que con una simple aplicación cualquier persona tiene acceso a generarlos, y al ritmo que avanza la tecnología en poco tiempo será cada vez más difícil identificar si es un video falso o no (SANZ ROMERO, 2019).

Gracias a las redes sociales, y al impacto que puede llegar a crear un video de autoridades políticas o personas públicas "diciendo" algo alarmante o llamativo, la viralización es inmediata y se extienden por todo internet resultando una amenaza para la sociedad al tener implicaciones sociales y políticas (OSI, 2020).

La importancia radica como ciudadanos en ser precavidos y empezar a educarnos en el mundo digital, logrando de manera crítica asimilar la información que recibimos constantemente gracias a las TICs, pudiendo seleccionar y discriminar cuando estamos frente a una *fake news* o un video adulterado, o por lo menos dudar del contenido que recibimos y hacer una investigación pertinente, si es que en dicha información basaremos nuestra elección a la hora de una votación.

2.2 Celebración de elecciones y proclamación de electos

Las operaciones realizadas durante esta etapa son aquellas relativas a la captura del voto (votación) y actividades pertinentes a la contabilización, transmisión y divulgación de resultados (OEA, 2014).

En esta etapa del proceso la tecnología puede intervenir de diversas maneras: para emitir el voto, para el conteo de los mismos[11], para la gestión dentro de los centros de votación[12]

[11] Al cierre de la jornada electoral se efectúa la contabilización de los votos. El proceso a seguir para contar los votos debe ser preciso, rápido e íntegro. Para ello, la automatización del conteo incluye herramientas de soporte al personal electoral para agilizar la labor de los mismos (OEA, 2014).

[12] Si durante la jornada electoral se requiere información sobre la elección, el software de gestión de centros de votación permite un centro de soporte para evacuar dudas e informar de manera fluida a todos los agentes involucrados en las elecciones (OEA, 2014).

así como también para la trasmisión[13] y publicación de resultados.

Nos encontramos dentro de una revolución tecnológica y de la información, donde se busca extender los beneficios y la injerencia de las tecnologías al máximo número de aplicaciones funcionales o ámbitos posibles (GONZÁLEZ DE LA GARZA, 2009), entre ellos la emisión del voto.

Cuando hablamos de procesos electorales, estamos hablando de democracia, de la base de nuestros estados, y por eso es necesario que se respeten las garantías que cada Constitución establece sobre el sufragio (TULA, 2012).

Cualquiera sea la fórmula especifica que acoja el Derecho Constitucional de cada Estado democrático, se recoge un núcleo mínimo de principios y garantías, que como mencionáramos anteriormente consiste en el carácter universal, igual, libre y secreto del voto, (DELGADO-IRIBARREN Gª-CAMPERO, 2008), y la importancia de la neutralidad, integridad, seguridad y fiabilidad del procedimiento electoral (GONZÁLEZ DE LA GARZA, 2009).

Se puede aprovechar las bondades de la tecnología para generar procesos más transparentes, ágiles y que den confianza, pero ello no se logra de un día para el otro (TULA, 2012), debiendo velar por qué las facilidades aportadas por las TICs, no sean en detrimento de principios y garantías reconocidas y adquiridas por el derecho constitucional (DELGADO-IRIBARREN Gª-CAMPERO, 2008).

“Las amenazas al proceso electoral en esta fase tienen que ver con los obstáculos al ejercicio del voto o con fórmulas que alteran el secreto del voto o su propio sentido” (RUBIO NÚÑEZ, 2018b:120).

Si dejamos a cargo de ceros y unos algo tan importante como la decisión de quiénes serán los futuros gobernantes de un Estado, debemos extremar las medidas de seguridad y así poder garantizar al electorado y a los partícipes de las elecciones, que el voto seguirá siendo secreto e íntegro y que nadie manipulará la libre elección de cada ciudadano que emitió el

[13] Utilizar tecnologías que permitan transferir datos de maneta electrónica a los centros de procesamiento de resultados facilita el proceso de cómputo y permite mayor rapidez y precisión para divulgar los resultados (OEA, 2014).

sufragio (DELGADO-IRIBARREN Gª-CAMPERO, 2008; GONZÁLEZ DE LA GARZA, 2009; TULA, 2012).

El desarrollo de nuevas tecnologías y su inclusión en las votaciones, requiere de un proceso de revisión de las normas electorales ya que, en general, la mayoría de la normativa vigente está relacionada con el manejo manual de los sistemas y ante una eventual reforma deberá hacerse con la debida cautela para evitar desconfianza en los electores (GARCÍA RODRÍGUEZ, 2011).

En base a todo lo expuesto, en este trabajo nos limitaremos a analizar dos modalidades en las cuáles puede intervenir la tecnología en el momento de la votación: el voto electrónico y el voto por internet.

2.2.1.- Voto electrónico

"La votación es el momento clave de la elección, el momento en el que los votantes ejercitan su derecho de elegir a sus representantes" (RUBIO NÚÑEZ, 2018b:14). Podemos distinguir entre dos modalidades básicas de emisión del sufragio (OEA, 2014; PANIZO ALONSO, 2007):

- *Presencial*, donde el elector se apersona al recinto electoral, se identifica físicamente como votante válido, y en una cabina aislada ejerce el sufragio.
- *Remota*, tanto la validación de su identidad, como la elección del voto y la captura del mismo se realiza fuera del recinto electoral, es decir, de forma remota, utilizando medios telemáticos.

Dentro de la modalidad presencial podemos encontrar distintas tecnologías[14] aplicables a la votación entre ellas incluimos al voto electrónico.

[14] Una tecnología que se puede aplicar consiste en escáneres ópticos digitales, que son dispositivos de contabilización de boletas electorales. El elector selecciona al candidato marcando en la boleta de papel y luego es colocada en el dispositivo. El escáner realiza la lectura de las marcas, captura una imagen digital de la boleta y almacena el voto en la memoria tras ser contabilizado. Algunos de estos escáneres transmiten directamente los votos desde el dispositivo hacia un centro de resultados (OEA, 2014). La ventaja de esta tecnología consiste en que al existir una copia papel del voto, en los supuestos de sospecha de fraude o manipulación, se puede corroborar manualmente entre el soporte papel y el electrónico, teniendo validez los datos de recuento manual en tales supuestos de fraude (GONZÁLEZ DE LA GARZA, 2009).

Cuando votamos con ayuda de una máquina dispuesta en un lugar específico, y para poder acceder a la misma, previamente, tenemos que ser identificados manualmente como electores y autorizados a utilizar la máquina, estamos frente a lo que se denomina sistema de registro electrónico directo -*Direct Recording Electronic*- (PANIZO ALONSO, 2007).

Estos dispositivos permiten al elector seleccionar sus candidatos directamente desde la máquina, desde una pantalla táctil o a través de dispositivos periféricos como tabletas o teclados numéricos. Una vez realizada la votación, la captura y contabilización del voto es inmediata. Algunos equipos generan un recibo en papel como constancia de emisión del voto, depende del dispositivo utilizado. Asimismo, las maquinas DRE pueden transmitir directamente los votos hacia un centro de resultados, si se los configura y habilita al efecto (OEA, 2014).

La decisión de implementar tecnologías en los procesos electorales, como el denominado voto electrónico directo, obedece a que se busca facilitar la emisión del sufragio, garantizar transparencia en las votaciones, lograr inmediatez en el escrutinio y reducir el tiempo de espera entre el cierre de los comicios y el recuento de los votos, así como también lograr una difusión del resultado con mayor rapidez (GARCÍA RODRÍGUEZ,2011), entendiéndose que estos objetivos gracias a la excelencia y operatividad tecnología se lograran eficientemente.

Las máquinas de registro electrónico directo, generan interrogantes con relación al sufragio, toda vez que el votante tiene que presumir que su voto ha sido debidamente contabilizado (GONZÁLEZ DE LA GARZA, 2009). "Así pues, tendrán que aceptarse como hechos consumados los datos entregados por un procedimiento automático cuyo funcionamiento se desconoce y, por lo tanto, tampoco puede controlarse" (BARRAT I ESTEVE, 2009:2).

Surgen muchas dudas sobra la necesidad real de aplicar tecnologías para resolver los procesos electorales, sobre todo este tipo de máquinas, lo cierto es que la seguridad del proceso de votación se pone en jaque entendiendo que la tecnología conlleva demasiados riesgos (PANIZO ALONSO, 2007).

La seguridad del voto va a depender de dos partes, la parte técnica y el procedimiento. Este último es el más débil, ya que, como nos basamos en normativa que se hereda de los procesos electorales clásicos, pensados para votaciones manuales, físicas, sin tecnologías, se torna

insuficiente lo existente para garantizar la seguridad en el voto electrónico (PANIZO ALONSO, 2007).

Al ser un sistema completamente nuevo el que se implanta en comparación con lo tradicional, con el papel y el recuento manual, es de suma importancia "…reforzar todos los mecanismos de control y supervisión con el objeto de brindar seguridad y garantizar el principio de integridad del sufragio" (TULA, 2012:4).

En los mecanismos informáticos de votación, la auditoría del procedimiento, tanto de forma previa como posterior, en un factor fundamental, pero que no pueden realizar los propios electores al carecer de los conocimientos necesarios (BARRAT I ESTEVE, 2009).

Atendiendo a la complejidad técnica de los datos solo podrán entenderlos un núcleo reducido de especialistas, pudiendo difundir los mismos sus conclusiones sobre el sistema, generando en la ciudadanía suficiente confianza en la tecnología utilizada si los expertos no tienen objeciones (BARRAT I ESTEVE, 2009).

Para ello se necesitarán crear nuevos agentes dentro del proceso electoral, requiriéndose personal con conocimientos técnicos, pero también con experiencia en materia electoral. Ya no tendremos solo "fiscales partidarios" sino que también necesitaremos "fiscales informáticos" (TULA, 2012).

Los sistemas de voto electrónico plantean el desarrollo de nuevas y costosas estructuras institucionales (GONZALEZ DE LA GARZA, 2009), los estados deben plantearse que tipo de *hardware* y *software*[15] utilizaran siendo necesario formar comités de expertos (TULA, 2012) para llevar a cabo el análisis y tomar la decisión que mejor se adapte al caso concreto.

Hay que tener en cuenta las consecuencias sociales que genera el voto electrónico, "la diversidad de mecanismos electrónicos de votación, las diferencias entre regulaciones y,

[15] Lo primero que se tendrá que decidir es si se generara un desarrollo propio dentro del país o se realizará una oferta pública para que proveedores especializados ofrezcan sus servicios, decidiendo por software libre que permite modificarse acorde las necesidades de cada estado, o una licencia de software propietario a medida (TULA, 2012). Lo cierto es que el software electoral debería estar disponible, publicarse y permitir su revisión y prueba en búsqueda de fallos, garantizar una inspección completa del sistema informático destinado al sufragio electrónico (GONZALEZ DE LA GARZA, 2009), una auditoría por parte de expertos que genere confianza a los electores.

sobre todo, la pluralidad de escenarios donde han de aplicarse aconsejan huir de estereotipos predeterminados" (BARRAT I ESTEVE, 2009:11), entendiendo que la tecnología para ejercer el voto tendrá que adaptar su estructura a las diferentes realidades sociales de cada país.

El electorado debe sentirse seguro, entender y confiar en el sistema, de no ser así toda la tecnología implementada en pos de agilizar el proceso se vuelve en contra, generando un quiebre en la libertad de elección, en la integridad y secreto del voto ya que el ciudadano no sabrá si ello se está cumpliendo (TULA, 2012).

No nos olvidemos que necesariamente deben garantizarse ciertos principios electorales, sea cual sea el sistema electrónico elegido. El secreto y autenticidad del voto y del votante, la fiabilidad de los resultados escrutados, el principio de participación y de la credibilidad de la sociedad en el sistema, así como también el reparo en que los costos de implementación sea una inversión amortizable (GARCÍA RODRÍGUEZ, 2011), son claves a la hora de que la ciudanía seleccione una tecnología que se adapte a su cultura electoral (BARRAT I ESTEVE, 2009).

