Papeles el tiempo de los derechos

ACERCAMIENTO AL VALOR PROBATORIO DE LAS PRUEBAS EN FORMATO DIGITAL: AMENAZAS EFECTUADAS POR MEDIO DE UNA APLICACIÓN MÓVIL

Francisco José Álvarez Gómez
Asesor Jurídico del Grupo Tragsa en la Secretaría General de Inclusión

Palabras Clave: Ciberdelincuencia, Redes Sociales, Delitos Informáticos, Prueba digital, Carga Probatoria.

Key Words: Cybercrime, Social Networking, Computer Crime, Digital Evidence, Burden of Proof.

Número: 21 Año: 2023

ISSN: 1989-8797

Comité Evaluador de los Working Papers “El Tiempo de los Derechos”

María José Añón (Universidad de Valencia)
María del Carmen Barranco (Universidad Carlos III)
María José Bernuz (Universidad de Zaragoza)
Rafael de Asís (Universidad Carlos III)
Eusebio Fernández (Universidad Carlos III)
Andrés García Inda (Universidad de Zaragoza)
Cristina García Pascual (Universidad de Valencia)
Isabel Garrido (Universidad de Alcalá)
María José González Ordovás (Universidad de Zaragoza)
Jesús Ignacio Martínez García (Universidad of Cantabria)
Antonio E Pérez Luño (Universidad de Sevilla)
Miguel Revenga (Universidad de Cádiz)
Maria Eugenia Rodríguez Palop (Universidad Carlos III)
Eduardo Ruiz Vieytez (Universidad de Deusto)
Jaume Saura (Instituto de Derechos Humanos de Cataluña)

“ACERCAMIENTO AL VALOR PROBATORIO DE LAS PRUEBAS EN FORMATO DIGITAL: AMENAZAS EFECTUADAS POR MEDIO DE UNA APLICACIÓN MÓVIL”

Francisco José Álvarez Gómez

Asesor Jurídico del Grupo Tragsa en la Secretaría General de Inclusión

SUMARIO: 1. Introducción 2. Delitos 2.1 Amenazas 2.2 *Stalking* 2.3 *Sexting* 3. Pruebas Digitales 4. Conclusiones 5. Bibliografía

RESUMEN

En el siguiente trabajo, voy a intentar analizar cuál es la práctica que se usa a la hora de presentar las pruebas con carácter digital, ante hechos que pueden ser constitutivos de delitos a través de redes sociales.

En el año 2021, se conocieron 305.477 hechos que podrían ser constitutivos de delitos a través de medios informáticos, de los que podríamos considerar que se comenten por medio de la “ciberdelincuencia”; pues bien, en el siguiente trabajo analizaré cual es la forma de poder presentar las pruebas derivadas de estos hechos, ya sea por las partes implicadas o por el Fiscalía, que, en estos casos será la Fiscalía especializada en Delitos Informáticos.

El uso común de redes sociales, así como smartphone o Tablet ha hecho que los tipos delictivos que pueden calificarse por el uso de estos medios, se haya incrementado de manera exponencial.

Al igual que los sujetos que pueden ser los que constituyan estos delitos, no se tratan de grandes organizaciones criminales, sino usuarios comunes siendo un gran número de los comitentes, menores de edad.

ABSTRACT

In the following work, I am going to try to analyse the practice used when presenting evidence of a digital nature, in the face of events that may constitute crimes through social networks.

In the year 2021, 305,477 facts were known that could be constitutive of crimes through computer media, of which we could consider that they are committed by means of "cybercrime"; well, in the following work I will analyse how to present the evidence derived from these facts, either by the parties involved or by the Prosecutor's Office, which, in these cases will be the Prosecutor's Office specialised in Computer Crimes.

The common use of social networks, as well as smartphones and tablets, has led to an exponential increase in the types of offences that can be classified by the use of these media.

As well as the subjects that may be involved in these crimes, they are not large criminal organisations, but common users, with a large number of the perpetrators being minors.

1. INTRODUCCIÓN

La actual situación social nos lleva a pensar que algo se esta haciendo mal. El crecimiento de los delitos cometidos por medios digitales es innegable, así como lo son las consecuencias que llevan aparejadas. Entidades como UNICEF están advirtiendo de las consecuencias o efectos derivados de ser victimas de estos delitos, como son los efectos mentales, físicos o emocionales que se dan al sufrir ciberacoso, siendo victimas de campañas contra uno mismo o las consecuencias del hostigamiento reiterado.