En conclusión, "la aplicación del voto electrónico no sólo supone la incorporación de máquinas electrónicas el día de los comicios sino, más bien, se trata de un profundo y gran cambio con impactos diferenciados en el orden social, jurídico y político". (TULA, 2012:19).

2.2.2.- Voto por Internet

Como acabamos de analizar, el voto electrónico es un sistema complejo que no se encuentra perfeccionado como para aplicarse a nivel global y que su mayor defecto recae en los riesgos de seguridad que conlleva la tecnología aplicable, pudiendo vulnerase los principios básicos garantistas del proceso electoral, y todo ello se incrementa en la votación por internet.

La modalidad de voto por internet, se encuadra dentro de una votación completamente telemática, remota, donde se hace uso de la infraestructura pública de internet para el registro, emisión y conteo del voto (OEA, 2014).

En base a los principios generales de integridad y secreto del voto, será necesario implementar diferentes niveles de seguridad y así afianzar la integridad del proceso en todas sus partes, garantizando que la selección de candidatos registrada por el votante ha sido emitido conforme a la intención del mismo con el fin de asegurar su libertad, que el almacenamiento ha sido conforme a su emisión respetando el secreto, y que ha sido computado según lo almacenado evitando que pueda ser adulterado (OEA, 2014; RUBIO NÚÑEZ, 2018b).

La aplicación del voto por internet se fundamenta en ciertas ventajas como la independencia del tiempo y del espacio permitiendo a los electores el registro de su voto, aun cuando no puedan hacer acto de presencia en los centros de votación habilitados, posible incremento de la participación en las votaciones gracias a evitar los desplazamientos y reducción de costos (OEA,2014; PANIZO ALONSO, 2007).

Sin embargo, las ventajas no son suficientes como para considerar esta opción de voto remoto adecuada, y surgen muchísimos interrogantes alrededor de la misma. Para decidir cambiar el modelo de proceso electoral que se utiliza en la actualidad, debemos encontrar una solución óptima que sea funcionalmente equivalente o mejor al sistema que se cuenta actualmente (GONZÁLEZ DE LA GARZA, 2009), y *a priori* podemos aseverar que tanto el sistema manual y papel, hasta la votación electrónica directa, respetan más las garantías del proceso y voto, que si se realizara por internet.

"Un diseño de voto electrónico remoto, bien desarrollado, es un reto de una gran complejidad y en el que, de partida, hay que renunciar a obtener una fiabilidad equivalente a la de un proceso de sufragio presencial" (GONZÁLEZ DE LA GARZA, 2009:215).

Se plantea numerosos interrogantes desde el punto de vista legal y de seguridad que ponen en jaque los principios del procedimiento electoral democrático (BARRAT I ESTEVE, 2012). Debemos pensar que el elector utilizará su ordenador personal a la hora de emitir su voto, lo cual plantea grandes dudas sobre la seguridad, ¿se encuentra el ordenador del elector libre de *malware*[16] para garantizar jurídicamente que el sufragio ha sido libremente emitido

[16] "Acrónimo de las palabras *"malicious*" (del inglés, "malicioso") y "*software*"…Es un programa o aplicación diseñada con algún fin dañino. Se considera *malware* a distintos tipos de amenazas, cada una con características particulares (troyano, gusano, virus, entre otros) y con métodos de propagación e instalación distintos" (WE LIVE SECURITY,

sin modificación alguna por terceros que maliciosamente tengan control del ordenador?, ¿cómo pueden el órgano electoral competente controlar y verificar que el *software* electoral proporcionado vía Internet, se ha instalado y configurado correctamente y que no ha sido infectado u "obligado" a ejecutar instrucciones no deseadas? , ¿ hay garantías de que el votante que realiza la acción es el titular legitimo del derecho a ejercer el sufragio pasivo? (GONZÁLEZ DE LA GARZA, 2009).

Como se puede observar el voto por internet genera serias dudas sobre su compatibilidad con la libertad del sufragio y el secreto del voto, así como también puede interferir en el principio de igualdad ya que sustituir por completo los mecanismos tradicionales conocidos y acuñados por los ciudadanos crea una obligación de adaptarse a nuevos sistemas que algunos electores pueden tornarse reticentes. En adhesión, el control del sistema no puede realizarse por ciudadanos u observadores electorales sin conocimientos técnicos, requiriéndose agentes especializados en la materia, sobre todo en tecnología (BARRAT I ESTEVE, 2012).

Por el momento no es posible garantizar, en base a la tecnología, que se podrá cumplir y respetar los principios esenciales del sistema electoral. La universalidad**,** la igualdad de sufragio, la libertad y el secreto, están en riesgo si con el sólo hecho de que el ordenador esté conectado a internet permite que se pueda interceptar, conocer, modificar y hasta eliminar, mediante distintas técnicas, el contenido del sufragio.

Por lo expuesto, y retomando lo que se mencionaba en el apartado de voto electrónico, el seleccionar una tecnología de este tipo para emitir el sufragio, tiene que acompañarse de cambios sociales, jurídicos y políticos, teniendo que evaluarse objetivamente la conveniencia de incorporar en este caso un sistema en internet al proceso electoral, analizando los riesgos que conlleva y priorizando siempre el respeto de las garantías y principios constitucionales-electorales.

2.3 La Postcampaña

La etapa post electoral va a integrar todas aquellas actividades que surgen una vez finalizado el día de las votaciones, así, por ejemplo, se lleva a cabo la rendición de cuentas sobre la financiación y los gastos de la campaña por parte de los partidos políticos, se elaboran estadísticas electorales sobre las elecciones (OEA, 2014), y lo más importante comienza el período de control de legalidad de la elección.

Lo cierto es que como hemos mencionado en este trabajo las TICs permiten que una vez finalizada la celebración de elecciones y proclamación de electos, las campañas de desinformación se basen en poner en dudas la legitimidad y transparencia del proceso, amenazando y debilitando la confianza de los electores en la democracia, frente a las dos fases anteriores que afectarían a la legalidad.

2.3.1.- La tensión entre legalidad y legitimidad en el contexto de desinformación, nuevas tecnologías y procesos electorales

Todo sistema jurídico tiene que descansar en dos pilares, legalidad y legitimidad. La esencia de la democracia radica en cumplir el estado de derecho – *rule of law*- pero a su vez los ciudadanos deben apoyar ese estado, y eso no se consigue solo en base a la legalidad, a los presupuestos legales, sino que se consiguen logrando que también sean legítimos.

Mientras la afectación de la manipulación desde las nuevas tecnologías y tecnologías de la información en las fases de campaña electoral, proclamación de candidatos, votación y proclamación de electos se reconduce al ámbito de la legalidad, la incidencia de éstas actuaciones en un momento posterior afecta a la legitimidad (SCHMITT, 2006).

Una acción es legitima en la medida que se ajusten a las normas jurídicas, sin embargo, los principios de legitimidad tienden a ir mas allá del mero cumplimiento de la norma, convirtiéndose en una guía orientativa, *supralegal* (SCHMITT, 2006) que permanece a pesar de las vicisitudes que se presenten con el precepto normativo.

Si las etapas electorales son desarrolladas conforme a la legalidad del proceso pero en la etapa post electoral se pone en duda ello y se está constantemente objetando lo ocurrido, la

creencia y apoyo del ciudadano en el sistema se ve debilitado, llevando así a que la legitimidad de las elecciones se encuentre en la mira.

2.3.2.- La desinformación no descansa: un permanente cuestionamiento de la legitimidad de las elecciones

En esta etapa veremos la consecuencia de la utilización de tecnologías en las etapas anteriores. Ante el desconocimiento del ciudadano sobre sistemas e informática, y al verse inmerso en el uso de las máquinas o de internet para poder ejercer su derecho a voto sin terminar de comprender cómo funciona el procedimiento, es más simple que se pueda poner en dudas la transparencia de lo sucedido y así las campañas de desinformación sean exitosas.

Es una realidad que el fantasma del fraude en una elección siempre aparece más allá del método utilizado para que se lleven a cabo las mismas, sin embargo, la tecnología al ser entendida por pocos permite que sea más fácil instalar la sospecha.

Convengamos que los propios políticos generalmente usan este artilugio para descalificar al contrincante y seguir desde un papel de oposición ejerciendo presiones y demás juegos de la política. Lo importa es hacer la distinción en esta etapa del marketing político, por llamarlo de una manera, y las herramientas jurídicas que permiten accionar ante un posible fraude en las elecciones.

No importa en qué país nos encontremos, el estado democrático en su normativa sobre el proceso constitucional brindará herramientas, recursos, para que si se tiene una sospecha fundada sobre un fraude, falla o manipulación durante el proceso, la justicia pueda investigar y fallar al respecto, con el fin siempre de proteger la democracia.

Las exigencias de control frente al fraude, la participación activa del ciudadano en las funciones de control y la publicidad sobre el procedimiento llevado a cabo, son las claves fundamentales sobre las que se construye todo el proceso electoral (GONZÁLEZ DE LA GARZA, 2009).

Es fundamental contar con estos mecanismos, sobre todo, si se utiliza la tecnología para ejercer el sufragio, ya que, al no ser comprendida por toda la sociedad y teniendo el ciudadano que confiar y delegar la auditoría y control en expertos, es garantía para los

electores saber que sus representantes legitimados al efecto, podrán iniciar recursos que peticionen las verificaciones correspondientes si se duda en la legalidad de la elección.

"Es preciso eliminar cualquier atisbo de desconfianza y procurar la mayor transparencia posible. Por eso, concluido el proyecto deberán establecerse diferentes procedimientos de validación del sistema, con controles y auditorias tanto de representantes de los partidos políticos como de otras instituciones públicas y privadas interesadas" (DELGADO IRRIBARREN GA-CAMPERO, 2008:21).

La Constitución Española en su artículo 70.2 establece que el mecanismo de control de los procedimientos electorales se realizará por vía judicial. Para ello cuenta, entre otros, con el *recurso contencioso electoral*, dirigido contra los acuerdos de las juntas electorales sobre proclamación de electos y contra la elección y proclamación de los presidentes de las corporaciones locales (LO 5/1985, art.109), *el recurso contra los acuerdos la proclamación de candidaturas y candidatos*, se interpone contra los acuerdos de proclamación de las juntas electorales sobre candidaturas y candidatos (LO 5/1985, art. 49), y el *recurso de amparo electoral*, que procede contra sentencias contencioso-administrativas dictadas en procesos electorales (LO 5/1985 art.49.3 y 4, 114.2).

Estos recursos mencionados, tienen plazos muy cortos para su interposición[17], teniendo en consideración los procesos de publicación de candidatos, electos, etc., tomemos un período genérico de tres meses donde se podría poner en dudas judicialmente algún acto del proceso electoral, y realizar las acciones jurídicas pertinentes.

Más allá de los plazos previstos en la norma -los cuales acertadamente son cortos-, no puede ser cuestionada la transparencia y legalidad de las elecciones indefinidamente, sería una gran falla a la democracia y a la seguridad jurídica.

[17] Si hablamos del *recurso contencioso electoral* se debe interponer tres días siguientes al acto de proclamación de electos; el *recurso contra los acuerdos de proclamación de las juntas electorales* se extiende el plazo por dos días desde la publicación de los candidatos proclamados; el *amparo electoral* se podrá imponer en un plazo de dos días o tres, desde que se notifica la sentencia que agota la vía jurisdiccional, dependiendo del recurso que dio origen a la misma (EL DERECHO, 2015).

Pero para las campañas de desinformación ello no es problema, y más cuando la tecnología permite fácilmente sembrar la duda sobre el procedimiento, toda vez que, el ciudadano no comprende el mismo y ante lo desconocido es más simple instalar las sospechas.

Debería entonces, y como ya se mencionara anteriormente, la norma prever mecanismos de auditoría y control de la transparencia del proceso y de cómo funcionó el sistema durante la elección, contándose con la actualización de los recursos jurídicos previstos contemplando la situación de las nuevas tecnologías.

Es decir, tal vez se requiere mayor plazo para auditar el sistema cuando es tecnológico por tener que recurrir a expertos, o viceversa, sea cual sea el caso, que los plazos procesales se adecuen con relación a la modalidad del proceso.

No dejemos de tener en mente, que el fin último es proteger las garantías electorales y resguardar al estado democrático, y que más allá del "juego político", si se tienen sospechas fundadas de un fraude, se debe estar a lo regulado jurídicamente, lo demás es otra maniobra más de la eterna campaña política.

CAPÍTULO TERCERO: LAS RESPUESTAS JURÍDICAS

3.1 Reacción del derecho ante el uso de las TICs en los procesos electorales

Como venimos analizando en este trabajo, las TICs se volvieron parte de nuestra vida, se convirtieron en aliadas para agilizar múltiples tareas y ante tantas bondades, los Estados, por un lado, y los mismos ciudadanos, hicieron que también se involucren en los procesos electorales.

No podemos negar la existencia de las TICs, y la importancia de internet, nos encontramos en un mundo digitalizado, donde obtenemos muchas cosas con un solo *click*, por eso el derecho no puede quedar ajeno a la situación.

Es una tarea difícil regular sobre temas relacionados con la tecnología, ya que, los procedimientos legales llevan un tiempo para consumarse y las herramientas tecnológicas avanzan con rapidez.

Sin embargo, cuando estamos hablando de la injerencia de distintas tecnologías en procesos que son pilares para el estado democrático como lo son los procesos electorales, el derecho debe encontrar la manera de regular, prever y contener distintas situaciones que se puedan generar en pos de proteger los principios fundamentales de la democracia.

3.1.1.- Planteamiento general de la UE sobre desinformación.

Las campañas de desinformación y las *fake news* que las incluyen, como hemos analizado en los capítulos anteriores, fueron ganando protagonismo, afectando a múltiples sectores, teniendo consecuencias políticas importantes. Es por ello, que empezaron a surgir las demandas a la Unión Europea desde diferentes ámbitos, para que redoblara sus esfuerzos en la lucha contra las noticias falsas y la desinformación (DE CASTRO RUANO, 2018).

No necesariamente regular se refiere a leyes como fuente formal emanada por autoridad competente, sino que recomendaciones, códigos de buenas prácticas, protocolos de actuación, entre otros tipos de normativa, que se vuelven acordes para poder controlar el uso de la informática y garantizar el cumplimiento de los derechos electorales.

Por ello como corolario de un recorrido de años de estudio, documentación y trabajo, la UE decide crear el Código de Buenas Prácticas de la Unión en materia de desinformación, en adelante el Código, con el fin de luchar contra la desinformación coordinándose con los distintos agentes públicos y privados vinculados a este fenómeno.

A continuación, repasaremos las iniciativas y comunicaciones más importantes que llevaron a la realización del Código.

3.1.2.- Marco Jurídico Unión Europea contra la desinformación

Desde el 2015 la UE viene combatiendo activamente la desinformación, lo cual surge por la preocupación de que potencias extranjeras, especialmente Rusia, lograran manipular los procesos electorales y vulnerar los principios democráticos de los Estados. Tras una decisión del Consejo Europeo en marzo de dicho año y con el fin de contrarrestar campañas de desinformación, se creó el Grupo de Trabajo *East StratCom*, adjunto al Servicio Europeo de Acción Exterior (COMISIÓN EUROPEA, 2019; TUÑON NAVARRO et.al., 2019).

Este grupo formó un equipo de comunicación que en colaboración con *fact checkers* y distintas fundaciones, denuncian la difusión de noticias falsas en los Estados orientales, centrándose en comunicar eficazmente las políticas de la UE a los países del Este, así como también apoyan medios de comunicación independientes, respaldando la libertad de los medios, y buscando mejorar la capacidad de la UE para prever, abordar y dar a conocer las actividades de desinformación (TUÑON NAVARRO et.al., 2019).

El Parlamento Europeo en su Resolución (2017) sobre las plataformas en línea y el mercado único digital destaca el incremento de la divulgación de las *fake news,* la necesidad de que los usuarios sean alertados cuando un contenido no es veraz, así como también la importancia de la libertad de intercambian opiniones y respetar la privacidad como elementos fundamentales democráticos. Ante ello solicita a la Comisión Europea que se analice la situación y el marco legal respecto a las noticias falsas y la situación jurídica para limitar la difusión de las mismas, verificando la posibilidad de una intervención legislativa.

Ante dicho pedido la Comisión Europea -en adelante la Comisión- a principios de 2018 impulsó la creación de un grupo independiente de alto nivel, el cual estaba formado por expertos representantes de redes sociales y empresas tecnológicas, *fact checkers*, medios de

comunicación, académicos y miembros de la sociedad civil. Este grupo sería el encargado de elaborar el "Informe del grupo independiente de alto nivel sobre *fake news* y desinformación en línea" para, delimitar el fenómeno de las noticias falsas y la desinformación y estudiar los posibles mecanismos legales y contramedidas para combatirlas (TUÑON NAVARRO et.al., 2019).

Otro hito importante fue el desarrollo por parte de la Comisión del denominado Eurobarómetro[18] diseñado con el fin de obtener datos y estadísticas sobre la conciencia y las actitudes de la ciudadanía de los Estados Miembros respecto de las noticias falsas, la desinformación en línea y la confianza en los medios de comunicación. Los resultados muestran una clara preocupación por la propagación de la desinformación en línea en Europa, y la relación del fenómeno con un conflicto para la democracia (EUROPEAN COMMISSION, 2018).

El Grupo de Expertos, ya referenciado, evaluó la responsabilidad sobre las noticias falsas en cuatro ámbitos: poderes públicos, plataformas de internet, medios de comunicación y sociedad civil, emitiendo su informe final en marzo de 2018 [19] .

Un aspecto importante que se realiza en el informe y nos interesa para este trabajo, es el análisis sobre la necesidad de legislar contra la desinformación o no hacerlo. Se interrogan acerca de si un marco jurídico enrolado en leyes seria lo acorde para decidir qué información es real y cuál no lo es. Al advertir los peligros de regular en este tópico, ya que podrían vulnerarse derechos fundamentales como la libertad de información y de prensa, la mayor parte de soluciones y propuestas planteadas no son de carácter legislativo. Por ello, se aboga

[18] La encuesta se realizó entre en febrero de 2018, fueron encuestados más de 26.000 ciudadanos de diferentes grupos sociales y demográficos, a través de vía telefónica y en su lengua materna.
Los resultados muestran que las noticias falsas están ampliamente difundidas en toda la Union Europea. Destacándose que El 37% de los encuestados se encuentran con noticias falsas todos los días o casi todos los días, el 85% percibe las *fake news* como un problema en su país y el 83% las percibe como un problema para la democracia en general (EUROPEAN COMMISSION, 2018).

[19] El informe cuenta con un enfoque multidimensional ya que se concluye que la desinformación es un problema multifacético por lo que no tiene tampoco una única solución. Por eso se aconseja basar las soluciones y análisis en cinco pilares: transparencia de las noticias y la circulación de datos en línea; promover la educación digital, con el fin de que el usuario esté preparado para navegar en entornos digitales; desarrollar herramientas técnicas para hacer frente a la desinformación; empoderar y colaborar con periodistas y medios para luchar contra la desinformación sosteniendo el ecosistema de los medios de comunicación; promover siempre la investigación continua sobre el impacto de la desinformación en Europa para evaluar las medidas tomadas por diferentes actores y ajustar constantemente las respuestas necesarias (EUROPEAN COMMISSION, 2018b).

por un código de buenas prácticas que incluya una serie de principios que las plataformas en línea y las redes sociales deberían hacer suyos (DE CASTRO RUANO, 2018).

Teniendo en cuenta el informe del Grupo de Expertos de alto nivel, el Eurobarómetro, la resolución del Parlamento Europeo mencionada y demás iniciativas de la Comisión[20] y entidades europeas, surge el Código de Buenas Prácticas contra la Desinformación que entra en vigor en octubre de 2018 y busca la unión de distintos agentes para luchar contra este fenómeno.

Es la primera vez que se aceptan estándares de autorregulación para combatir la desinformación, por los distintos agentes de la industria. No es solo un instrumento jurídico elaborado por la Unión Europea que busca luego de la adhesión de terceros, sino que se elaboró en conjunto con los actores involucrados en la lucha contra la desinformación, ello hace que el trabajo multidisciplinario augure una efectiva solución al fenómeno que se quiere controlar (COMISIÓN EUROPEA, 2019).

El Código fue firmado por las plataformas en línea Facebook, Google, Twitter y Mozilla, así como por los anunciantes y la industria publicitaria en octubre de 2018. Microsoft se unió en mayo de 2019, mientras que *TikTok*[21] firmó el Código en junio de 2020, lo importante es que cualquier otro interesado dentro de los perfiles que determina el Código puede adherir al mismo (EUROPEAN COMMISSION, 2020).

[20] Otros documentos importantes sobre el tema son las Conclusiones del Consejo del 28 de junio de 2018 (CONSEJO EUROPEO,2018) y la comunicación de la Comisión titulada "La lucha contra la desinformación en línea: un enfoque europeo" (COMISIÓN EUROPEA, 2018b), entre otros, todos con el fin de analizar y proponer soluciones para luchar contra la desinformación en línea y el impacto de ello en la democracia y en la libre navegación de los usuarios -ciudadanos en Internet.

[21] *TikTok* es una aplicación de origen chino que permite a los usuarios crear y compartir videos cortos, mayormente clips musicales. Esta aplicación se volvió muy famosa entre los adolescentes desde el año pasado, pero a partir de la cuarentena creció exponencialmente la cantidad de usuarios, y tanto grandes como chicos poseen cuentas en esta nueva red social. El conflicto radica en que al ser una aplicación de origen chino, se empezó a cuestionar que se estaban comunicando millones de datos de ciudadanos de distintos países al gobierno de China, y que podría usarse la app para manipular a los usuarios sobre ideologías políticas. Trump decretó que si la empresa no pasa a capital estadounidense la iba a prohibir en el país por afectar la seguridad nacional (DE LA CAL, 2020). Es importante que *TikTok* sea parte del código de buenas prácticas, toda vez que mas de 2.000 millones de personas han descargado la aplicación (PÉREZ COLOMÉ, 2020) y eso genera un ambiente propicio para viralizar cualquier campaña de desinformación. Tal es el desconocimiento y temor que se tiene sobre esta aplicación ,por los millones de usuarios que posee y la gran cantidad de datos personales que maneja, que la Agencia de Protección de Datos de la Unión Europea estableció un grupo de trabajo para estudiar el impacto de la aplicación en cuestión (EUROPEAN DATA PROTECTION BOARD,2020).

Algo destacable del código es que se prevé el continuo monitoreo de su funcionamiento, y se solicita a las distintos agentes que suscribieron el mismo que realicen informes sobre como resultan las medidas que fueron tomando para la lucha contra la desinformación. La propia Comisión realizará una evaluación global del funcionamiento y la eficacia del código, teniendo en cuenta que de no funcionar el mismo, se podría pensar en una solución legislativa contra la desinformación.

Por todo lo que hemos expresado en este apartado, vemos como la UE toma en cuenta y con seriedad el fenómeno de la desinformación y reconoce que de no controlarse el mismo se está poniendo en peligro la democracia. Asimismo, es interesante que para resolver este conflicto se decidiera por no regular de manera clásica, formal, sino que se aplicara un método de autorregulación y buenas prácticas.