Según *Save the Children*: el 40% de los menores españoles podrían haber sufrido ciberacoso durante su infancia.

El ser victima de estos hechos, pueden llevar aparejados los siguientes daños: problemas físicos, daños en la autoestima, cambios de humor, depresión, alteración en el sueño o incluso puede llevar al suicidio de la víctima (hecho demasiado común).

Como señala Escarlata Gutiérrez Mayo: "*El uso de redes sociales es práctica habitual y los cambios que experimentan las mismas son continuos, ya que se someten a constante evolución para responder a las exigencias e intereses que mueven la sociedad. Todo ello supone, a su vez, un importante desconocimiento por parte del usuario sobre la herramienta que está utilizando ya que, a pesar de que se sobreentiende el buen manejo del mundo digital por cualquier persona habituada al mismo, las diferentes peculiaridades de cada red social pueden hacer peligrar el buen uso de estas y la aparición o concurrencia de conductas que, muchas veces, cuesta distinguir y denunciar y denunciar como delictiva.*

Es por ello por lo que, en el siguiente trabajo, expondré dos marcos: el primer marco va a ser un acercamiento a los posibles delitos que pueden derivar para el ciberacoso entre ellos comentaré: amenazas (artículo 171.4 del Código Penal), *stalking* (artículo 172 ter párrafo 2 del Código Penal) o *sexting* (artículo 197.7 del Código Penal); y el segundo marco es como habría que presentar las pruebas para poder denunciar y enjuiciar el posible delito derivado de los hechos.

2. DELITOS

2.1 AMENAZAS

La Ley Orgánica 10/1995 de 23 de noviembre, del Código Penal, tipifica el delito de Amenazas en los artículos 169 y siguientes, donde establece:

"*El que amenazare a otro con causarle a él, a su familia o a otras personas con las que esté íntimamente vinculado un mal que constituya delitos de homicidio, lesiones, aborto, contra la libertad, torturas y contra la integridad moral, la libertad sexual, la intimidad, el honor, el patrimonio y el orden socioeconómico, será castigado:*

1.º Con la pena de prisión de uno a cinco años, si se hubiere hecho la amenaza exigiendo una cantidad o imponiendo cualquier otra condición, aunque no sea ilícita, y el culpable hubiere conseguido su propósito. De no conseguirlo, se impondrá la pena de prisión de seis meses a tres años.

Las penas señaladas en el párrafo anterior se impondrán en su mitad superior si las amenazas se hicieren por escrito, por teléfono o por cualquier medio de comunicación o de reproducción, o en nombre de entidades o grupos reales o supuestos.

2.º Con la pena de prisión de seis meses a dos años, cuando la amenaza no haya sido condicional."

Queda claro que las amenazas son la expresión conferida por un sujeto contra otro u otros para causarle un mal con el fin de menoscabar su libertad.

Es por tanto que podemos asegurar que el bien jurídico protegido es la libertad, aunque destacaría que la jurisprudencia lo ha extendido a la seguridad del individuo.

En el caso que nos ocupa, estaríamos considerando que las amenazas son cometidas por medio de redes sociales o dispositivos electrónicos, donde la doctrina, la jurisprudencia, así como la practica aceptada entiende que es método de comisión del hecho delictivo.

Me gustaría señalar como medio probatorio la IP, tanto para aquellas partes que puedan intervenir en el proceso, ya sea la parte defensora o la acusación, es la Sentencia del Tribunal Supremo 342/2013 de 17 abril.

Es entendible, por tanto, que el Juez instructor, a raíz de la denuncia que se pueda interponer por la víctima de una amenaza *on line* pueda acordar dirigir mandamiento al prestador del servicio en internet con el fin de que facilite a la Brigada Provincial de Policía Judicial de delitos tecnológicos las IP de las conexiones al ordenador en la cuenta del correo electrónico de la víctima en su generación, accesos a bandejas de correo electrónico más recientes que se conserven, así como IPs de conexión.

Una vez obtenida la información requerida, la Policía Judicial se dirigirá al Juez instructor solicitando mandamiento judicial, dirigido a las operadoras, con el fin de que faciliten a los agentes comisionados cuantos datos dispongan del usuario o usuarios a los que se les asignaron las direcciones IPs que se conozcan debiendo incluir en esa información los momentos exactos de inicio y finalización de asignación de dicha dirección IP al usuario, así como, en su caso, de las líneas telefónicas de conexión desde las que se produjeron los accesos, el titular y ubicación de las mismas.