Dentro de este capítulo y a continuación, analizaremos la conveniencia o no de esa decisión, y el funcionamiento de las buenas prácticas como medida de lucha contra la desinformación y/o la injerencia de las TICs en los procesos electorales.

3.2 Propuesta *Lege Ferenda*

Un aspecto central que se debate sobre todo en la lucha contra la desinformación, se refiere a la necesidad de legislar o no hacerlo. Como mencionamos la UE decidió, por el momento, enfrentar el fenómeno de la mano de Códigos de conductas y medidas de autorregulación.

El punto principal es que se "interrogan acerca de la posibilidad o imposibilidad de que una ley pueda decidir qué información es real y cuál no lo es. ¿Puede una ley decidir lo que es cierto y lo que es incierto?, ¿es adecuado crear una especie de Ministerio de la Verdad?" (DE CASTRO RUANO, 2018:10).

Por otro lado, respecto a la utilización de tecnologías como las máquinas de votación electrónica, el voto por internet o herramientas para agilizar el proceso electoral, tampoco existen normas actualizadas que recepten la aplicación de las TICs en este aspecto.

Ante lo expuesto, analizaremos si es necesario que el derecho plantee como solución la regulación formal de la desinformación o del uso de las tecnologías a través de una ley, y

que conflictos pueden generarse con los derechos fundamentales en juego si existe o no una norma regulando al respecto.

3.2.1.-*Planteamiento formal: ¿Es necesaria una ley?*

Una ley, es "toda aquella norma jurídica que emana del Parlamento siguiendo un determinado procedimiento. Es, además, la norma que ocupa la posición jerárquica inmediatamente inferior a la Constitución" (MARTÍN NÚÑEZ, 2018:273).

La importancia de esta fuente de derecho y el procedimiento riguroso y detallado en la Constitución para sancionarla y modificarla, hace que a la hora de decidir si es necesario o no regular determinados temas, se estudie la situación correctamente y se busquen soluciones alternativas, sobre todo si nos referimos a tópicos vinculados con la tecnología que requieren mucho cuidado a la hora de legislar por el gran cambio que sufren constantemente las TICs y la dificultad de modificar al mismo ritmo una norma jurídica.

Por ello, vamos a analizar que soluciones nos ofrece actualmente el derecho para resolver conflictos que se puedan generar producto de las campañas de desinformación y la utilización de las tecnologías en los procesos electorales, para luego poder concluir si es necesaria una ley nueva o modificar normas existentes.

En el primer capítulo conceptualizamos a las *fakes news* como contenido que tomando la apariencia de ser legitimo busca manipular a la opinión pública (ROMERO RODRÍGUEZ et.al., 2018). Si quisiéramos controlar este fenómeno, con el fin de evitar que dentro de las grandes campañas de desinformación se siga manipulando al usuario que es el electorado que luego va a ejercer su voto viciado, tendemos que preguntarnos de que tipo de contenido estamos hablando para luego poder decidir su mejor regulación.

Las noticias falsas dentro de las campañas de desinformación pueden contener datos personales o imágenes de una persona que verídicos o no, pero, de la manera que se presentan pueden causar un daño a su honor o a su privacidad.

Para ello, el derecho tiene ya soluciones consolidadas, por ejemplo, en el ámbito de los datos personales, los últimos años se ha actualizado la normativa adaptándose a las nuevas tecnologías y así, el RGPD o tomando como ejemplo a España, la LOPDyGDD nos brindan

mecanismos para que el titular de los datos personales que viera vulnerado sus derechos, tenga la opción de iniciar las acciones correspondientes al caso concreto.

El uso de datos personales relativos a opiniones políticas para luego hacer envió de propaganda electoral a través de medios electrónicos, está regulado por el art. 58 bis[22] de la LOREG incorporado por la disposición final tercera, apartado dos, de la LOPDyGDD, de protección de datos personales y garantía de los derechos digitales.

Dicho artículo es interesante para el período de la campaña electoral toda vez que permite a los partidos políticos, coaliciones y agrupaciones electorales utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas y el envío de propaganda electoral por redes sociales, siempre respetando los derechos de los titulares de los datos y brindándoles las garantías adecuadas. Al respecto la AEPD en su Circular 1/2019 reglamenta la actuación del art. 58 bis de la LOREG siendo muy rigorosa en las garantías adecuadas de protección que deben llevarse a cabo para el tratamiento de tales datos.

El TC se ha pronunciado estableciendo que "las garantías adecuadas deben velar por que el tratamiento de datos se realice en condiciones que aseguren la transparencia, la supervisión y la tutela judicial efectiva, y deben procurar que los datos no se recojan de forma desproporcionada y no se utilicen para fines distintos de los que justificaron su obtención" (STC 76/2019:FJ6).

De acuerdo con el apartado 1 del artículo 9 RGPD, está prohibido el tratamiento de datos personales que revelen las opiniones políticas, y así lo prevé también la norma española. La excepción está dada si el tratamiento lo realiza un organismo autorizado dentro de sus actividades, los partidos políticos por ejemplo, y siempre brindando las debidas garantías[23].

---

[22] "Artículo cincuenta y ocho bis. *Utilización de medios tecnológicos y datos personales en las actividades electorales.* 1. (Anulado) 2. Los partidos políticos, coaliciones y agrupaciones electorales podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral. 3. El envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial. 4. Las actividades divulgativas anteriormente referidas identificarán de modo destacado su naturaleza electoral. 5. Se facilitará al destinatario un modo sencillo y gratuito de ejercicio del derecho de oposición." (LO 5/1985).

[23] Tal es la importancia de proteger al titular de los datos que revelen sus opiniones políticas, que el TC declaró inconstitucional el inciso 1 del art. 58 bis de la LOREG incorporado por la LOPDyGDD que rezaba: "1. La

Por ende, si un tercero no autorizado utiliza datos personales dentro de una campaña de desinformación, el titular de dichos datos podrá ejercer las acciones que le brinda la normativa de protección de datos. Asimismo, si el uso indebido lo realiza una asociación que esté autorizada por la norma a tratar los datos, si se excede en la finalidad prevista para el tratamiento, obtuvo de manera fraudulenta la información o no se brindaron las garantías acordes al titular y ello le causó un daño, también podrá recurrir a la misma normativa para hacer valer sus derechos.

Siguiendo en la línea de protección de datos, también podemos encontraros que el daño causado se relacione con el uso de una imagen sin autorización o excediendo la finalidad para la cual se posea la misma, para ello se puede recurrir a la normativa de datos personales referenciada y a Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

Una noticia falsa, sobre todo en el ámbito de la desinformación electoral, puede contener una expresión que lesione la dignidad de una persona o la imputación falsa de un delito sabiendo de su falsedad, ante tales situaciones el damnificado puede recurrir al derecho penal, encontrándonos frente a los delitos de calumnias o injurias[24].

Obviamente, dependerá del caso concreto que se configure el delito tipificado pero es otra alternativa de protección ante la desinformación.

Un conflicto que se podría generar es que como Internet borra fronteras, la persecución de delitos o iniciar acciones cuando el autor o demandado se encuentra en otro estado se torna muchas veces dificultoso. Para ello, si es clave la cooperación internacional y que se generen

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…" (LO 5/1985: 58 BIS 1), fundamentando que "se concluye que la ley no ha identificado la finalidad de la injerencia para cuya realización se habilita a los partidos políticos, ni ha delimitado los presupuestos ni las condiciones de esa injerencia, ni ha establecido las garantías adecuadas que para la debida protección del derecho fundamental a la protección de datos personales reclama nuestra doctrina, por lo que se refiere a la recopilación de datos personales relativos a las opiniones políticas por los partidos políticos en el marco de sus actividades electorales"(STC 76/2019:FJ9).

[24] Los delitos de injurias y calumnias están contemplados en el titulo XI Delitos contra el Honor, capítulos I, II y III del Código Penal español (LO 10/1995). Si bien tomamos como ejemplo España, son delitos que se replican en casi todos los códigos penales de los países democráticos. En Argentina encontraremos su regulación en Libro Segundo, título II del Código Penal Argentino (TO. 1984).

convenios internacionales para agilizar la colaboración en los procesos donde hay elementos que vinculan a más de un estado[25].

Como podemos apreciar, los daños que puede llegar a causar el contenido de las campañas de desinformación, no responden a bienes jurídicos nuevos sin protección, sino que tanto el honor, los datos personales, la privacidad y la propia imagen son cuestiones que el derecho viene protegiendo hace mucho tiempo y que analizando el caso concreto encontraremos en los ordenamientos jurídicos vigentes leyes que pueden aplicarse para ejecutar tal protección.

Ahora debemos analizar para el caso del uso de tecnologías en la etapa de la votación o en el recuento y proclamación de electos, que encontramos en el derecho.

Los procesos electorales generalmente en un estado democrático los encontramos determinados en la Constitución del país y una ley especial que regule en detalle el proceso. En el caso de España, por ejemplo, hablamos de la LOREG.

Estas normas constitucionales, son anteriores a las tecnologías, y por ende el sistema que se regula es pensado en papel y manual, nada de voto electrónico o por internet.

En el 2004 el Consejo Europeo dictó una recomendación sobre las normas legales para la utilización del voto electrónico, estableciendo que se deben respetar los principios de las elecciones democráticas. Es decir, que si se aplican mecanismos electrónicos los mismos deben ser seguros e inspirar la misma confianza que los sistemas de votación tradicional (CONSEJO DE EUROPA, 2004).

“El derecho de sufragio pasivo – derecho al voto - es un elemento primordial de los cimientos básicos de la democracia, y que, por ende, los procesos electorales desarrollados con motivo

[25] Por ejemplo, en el área penal el Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001 es un instrumento jurídico importante que vincula a mas de 50 estados, y busca unificar criterios y establecer una política criminal común, fomentando mecanismos de cooperación internacional en materia de detección y persecución de ciberdelincuentes. Por otro lado, en el ámbito del derecho internacional privado el Reglamento 1215/2012 del Parlamento Europeo y Del Consejo de 12 de diciembre de 2012, conocido como Bruselas I Bis, recepta lo relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil, siendo util tambien para situaciones que se generen por las campañas de desinformacion.

de la introducción de los sistemas de voto electrónico deben adecuarse a los principios fundamentales predicables de toda elección…" (CONSEJO DE EUROPA,2004).

Es interesante como la recomendación les indica a los estados que deben respetar los principios básicos electorales a la hora de introducir y/o regular sobre el voto electrónico, teniendo como punto de comparación los sistemas de sufragio presencial tradicional (GONZÁLEZ DE LA GARZA, 2009).

Lo importante en este punto es entender que los estados si quieren incluir herramientas tecnológicas para llevar a cabo el proceso electoral, deben establecer un mecanismo de garantías que aseguren la confianza en el proceso, la transparencia, así como su integridad, y ello reflejarlo en una norma acorde.

El voto universal, secreto, igual y libre debe receptarse sin importar el mecanismo elegido para su emisión, y es así que en este punto, si es adecuado o una modificación o una norma especial regulando el proceso detalladamente si se desea utilizar algún tipo de tecnología en alguna de las etapas electorales.

Lo cierto es que son pocos los países que tienen implementado en su totalidad el voto electrónico[26], algunos están en proceso o se permite a nivel autonómico o provincial pero no en el estado nacional[27], en otros se encuentra legalmente prohibido o paralizado[28], sea cual sea la situación, como mencionamos en capítulos anteriores, las TICs vinieron para quedarse, y la implementación de la tecnologías en el proceso electoral requiere de un gran cambio social, político y sobre todo jurídico (TULA, 2012).

[26] Por ejemplo, Estonia, Bélgica en la mayoría de las elecciones, Brasil, Venezuela y Filipinas (EUSKADI, 2018).

[27] España, Italia, Francia, EEUU, Ecuador, son algunos de los paises que tienen algunas elecciones internas previstas a través de voto electrónico (EUSKADI, 2018).

[28] Alemania y Holanda, por ejemplo, este último fue pionera en la implementación del voto electrónico desde 1965 que la legislación permite su uso, sin embargo, por encontrar fallos de seguridad en el sistema utilizado a partir del 2008 se anuncio que se retornaba al sistema clásico papel (EUSKADI, 2018).

3.2.2.- Planteamiento material: Posición de los derechos fundamentales ante la posibilidad de la sanción de una ley.

Los "Derechos fundamentales, son normas que reconocen y garantizan a los individuos determinadas facultades para que puedan desarrollar una vida digna, concediendo ámbitos de protección y reacción frente a intromisiones ilegítimas producidas por la acción de los poderes públicos y/o particulares" (MARTÍN NÚÑEZ, 2018:238). "…Pueden ser definidos como los derechos subjetivos reconocidos en la Constitución" (ESCOBAR ROCA, 2018:434).

Cuando se piensa en promulgar una nueva ley se debe tener cuenta qué derechos fundamentales pueden estar en juego, y ser cuidadosos, evitando que la futura nueva norma vulnere alguno de ellos, ya que podría determinarse como inconstitucional. Especial énfasis se debe poner si lo que se quiere regular esta vinculado a las nuevas tecnologías, ámbito todavía en algunos aspectos desconocido para el derecho y con dificultades para legislar.

En el caso de las *fake news* debemos tener en cuenta que querer restringir la divulgación de noticias falsas puede llegar a generar conflictos con la libertad de expresión y la libertad de información, esto es, el derecho a "comunicar o recibir libremente información veraz por cualquier medio de difusión" (art. 20. 1 d, CE).

Las medidas adoptadas por la Unión Europea, sus Estados miembros, otros Estados y demás partes interesadas para luchar contra la desinformación deben interpretarse y limitarse dentro del marco jurídico vigente.

La Carta de los Derechos Fundamentales de la Unión Europea y el Convenio Europeo de Derechos Humanos, consagran en sus artículos 11 (CDFUE) y 10 (CEDH), la libertad de expresión, la cual incluye la libertad de opinión y la libertad de recibir o comunicar datos o ideas sin injerencia de autoridades públicas y sin importar las fronteras.

"Las libertades informativas no son monopolio de los –clásicos– medios de comunicación, sino que todos los ciudadanos las pueden ejercer hoy día a través de internet y su protección puede llegar a ser igual de intensa que un medio de comunicación. La clave no es tanto el sujeto emisor de la opinión o información, sino el interés público o relevancia de la misma. Cuanto más interés público tenga lo informado o expresado, mayor protección constitucional tiene. Ahora bien, ya que todos somos titulares de estas libertades, también a cualquier

ciudadano puede exigírsele la responsabilidad por el ejercicio de las mismas y el cuidado y diligencia" (COTINO HUESO, 2018:486).

Es interesante detenernos en el cuidado y diligencia tanto de los medios, como del ciudadano, a la hora de ejercer estas libertades. No debemos olvidar que ningún derecho es absoluto, y por ende, la libertad de expresión si bien no puede estar sujeto a censura previa de corresponder habrá responsabilidades ulteriores que cumplir (Art. 13 CIDH).

"El punto de partida en cualquier caso es que cualquier usuario puede emitir contenidos susceptibles de ser protegidos por las libertades informativas por cuanto tengan interés público. Del mismo modo, cualquier usuario ha de ser responsable de la constitucionalidad y licitud de los contenidos que emite" (COTINO HUESO, 2018:490).

Por lo expuesto, la libertad de expresión e información son derechos fundamentales que están altamente regulados en los Estados democráticos y que entran en escena cuando hablamos de desinformación.

Si se pretendiera legislar con una ley que tenga como fin limitar las f*ake new*s o la desinformación masiva especialmente en periodos electorales, seria muy probable, por la dificultad que engendra regular temas libertad de opiniones de los ciudadanos o la información que brindan los medios o el usuario de internet, que vulneraremos alguno de estos derechos, sumándole a ello la libertad ideología que poseen los ciudadanos[29], siendo muy complejo crear una legislación eficaz que no cercenen este tipo de derechos (CCN, 2019).

Si se legisla, debemos entender que algún organismo, algún poder del estado, tendrá la facultad de decidir qué es una noticia falsa, que no lo es, que es lo verdadero o no. Lo cual, a criterio de esta autora, es demasiado peligroso dotar al estado con ese poder, estaríamos entregando una de las libertades más importantes que es la de poder obtener toda la información que consideremos necesaria para generar un pensamiento crítico. Si dejamos que el estado decida que podemos acceder a ver y que no, pondríamos en jaque la democracia, y nuestras decisiones ya no se basarían en datos objetivos.

[29] El articulo 16 de la CE garantiza la libertad ideológica de los individuos y las comunidades sin más limitación que la necesaria para el mantenimiento del orden público, sumándole que nadie podrá ser obligado a declarar sobre su ideología.

Las respuestas jurídicas al fenómeno de la desinformación son complejas y pueden ser una excusa para restricción de las libertades. Por eso las soluciones deben enfocarse en conseguir que los grandes intermediarios de la información colaboren con los estados, utilizando herramientas técnicas para evitar la intoxicación masiva de información y/o alertar en la medida de lo posible a los usuarios de informaciones que provienen de cuentas bots o de dudosa procedencia (COTINO HUESO, 2018).

También podemos vincular a la desinformación con la afectación del derecho al sufragio activo, manipulando nuestra libre elección, y pasivo, entendiendo que debido a estas campañas de desinformación el futuro candidato se encuentra ante un escenario de a su vida personal o política pero en base a situaciones o noticias falsas, generando una condición injusta que lo damnifique notablemente y le haga reconsiderar su postulación.

Desde el punto de vista del voto electrónico o remoto y los derechos fundamentales, destacaremos dos características primordiales que una legislación que quiera incorporar las tecnologías al proceso electoral debe respetar: el secreto del voto y el respeto de la voluntad del elector.

Como ya se ha explicado anteriormente el secreto es una de las características que las Constituciones de los estados democráticos imparten sobre el voto, y consiste en que no debe haber ninguna posibilidad de conocer el sentido del voto emitido (DELGADO IRRIBARREN Gª-CAMPERO, 2008).

Asimismo, se debe garantizar que el ciudadano decida su voto libremente gracias a la información que puedo acceder para formar su opinión del candidato que desea, para ello aplicamos todo lo visto respecto a la desinformación y la manipulación del electorado, y en lo que respecta a las tecnologías se debe asegurar que el voto emitido se contabilizará íntegro y conforme a la voluntad expresada por el votante (OEA, 2014).

Es decir, que la normativa que se promulgue debe incluir niveles de seguridad que garanticen que el voto emitido por el ciudadano no puede ser visto por terceros, ni ser trazado para unir al emisor con el voto, ni manipulado (OEA, 2014; TULA,2012), debiendo "exigir las mayores cautelas respecto al cumplimiento estricto de las garantías jurídicas del derecho fundamental de sufragio: igualdad y secreto del voto, pureza y transparencia del procedimiento" (DELGADO IRRIBARREN Gª-CAMPERO CAMPERO, 2008:2).

El procedimiento debe garantizar que los resultados reflejen con exactitud la voluntad de los electores, el conflicto surge sobre la utilización de medios electrónicos pues una manipulación de la herramienta tecnológica podría llevarse a cabo con el desconocimiento de los electores e incluso de las autoridades electorales (DELGADO IRRIBARREN Gª-CAMPERO CAMPERO, 2008)

Para eso es importante que el Estado estudie con expertos el tipo de *hardware* y *software* que se va a utilizar (TULA, 2012), siendo útil incorporar software de código abierto para así garantizar una inspección detallada, completa y rigurosa del sistema que se aplicara al sufragio electoral, teniéndose que prever si la Ley de Propiedad Intelectual de cada estado tiene que ser modificada o pude regularse respecto a las características, derechos y responsabilidad sobre el *software* electoral (GONZÁLEZ DE LA GARZA, 2009).

Lo importante entonces es que antes de implantar este tipo de tecnologías, las normas garanticen la fiabilidad del procedimiento, implementando medidas que den seguridad y preserven las garantías fundamentales del derecho de sufragio.

"La diversidad de mecanismos electrónicos de votación, las diferencias entre regulaciones y, sobre todo, la pluralidad de escenarios donde han de aplicarse aconsejan huir de estereotipos predeterminados. Una vez consolidados ciertos principios electorales básicos, hay que adaptarse a la cultura electoral de cada país. Tiene que ser, en definitiva, cada ciudadanía la que busque el equilibrio apropiado entre las utilidades del sistema y los mecanismos de garantía y transparencia, pero esta elección debe realizarse de forma totalmente informada, siendo consciente de los riesgos que comporta el voto electrónico" (BARRAT I ESTEVE, 2009:11).

3.3 Buenas Prácticas

Luego de todo lo expuesto y analizado en este trabajo, sabemos que querer legislar contra la desinformación es un camino difícil, que se debe hacer con cautela porque se podría llevar a vulnerar la libertad de expresión y de información de los ciudadanos y se le estaría otorgando un súper poder al estado para decidir sobre la veracidad de toda la información que circula.

Asimismo, todo lo que implique referenciar tecnologías en una ley, requiere de un trabajo arduo y bien pensado, ya que la técnica cambia constantemente y la norma se volvería vetusta en cuestión de días o meses, siendo una tarea parlamentaria larga modificar y actualizar una ley. Por ende, legislar utilizando la neutralidad tecnológica es lo más acorde, pero no quiere decir que ello sea siempre lo más adecuado y sencillo.

En consecuencia, utilizar métodos de buenas prácticas para lograr resolver futuros conflictos que se pueden presentar con las tecnologías, educando a los usuarios, y generando colaboración entre estados, empresas tecnológicas y ciudadanos, parece ser la mejor opción.

Así fue que como mencionamos que la UE decidió encarar su lucha contra la desinformación a través del Código de Buenas Prácticas de la Unión en materia de desinformación que analizaremos a continuación, destacando lo más relevante del mismo en relación con este trabajo.

3.3.1.- Propuesta de buenas prácticas como solución

El Código (2018) en su preámbulo establece que su función es lograr soluciones para los problemas generados por la desinformación y quienes suscriben el mismo reconocen y aceptan que la exposición de los ciudadanos a la desinformación representa un gran reto para Europa. Entendiendo que las sociedades democráticas dependen de debates públicos que permiten que los ciudadanos bien informados expresen su voluntad mediante procesos políticos libres y justos.

Asimismo, los signatarios se comprometen a llevar a cabo las acciones previstas en el Código garantizando del pleno cumplimiento de la legislación vigente que corresponda, y respetar el derecho fundamental a la libertad de expresión y a una internet abierta, buscando el equilibrio entre cualquier acción para limitar la difusión e impacto de contenido y los derechos fundamentales.

Los objetivos que describe el código son once enmarcados en la implementación y puesta en marcha de herramientas y políticas para la prevención, mitigación y reducción de la desinformación, buscando siempre respetar y garantizar los derechos fundamentales de los usuarios de la sociedad de la información.

Dentro de los objetivos nos encontramos con que los que adhieran al Código deberán garantizar la transparencia de la publicidad política permitiendo por ejemplo que los usuarios sepan porqué han sido objetivo de un determinado anuncio publicitario (objetivo ii); esforzarse por cerrar cuentas falsas, establecer sistemas que identifiquen *bots* y que no se confunda la interacción de los mismos con personas físicas (objetivo v); que el usuario sepa porque ha sido objeto de algún anuncio político, mediante indicadores de la fiabilidad de las fuentes de contenido (objetivo viii), (ix) luchar por reducir la visibilidad de la desinformación facilitando como contraposición, la localización de contenido fiable.

Un punto interesante del Código es la obligación de los signatarios de revisar su labor respecto a la lucha contra la desinformación, y poder de esta manera generar un panorama sobre la eficacia o no de las obligaciones y los compromisos que aborda el instrumento jurídico en análisis, comprometiéndose a redactar un informe anual sobre su trabajo para luchar contra la desinformación, el cual deberá hacerse público.

A su vez, los signatarios colaborarán con la Comisión Europea y otras partes interesadas para desarrollar una estrategia concreta en relación con la propaganda política, siempre en búsqueda de transparencia. Este punto resulta interesante y refleja el fin principal de la UE en materia de desinformación, que es la protección de los ciudadanos frente a la manipulación durante las distintas etapas de los procesos democráticos.

Lo destacable de los apartados sobre medición y seguimiento y evaluación que trae el Código, es la obligatoriedad de continuar trabajando en el mismo, en seguir debatiendo, proponiendo soluciones en conjunto todos los agentes involucrados, y que no quede el mismo en letra muerta o una forma de autorregulación voluntaria que pocas veces consiguen resultados materiales concretos.

En el año 2019 se publicó un reporte anual en base a los informes de los signatarios, y como resultado la Comisión Europea concluye que los informes de los signatarios indican un aumento en los esfuerzos de trabajar en conjunto entre las plataformas y otras partes como pueden ser los verificadores de datos, los investigadores, la sociedad civil y las autoridades nacionales, sin embargo, todavía se tiene que mejorar la cooperación entre los distintos agentes involucrados. Ello con el objetivo de mejorar la resiliencia de las plataformas contra diversas formas de intromisión y manipulación de los medios y minimizar la distribución de

desinformación. Se destaca que existe una mayor transparencia en comparación con el año anterior a la entrada en vigor del Código (EUROPEAN COMMISSION, 2019).

El código es vinculante para los signatarios y los mismos deberán ceñirse a sus planteamientos, lo cual es un gran logo de la UE, siendo que las grandes plataformas digitales como Google, Facebook o Twitter se comprometan colaborar y autorregularse de forma voluntaria para hacer más transparente la publicidad política o introducir mecanismos de verificación de datos para luchar contra la desinformación, es un gran avance.

Los estados deben entender que en este nuevo mundo donde internet borra fronteras, donde nadie es el dueño de lo que pase por la red, donde grandes empresas privadas manejan millones de datos de ciudadanos de diversos países, no se puede querer encontrar una solución a la antigua dictando una norma y obligando a cumplir la misma.

Si queremos que funcione, se debe trabajar en equipo y medidas como el Código de buenas practicas son un gran comienzo, si todos los agentes involucrados se comprometen en su redacción y se encuentran objetivos en común los resultados fructíferos y reales.

No nos olvidemos que el fin último es la protección de la democracia y la transparencia de los procesos electorales, algo que tanto a los estados como los ciudadanos nos debe importar.

Como crítica hacia el Código podemos decir que no contempla un régimen sancionador donde se estipule las consecuencias tanto jurídicas, como sociales, para quienes lo incumplan, situación que se puede evaluar y solucionar tal vez adicionándose estos supuestos dentro del mismo que al ser vinculante integraría la obligatoriedad de las sanciones impuestas o creando un nuevo mecanismo acorde para lograr su cumplimiento, cuestiones a analizar e investigar.

3.3.2.- Educación en lo digital

Como corolario de todo lo desarrollado, se debe hacer una breve reflexión a la falta de educación del ciudadano en el mundo digital.

Ya mencionamos que las TICs son un fenómeno que llego para quedarse, que se busca agilizar y optimizar las labores del día a día, y que tanto es así que hasta en los procesos electorales podemos ver su injerencia.

Por eso es importante que todos los Estados tomen conciencia de que vivimos en la sociedad de la información y que "el desarrollo de competencias fundamentales y digitales a lo largo de toda la vida…resulta esencial" (COMISIÓN EUROPEA,2018b:14).

"Es la educación una de las tareas más importantes que deben abordan los Estados y las sociedades. Con mayor razón hoy que asistimos a dos situaciones coetáneas, pero de diferente desarrollo. Por un lado, estamos sumidos en la sociedad de la información y por otro somos testigos del permanente deterioro de la democracia como régimen político. Ante semejante situación los Estados que quieran conservar la democracia, tendrán que, entre otras variables, tomar a la educación como uno de los sustentos de este régimen político. Y la educación con su enorme importancia, también deben asumir el tiempo que tienen de frente y adecuarse al mismo... Así en el marco de la sociedad de la información, la educación debe asumir elementos que permitan prepara a los sujetos para este verdadero tsunami de datos" (LAGOMARSINO MONTOYA, VÉLIZ BURGOS, PAVIÉ NOVA, y NASS ÁLVAREZ, 2019).

La desinformación transciende fronteras, y como usuarios debemos también ser responsables a la hora de recibir una información, teniendo nuestras buenas practicas de actuación.

"La capacidad del lector para diferenciar entre noticias y relatos, entre información y propaganda, entre datos y adoctrinamiento, es fundamental para la preservación de su capacidad para decidir de una forma racional" (GOMEZ DE AGREDA, 2018:18).

"La primera y última víctima de las guerras de comunicación son los ciudadanos… por ese motivo, es necesario que los usuarios de medios digitales estén prevenidos para detectar una campaña de desinformación y tengan las capacidades para evitar ser manipulados" (CCN, 2019:31) y será el rol del estado brindar esa educación.

CAPÍTULO FINAL

4.1 Reflexiones Finales

El mundo está cambiando, atravesamos una situación de salud pública a nivel mundial impensado que nos obligó a todos a cambiar nuestros hábitos. Como consecuencia de esto, las TICs se transformaron en el mejor aliado para nuestras vidas, tanto que casi todas las actividades que antes hacíamos presencialmente, se trasladaron al mundo digital. El problema radica en que ni los estados, ni los sistemas, ni los ciudadanos estábamos preparados para migrar abruptamente a este nuevo mundo tecnológico.

Esta experiencia que estamos atravesando, nos hace reflexionar respecto a si nuestros ordenamientos jurídicos están preparados para brindar soluciones a conflictos que surgen de la interacción con la tecnología. Y algo muy importante, sobre derechos adquiridos que, como el sistema funciona y hace años está equilibrado habíamos dejado de pensar, pero con la irrupción de las TICs, debemos volver a analizar.

Con esto último nos referimos a, por ejemplo, nuestra libertad de elegir a quién queremos votar sin influencia de terceros, o que el sufragio que emitimos sea secreto, o que si queremos expresarnos o informarnos podamos hacerlo sin temor a censuras o sabiendo que la información a la que accedemos no está sesgada.

Entonces es allí que no solo el derecho debe tomar cartas en el asunto, sino que también los estados y los ciudadanos tienen sus responsabilidades.

El mundo debe continuar, eso quiere decir que los procesos electorales se tendrán que seguir llevando a cabo -así ha sido con las elecciones autonómicas de País Vasco o Galicia, más no en Nueva Zelanda o posiblemente en Estados Unidos-, pero eso no significa que sea a costa de principios y derechos que son pilares fundamentales de los estados democráticos.

La ciberseguridad es un pilar importante a tener en cuenta. En conjunto, con normas jurídicas acordes, se concibe blindar los procesos democráticos de la mejor manera posible, si es que se necesita migrar todo o en parte a unas votaciones con herramientas tecnológicas.

Por último, hay que remarcar que las campañas de desinformación existen desde siempre, la diferencia es que, gracias a las TICs, llegan a mayor cantidad de gente. Si bien es correcto

que los estados quieran controlar estos fenómenos ya que perjudica las bases democráticas, esta autoría no considera que una ley sea la solución por ahora a ese problema.

Las buenas prácticas para que las empresas comiencen a autorregularse en pos de luchar contra las *fake news* y la desinformación, es un buen comienzo. No siempre debemos recurrir a la ley obligatoria, prohibitiva como solución, ya que estamos frente a tópicos multidisciplinarios, que se necesitan coordinar actores de muchos rubros, y que una norma que sea eficiente y logre ello sin vulnerar derechos de alguna de las partes, no es fácil de conseguir.

Como reflexión final es importante recordar que como usuarios tenemos el compromiso de protegernos y proteger nuestros derechos en el mundo físico y digital. Si las campañas de desinformación prosperan no es culpa de las tecnologías y del estado exclusivamente, como usuarios ayudamos a que se replique la información, no nos tomamos el tiempo de pensar que compartimos en las redes, si es verdad o no. Tenemos que dejar de ser ciudadanos pasivos con la tecnología y aportar desde nuestro lugar en evitar que terceros con información falsa, con videos manipulados nos digan que pensar.

La educación en lo digital tiene que ser un compromiso de todos los estados. El reto radica en superar la sociedad de la información hacia una sociedad del conocimiento.

4.2 Conclusiones

Primera. *Posverdad y fake news como elementos claves de las campañas de desinformación.*

Cuando las creencias o sentimientos personales que genera un hecho prevalecen sobre la información objetiva a la hora de formular una opinión pública, estamos frente a lo que se conoce como posverdad. Este fenómeno tiene un gran desarrollo gracias a elementos como las *fake news,* información falsa o manipulada que aparenta ser legítima, que permiten que el receptor de la noticia exacerbe esos prejuicios, sentimientos y creencias dejando de lado la búsqueda de la verdad objetiva de los hechos ocurridos.

En conjunto con la aparición de los nuevos medios sociales, que se valen de las tecnologías para crear un nuevo espacio de comunicación, donde el ciudadano deja su papel de receptor

para crear y compartir activamente contenidos, se genera el escenario propicio para que las campañas de desinformación se desarrollen y lleguen a un gran grupo de personas.

Lograr manipular electores se convierte en algo mucho más sencillo desde que la posverdad se implanta en nuestra sociedad. Buscamos creer aquello que nos gusta, y si una *fake news* se alinea a nuestra ideologia y sentir, asimilaremos esa información como verdadera sin cuestionarnos los hechos objetivos y contribuiremos a la campaña de desinformación compartiendo tal noticia.

Segunda. Las etapas de los procesos electorales se ven atravesadas por la utilización e injerencia de las Tecnologías.

Tanto en la precampaña y campaña electoral, como en la celebración de elecciones y proclamación de electos y la postcampaña, la tecnología se hace presente.

Existen innumerables herramientas tecnológicas a aplicarse en el proceso electoral, podemos encontrarnos con el uso de redes sociales y nuevos medios de comunicación, para viralizar *fake news* y manipular así las decisiones del electorado, como con la implementación de máquinas de voto electrónico en los recintos de votación, o la emisión remota del sufragio a través de internet.

Lo cierto es que si resulta que de la injerencia de las tecnologías, en la presentación de candidatos, en la proclamación de electos o en la votación, se deduce una manipulación o fraude a través de las herramientas utilizadas, esas elecciones deberán invalidarse por afectar la legalidad del proceso.

Ahora bien, si nos encontramos frente a la postcampaña y la injerencia de la tecnología son las constantes campañas de desinformación a través de redes sociales y demás nuevos medios sociales donde se quiere comunicar el mensaje de que podría haber existido un fraude en las etapas anteriores, el ataque se dirige a la legitimidad del proceso. Ello obligará a reconducir la gestión política para que no afecte ese cuestionamiento a la gestión del gobierno.

Cualquier herramienta o sistema tecnológico que se quiera implementar debe ser acompañado por una adecuación de las normas sobre el proceso y educación al electorado

para que logre un uso correcto de las tecnologías y una apreciación objetiva de la información a la que accede.

Ello en pos de resguardar los principios que sostienen el sistema de un estado democrático representativo y la legalidad y legitimidad de los procesos electorales.

Tercera. Algoritmos y bots: la manipulación del electorado nunca fue más fácil.

Con internet, los nuevos medios sociales y el empoderamiento del usuario que se convirtió no solo en receptor de información, sino también en comunicador de la misma, el panorama es propicio para que las campañas de desinformación tengan éxito.

Los algoritmos nos presentan infinidades de opciones de actuación, y en el caso de las campañas de desinformación, nos permiten que aparezcan fenómenos como los "bots políticos", los cuales se programan para analizar información y tomar decisiones automatizadas generando contenido e interacción con usuarios humanos.

Estos bots van a permitir crear usuarios ficticios en redes sociales, aumentar el número de seguidores de los candidatos en sus perfiles y desorientar al electorado con grandes cantidades de información – la mayoría falsa o manipulada- sobre un candidato para lograr que la opinión pública cambie su percepción del mismo, convirtiéndose en el ataque perfecto de las campañas electorales.

Asimismo, debemos sumarle a los "bots políticos", la aparición de videos manipulados para que el usuario crea que la persona que está viendo realiza determinada declaración, pero que en realidad es producto de la utilización de herramientas tecnológicas que logran lo que se denomina *"deepfakes"*.

Estos videos modificados se acompañan con las *fake news* y gracias a los algoritmos adecuados logran llegar a miles de personas, tornándose la manipulación de la opinión publica mucho más sencilla gracias a las TICs.

Cuarta. Las bases y principios de la democracia peligran: los derechos fundamentales que necesitan protección.

Si las tecnologías formarán parte de los procesos electorales, se deberá proteger con creces los derechos en juego, en pos de que las bases constitucionales de la democracia no se encuentren en peligro.

El derecho al sufragio desde sus dos dimensiones, tanto activa como pasiva, se ve afectado por la utilización de las TICs.

Desde el punto de vista del electorado, ante las campañas de desinformación que es sometido constantemente, podría verse vulnerada la libre elección del sufragio, entendiendo que cada vez es mas complejo lograr una apreciación objetiva de los hechos si está siendo bombardeado por informaciones falsas.

Asimismo, si el estado buscara regular para erradicar las *fake news*, podría vulnerarse la libertad de expresión o de información, tornado compleja una regulación prohibitiva, teniendo que articularse los mecanismos acordes entre la tecnología y las normas para encontrar el equilibrio.

Por otro lado, si se utilizan tecnologías para la emisión del sufragio tanto de manera presencial (voto electrónico) como de manera remota (voto por internet), se estaría poniendo en riesgo el secreto del voto y la manipulación del mismo, toda vez que la ciberseguridad de los mecanismos elegidos para la votación se puede ver comprometida generándose cambios en la voluntad del elector a la hora de emitir el sufragio

Si nos enfocamos en el sufragio pasivo, las campañas de desinformación ubican al futuro candidato en una situación incomoda, toda vez que, *a priori* puede prever que su vida personal y política será atacada injustamente con aseveraciones falsas sin principios éticos, ni limites, más allá de lo que es políticamente esperable en una carrera política. Teniendo esto como consecuencia, el temor de un ciudadano a ejercer su derecho de ser candidato y participar activamente en un proceso electoral.

Quinta. El derecho como solución a medias de los conflictos con la tecnología

Es necesario que los procesos electorales previstos por las constituciones de los estados se adapten para hacer frente a la utilización de nuevas tecnologías.

Las constituciones y las leyes especiales que regulan el ejercicio del sufragio, generalmente, son anteriores a las tecnologías, y por ende el sistema que se regula es pensado en papel, no para la existencia de un voto electrónico o por internet.

Por lo tanto, aquí la norma jurídica sí se plantea como solución, teniendo que modificarse y adaptarse los mecanismos de los procesos existentes, para salvaguardar que ante la inclusión de tecnologías no se vulneren derechos democráticos, teniendo siempre en mira el respeto por el voto universal, igual, secreto y libre.

Sin embargo, si de desinformación se trata, una norma jurídica puede llegar a vulnerar la libertad de expresión y el acceso a la información teniendo como consecuencia la censura y la dotación al estado de un súper poder de decidir que contenido es verdadero y cual no.

La UE, ha realizado un largo recorrido de estudio para concluir que la mejor manera de luchar contra la desinformación era a través de un Código de Buenas Prácticas, que involucra no solamente a los estados, sino a todos los agentes que intervienen en la comunicación digital de la información y que, en definitiva, son los que tienen la capacidad técnica de evitar la propagación de las *fake news*.

Querer solucionar y proteger a la democracia de la desinformación es algo que deberá hacerse paulatinamente para evitar el efecto contrario a la protección que se busca.

Sexta. Buenas prácticas y educación en lo digital, ¿la solución?

La creación del Código de Buenas Prácticas sobre desinformación por parte de la UE, en el cual se encuentran adheridos y trabajando en conjunto grandes plataformas digitales es un ejemplo que, ante la dificultad de regular sobre tecnología sin restringir derechos fundamentales y coordinando distintos agentes, podríamos tener una solución.

Debería replicarse esta metodología en otros estados, siempre entendiendo que es fundamental la cooperación y el trabajo multidisciplinario.

También poner énfasis en educar a los ciudadanos sobre el mundo digital es una excelente herramienta para evitar conflictos futuros. Un ciudadano alfabetizado digitalmente es más difícil de convencer y puede discernir ante una campaña de desinformación.

Que podamos tener acceso a toda la información que deseáramos es un gran avance como sociedad, pero es sólo el primer paso. No es sinónimo de certeza de que la sociedad va a tomar mejores decisiones por acceder masivamente a un gran caudal de información.

El eje radica en que se tiene que trabajar, y aquí es donde la alfabetización y educación en lo digital se torna vital, en evolucionar de una sociedad de la información, a una sociedad del conocimiento. En esta última, se pretende que el receptor de la información produzca una apropiación critica y selectiva de la misma, realizando este ejercicio, se evitaría una fácil manipulación de su opinión y como consecuencia las campañas de desinformación ya no tendrían tanto éxito.

"La gente, valiéndose de criterios convencionales, lo tiene todo resuelto, inclinándose siempre hacia lo más fácil, y buscando aún el lado más fácil de lo fácil."

Rainer Maria Rilke

BIBLIOGRAFÍA

1. Doctrina:

- BARRAT I ESTEVE, Jordi (2012). "El secreto Del voto en el sufragio Por internet". *Revista Mexicana de Análisis Político y Administración Pública,* [en línea]. V. I, nro. 2, pp. 57-71. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=4219628
- BARRAT I ESTEVE, Jordi (2009). "Observación electoral y voto electrónico". *Revista catalana de dret públic*, [en línea]. Nro. 39, pp. 1-12. Disponible en: http://revistes.eapc.gencat.cat/index.php/rcdp/article/view/2194/n39-barrat-es.pdf
- CALDEVILLA DOMÍNGUEZ, David (2010). "Las nuevas tecnologías cambian el panorama de la comunicación política". *Perspectivas de la comunicación,* [en línea]. V. 3, nro. 1, pp. 111–122. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=5283592
- CASTELLÁ ANDREU, Josep Mª (2018). "La representación y la participación políticas", en AA.VV. (CASTELLÁ ANDREU, Josep Mª, editor): *Derecho Constitucional Básico.* Barcelona: Huygens, pp. 93-110.
- CENTRO CRIPTOLÓGICO NACIONAL (2019). *Desinformación en el Ciberespacio*, [en línea]. Pp. 1-33. Disponible en: https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/3549-ccn-cert-bp-13-desinformacion-en-el-ciberespacio/file.html
- COMISIÓN EUROPEA (2019). *El código de buenas prácticas contra la desinformación cumple un año: las plataformas en línea presentan informes de autoevaluación.* Disponible en: https://ec.europa.eu/commission/presscorner/detail/es/STATEMENT_19_6166
- CONSEJO EUROPEO (2018). *Conclusiones del Consejo Europeo del 28 de junio de 2018.* Disponible en*:* www.consilium.europa.eu/es/press/press-releases/2018/06/29/20180628-euco-conclusions-final/

- COMISIÓN EUROPEA (2018b). *La lucha contra la desinformación en línea: un enfoque europeo*. COM/2018/236. Disponible en: https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A52018DC0236
- CONSEJO DE EUROPA (2004). *Recomendación del Comité de Ministros del Consejo de Europa a los Estados Miembros sobre los estándares legales, procedimentales y técnicos de los sistemas de votación electrónica*. Disponible en: https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/E-votingRec_Spanish.asp.
- COTINO HUESO, Lorenzo (2018). "El principio de igualdad. Derechos y libertades fundamentales, derechos sociales y otros derechos constitucionales", en AA.VV. (CASTELLÁ ANDREU, Josep Mª, editor): *Derecho Constitucional Básico.* Barcelona: Huygens, pp. 471-500.
- DE CASTRO RUANO, José Luis (2018). "La desinformación como instrumento político en la Sociedad Internacional actual: las respuestas desde la Unión Europea". *Revista Aranzadi Unión Europea*, [en línea]. Nro. 7, pp.1-13. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6528766
- DE LA CAL, Lucas (2020). *La guerra por TikTok: China tomará medidas si EEUU le "roba" su popular app*. Disponible en: https://www.elmundo.es/economia/empresas/2020/08/04/5f29556cfc6c83ed5a8b458e.html
- DELGADO-IRIBARREN Gª-CAMPERO, Manuel (2008). "Voto electrónico y nuevas tecnologías" En*: ¿Exige la sociedad-red una nueva democracia?*, [en línea]. Zaragoza: Fundación Manuel Giménez Abad de Estudios Parlamentarios y del Estado Autonómico: Universidad Internacional Menéndez Pelayo. Disponible en: https://www.fundacionmgimenezabad.es/es/actividades/jornadas-exige-la-sociedad-red-una-nueva-democracia
- EL DERECHO (2015). *Recursos Electorales.* Disponible en: *https://elderecho.com/recursos-electorales*
- ESCOBAR ROCA, Guillermo (2018). "Los derechos humanos y los derechos fundamentales", en AA.VV. (CASTELLÁ ANDREU, Josep Mª, editor): *Derecho Constitucional Básico.* Barcelona: Huygens, pp. 425-448.

- EUROPEAN COMMISSION (2019). *Annual self-assessment reports of signatories to the Code of Practice on Disinformation*. Disponible en: https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019
- EUROPEAN COMMISSION (2018). *Flash Eurobarometer 464 Fake news and disinformation online,* [online]. Pp.1-51. Disponible en: https://op.europa.eu/en/publication-detail/-/publication/2d79b85a-4cea-11e8-be1d-01aa75ed71a1/language-en
- EUROPEAN COMMISSION (2018b). *A multi-dimensional approach to disinformation. Report of the independent High level Group on fake news and online disinformation.* Disponible en: https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1
- EUROPEAN COMMISSION (2020). *Code of Practice on Disinformation*. Disponible en: https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation
- EUROPEAN DATA PROTECTION BOARD (2020). *Thirty-first Plenary session: Establishment of a taskforce on TikTok, Response to MEPs on use of Clearview AI by law enforcement authorities, Response to ENISA Advisory Group, Response to Open Letter NYOB.* Disponible en: https://edpb.europa.eu/news/news/2020/thirty-first-plenary-session-establishment-taskforce-tiktok-response-meps-use_en
- EUSKADI (2018). *Voto electrónico. Voto electrónico en el mundo.* Disponible en: www.euskadi.eus/informacion/voto-electronico-voto-electronico-en-el-mundo/web01-a2haukon/es/
- FERNÁNDEZ DELPECH, Horacio (2014). *Manual de Derecho Informático.* Ciudad Autónoma de Buenos Aires: Abeledo Perrot.
- FREEDOM HOUSE (2019). "*The Crisis of social media*", [online]. Pp.1-30. Disponible en: https://freedomhouse.org/report/freedom-net/2019/crisis-social-media
- GARCÍA RODRÍGUEZ, Juan Ignacio (2011). "Los desafíos de los organismos electorales latinoamericanos en el siglo XXI y la incorporación de la tecnología". *Revista Derecho Electoral Tribunal Supremo de Elecciones Republica de Costa*

Rica, [en línea]. Nro.11, pp. 1-20. Disponible en: www.tse.go.cr/revista/art/11/garcia_rodriguez.pdf

- GÒMEZ DE ÁGREDA, Ángel (2018). "Posverdad y 'fake news'. Falsas noticias, no noticias falsas".*Telos: Cuadernos de comunicación e innovación*, [en línea]. Nro. 109, pp.18-21. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6855661

- GONZÁLEZ DE LA GARZA, Luis Miguel (2009). "Voto electrónico por internet y riesgos para la democracia (II)". *Revista de Derecho Político,* [en línea]. Nro. 77, pp. 213-249. Disponible en: http://revistas.uned.es/index.php/derechopolitico/article/view/9109

- HOWARD, Philip N., WOOLLEY, Samuel & CALO, Ryan (2018) "Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration". *Journal of Information Technology & Politics*, [online]. V.15, nro. 2, pp. 81-93.Disponible en: https://www.tandfonline.com/doi/full/10.1080/19331681.2018.1448735

- LAGOMARSINO MONTOYA, Mario, VÉLIZ BURGOS, Alex, PAVIÉ NOVA, Alex y NASS ÁLVAREZ, Juan Luis (2019)."Educación y Democracia. Una alianza necesaria para la sociedad abierta y contra la demagogia, conducida por la Fake News". *Revista internacional de filosofía y teoría social,* [en línea]. Nro.4, pp.137-146. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7529042

- LÓPEZ AGUIRRE, José Luis, ACOSTA VALVERDE, Miguel y ESTRADA GARCÍA, María Concepción (2019). "Notas falsas en la contienda electoral: análisis de la labor de Verificado 2018", en AA.VV. (GOMEZ AGUILERA, *Blanca Nahayeli* Y LOPEZ AGUIRRE, Jose Luis. Coord.): *Agenda sociodigital de la campaña presidencial de 2018 Temas, emociones y notas falsas que motivaron la interacción político-ciudadana,*[en línea]. Pp.179-206.Coahuila: Universidad Autónoma de Coahuila. Disponible en: https://www.researchgate.net/publication/341554381

- LÓPEZ BORRULL, Alexandre, VIVES GRÀCIA, Josep y BADELL, Joan-Isidre (2018). "Fake news, ¿amenaza u oportunidad para los profesionales de la información y la documentación?". *El profesional de la información,* [en línea]. V.

27, nro. 6, pp.1346-1357. Disponible en: www.researchgate.net/publication/329452860_Fake_news_amenaza_u_oportunidad_para_los_profesionales_de_la_informacion_y_la_documentacion

- MARTÍNEZ LADRÓN DE GUEVARA, Jorge (2013). *Fundamentos de programación en Java.* [en línea] Madrid: Maths Universidad, s.l. Disponoble en: https://www.academia.edu/28946526/Fundamentos_de_Programacion_en_Java_Jose_Martinez_Ladron_de_Guevara
- MARTÍN NÚÑEZ, Esther (2018). "La ley y los tipos de ley", en AA.VV. (CASTELLÁ ANDREU, Josep Mª, editor): *Derecho Constitucional Básico.* Barcelona: Huygens, pp. 273-292.
- MARTÍN NÚÑEZ, Esther (2018b). "La constitución y el ordenamiento jurídico", en AA.VV. (CASTELLÁ ANDREU, Josep Mª, editor): *Derecho Constitucional Básico.* Barcelona: Huygens, pp. 227-250.
- MEIXUEIRO NÁJERA, Gustavo (2017). *Las fake news y las elecciones*. Disponible en: http://www.ieepco.org.mx/articulos-opinion/las-fake-news-y-las-elecciones
- OFICINA DE SEGURIDAD DEL INTERNAUTA (2020). *Deepfakes, ¿cómo se aprovechan de esta tecnología para engañarnos?*. Disponible en*:* www.osi.es/es/actualidad/blog/2020/04/01/deepfakes-como-se-aprovechan-de-esta-tecnologia-para-enganarnos
- ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (2014). *Tecnologías aplicadas al ciclo electoral*, [en línea]. Pp. 1-67. Disponible en: www.oas.org/es/sap/docs/deco/tecnologias_s.pdf
- PANIZO ALONSO, Luis (2007). *Aspectos tecnológicos del voto electrónico,* [en línea]. Lima: ONPE. Disponible en: www.researchgate.net/publication/259668840_Aspectos_tecnologicos_del_voto_electronico
- PARLAMENTO EUROPEO. Resolución del Parlamento Europeo, de 15 de junio de 2017, sobre las plataformas en línea y el mercado único digital (2016/2276(INI)). Disponible en: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0272_ES.html

- PÉREZ COLOMÉ, Jordi (2020). *La guerra contra TikTok: ¿es la 'app' china un peligro para Occidente?*. Disponible en: https://elpais.com/tecnologia/2020-08-02/la-guerra-contra-tiktok-es-la-app-un-peligro-para-occidente.html
- PUIG, Sebastián (2017*). "Desinforma, que algo queda": el fenómeno de las 'fake news' en el siglo XXI.* Disponible en: http://agendapublica.elpais.com/desinforma-algo-queda-fenomeno-las-fake-news-siglo-xxi/
- RAE. Real Academia Española (2014). Disponible en: https://dle.rae.es/medio#BgOCDE6
- RODRÍGUEZ-FERNÁNDEZ, Leticia (2019). "Desinformación y comunicación organizacional: estudio sobre el impacto de las fake news". *Revista Latina de Comunicación Social,* [en línea]. Nro. 74, pp. 1714 a 1728. Disponible en: http://www.revistalatinacs.org/074paper/1406/89es.html
- ROMERO RODRIGUEZ, Luis M., VALLE RAZO, Ana L., TORRES TOUKOUMIDIS, Ángel (2018). "Hacia una construcción conceptual de las Fake News: Epistemologías y Tipologías de las Nuevas Formas de Desinformación", en AA.VV. (PEREZ SERRANO, María José, ALCOLEA DIAZ, Gema y NOGALES BOCIO, Antonia I., Coord.): *Poder y Medios en las Sociedades del Siglo XXI.* España: Egregius, pp. 259-274.
- RUBIO, Rafael y JOVE, Matías (2006). "Una nueva revolución electoral". *Cuaderno de pensamiento político,* [en línea]. Nro.9, pp. 211-225. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=1376308
- RUBIO NÚÑEZ, Rafa (2018). "Los efectos de la posverdad en la democracia". *Revista de Derecho Político,* [en línea]. Nro. 103, pp. 191-228. Disponible en: http://revistas.uned.es/index.php/derechopolitico
- RUBIO NÚÑEZ, Rafael (2018b). "La amenaza tecnológica en los procesos electorales. Una respuesta jurídica". *Revista de Privacidad y Derecho Digital,* [en línea]. Nro.11, pp. 109-146. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6673789

- RUBIO, Rafa (2010) “Las nuevas tecnologías en la campaña electoral”, en AA.VV. (CARPIO GARCÍA, José Ángel y BARNÉS, Jorge Santiago Barnés, coords.): *Gestión Actual del consultor político.* Madrid: LID.
- SANZ ROMERO, Marta (2019).*¿Qué es y en qué consiste Deepfake?*.Disponible en: https://computerhoy.com/reportajes/tecnologia/consiste-deepfake-446355
- SCHMITT, Carl (2006). *Legalidad y Legitimidad.* Granada: Comares.
- TELLO LEAL**,** Edgardo; TELLO LEAL, Diego Armando y SOSA REYNA, Claudia Maricela (2012). “Reflexiones sobre el uso de las tecnologías de información y comunicación en las campañas electorales en México: e-campañas”**.** *Revista Virtual Universidad Católica del Norte,* [en línea]. Nro.36**,** pp. 33-47. Disponible en: https://revistavirtual.ucn.edu.co
- THOMPSON, Alex (2016). *Journalists and Trump voters live in separate online bubbles, MIT analysis shows.* Disponible en: www.vice.com/en_us/article/d3xamx/journalists-and-trump-voters-live-in-separate-online-bubbles-mit-analysis-shows
- TORRES SORIANO, Manuel R. (2017). *Hackeando la democracia: operaciones de influencia en el ciberespacio*. Disponible en: http://www.ieee.es/contenido/noticias/2017/06/DIEEEO66-2017.html
- TULA, María Inés (2012). “Democracia, elecciones y nuevas tecnologías. El voto electrónico”. *Revista Mexicana de Análisis Político y Administración Pública*, [en línea]. V. 1, nro. 2, pp. 9-21. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=4219614
- TUÑON NAVARRO, Jorge, OLEART, Álvaro. y BOUZA GARCÍA, Luis (2019). “Actores Europeos y Desinformación: la disputa entre el *factchecking*, las agendas alternativas y la geopolítica”. *Revista de Comunicación*, [en línea]. Vol.18, nro. 2, pp. 245-260. Disponible en: https://doi.org/10.26441/RC18.2-2019-A12
- WE LIVE SECURITY (2020) *Glosario*. Disponible en: https://www.welivesecurity.com/la-es/glosario/

2. Normativa:

- AEPD. Circular 1/2019, de 7 de marzo, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales relativos a opiniones políticas y envío de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos, federaciones, coaliciones y agrupaciones de electores al amparo del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General. Boletín Oficial del Estado. Nro. 60, de 11 de marzo de 2019, páginas 22834 a 22840. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-3423
- CDFUE. Carta de los Derechos Fundamentales de la Unión Europea. Diario Oficial de la Unión Europea. Nro. 83, de 30 de marzo de 2010, páginas 389 a 403. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70003
- CEDH. Instrumento de Ratificación del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950, y enmendado por los Protocolos adicionales números 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966, respectivamente. Boletín Oficial del Estado. Nro. 243, de 10 de octubre de 1979, páginas 23564 a 23570. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1979-24010
- CIDH. Convención Americana sobre derechos Humanos.(1969). Disponible en: www.oas.org/dil/esp/tratados.htm
- CODIGO ELECTORAL NACIONAL ARGENTINO. Ley 19.945, texto ordenado por Decreto No. 2135/83, del Código Electoral Nacional Argentino. Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/19442/texact.htm
- CÓDIGO PENAL DE LA NACIÓN ARGENTINA. LEY 11.179, T.O. 1984 actualizado. Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm

- CÓDIGO PENAL ESPAÑOL. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Boletín Oficial del Estado. Nro. 281, 24 de noviembre de de 1995. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444
- COMISIÓN EUROPEA (2018). "*Código de buenas prácticas de la Unión en materia de desinformación"*, [en línea]. Pp.1-12. Disponible en: https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation
- CONSTITUCION DE LA NACION ARGENTINA (1953). Ley Nº 24.430. Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm
- CONSTITUCION ESPAÑOLA. Boletín Oficial del Estado, nro. 311, de 29 de diciembre de 1978. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229
- CONVENIO SOBRE LA CIBERDELINCUENCIA. Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. Boletín Oficial del Estado. Nro. 226, de 17 de septiembre de 2010, páginas 78847 a 78896. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221
- ESTRATEGIA DE SEGURIDAD NACIONAL. Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2017. Boletín Oficial del Estado, nro. 309, de 21 de diciembre de 2017, páginas 125966 a 126004. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2017-15181
- LEY ORGÁNICA 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Boletín Oficial del Estado. Nro. 115, de 14 de mayo de 1982, páginas 12546 a 12548. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1982-11196
- LOPDyGDD. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Boletín Oficial del Estado. Nro. 294, de 06 de diciembre de 2018. Disponible en: *https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673*

- LOREG. Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General. Boletín Oficial del Estado, nro.147, de 20 de junio de 1985. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1985-11672
- REGLAMENTO (UE) Nro. 1215/2012 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 12 de diciembre de 2012 relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil. Diario oficial de la Unión Europea. Nro.351, de 20 de diciembre de 2012, páginas 1 a 32. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2012-82604
- RGPD. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

3. Jurisprudencia:

- STC. España. Tribunal Constitucional (Pleno). Sentencia núm. 76/2019 de 22 de mayo de 2019.