A raíz de los datos proporcionados por las operadoras, será posible la identificación de la persona que, desde esa IP, accedía a la red y utilizaba la red como vehículo para contactar con la víctima.

2.2 STALKING

La Ley Orgánica 1/2015, de 30 de marzo, introdujo dentro de los delitos contra la libertad un nuevo tipo penal, que es el delito de acoso. Se intentaba dar encaje a conductas de indudable gravedad que no pueden ser calificadas como delito de amenazas o de coacciones.

"*Se trata de todos aquellos supuestos en los que, sin llegar a producirse necesariamente el anuncio explicito o no de la intención de causar algún mal (amenazas) o el empleo directo de violencia para coartar la libertad de la victima (coacciones), se producen conductas reiteradas por medio de las cuales se menoscaba gravemente la libertad y sentimiento de seguridad de la víctima, a la que se somete a persecuciones o vigilancias constantes, llamadas reiteradas, u otros actos continuos de hostigamientos".*

El bien jurídico protegido es el proteger a la victima frente a conductas que menoscaban la libertad o sentimiento de seguridad de la víctima. Esto lo señala la Sentencia del Tribunal Supremo 554/2017, de 12 de julio, donde se establece: "*Es claro que en relación con este delito en la medida que supone un ataque al bien jurídico de la libertad individual y al derecho a vivir tranquilo y sin zozobra, se está ante un caso de merecimiento de pena y de necesidad de la pena, en definitiva, de otorgar relevancia penal a las conductas típicas".*

Me gustaría desarrollar dos conceptos, el primero es la prolongación en el tiempo de los hechos que pueden ser constitutivos de stalking, es por ello por lo que en la Sentencia 324/2017 de 8 de mayo, donde se establece: "*Esos acercamientos metajurídicos no condicionan la interpretación de la concreta formulación típica que elija el legislador. Se trata de estudios desarrollados en otros ámbitos de conocimiento dirigidos a favorecer el análisis científico y sociológico del fenómeno y su comprensión clínica. Pero tampoco son orientaciones totalmente descartables: ayudan en la tarea de esclarecer la conducta que el legislador quiere reprimir penalmente y desentrañar lo que exige el tipo penal, de forma explícita o implícita.*

No es sensato ni pertinente ni establecer un mínimo numero de actos intrusivos como se ensaya en algunas definiciones, ni fijar un mínimo lapso temporal. Pero sí podemos destacar que el dato de una vocación de cierta perdurabilidad es exigencia del delito descrito en el articulo 172 ter CP, pues solo desde ahí se puede dar el salto a esa incidencia en la vida cotidiana."

El otro concepto que me gustaría destacar es la alteración grave de la vida cotidiana del ofendido. La Sentencia 324/2017 de 8 de mayo expone que, si el tipo penal no exige una planificación del delito, lo que sí requiere es una "metódica secuencia de acciones que obligan a la víctima, como única vía escapatoria, a variar, sus hábitos cotidianos", y la evaluación de tal secuencia se realizará atendiendo al estándar del "persona media", con particular cuidado de las circunstancias concretas de la victima ante su especial vulnerabilidad, capacidades psíquicas, etc.

Por ejemplo, constituye alteraciones en la vida rutinaria de la víctima, entre otras, la necesidad de cambiar de número de teléfono o tener que cambiar los lugares de ocio o sus rutas habituales, así como el miedo de la victima a salir sola a la calle, insomnio o intranquilidad, no siendo necesario un informe médico que recoja esta alteración en la víctima.

2.3 SEXTING

El Sexting, se introdujo a raíz de la reforma en la Ley Orgánica 1/2015, de 30 de marzo, donde se establece en el articulo 197.7 lo siguiente: "*Será castigado con una pena de prisión de tres meses a*

un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona".

El bien jurídico protegido en es el derecho a la intimidad, que esta amparado en el articulo 18.1 de la Constitución, que garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

La Sentencia 379/2018, de 23 de julio establece: "*forman parte de los bienes de la personalidad que pertenecen al ámbito de la vida privada. Salvaguardan estos derechos un espacio de intimidad personal y familiar que queda sustraído a intromisiones extrañas, destacando la necesaria protección frente al creciente desarrollo de los medios y procedimiento de captación, divulgación y difusión de esta y de datos y circunstancias que pertenecen a la intimidad".*

La Circular 3/2017 de la Fiscalía General del Estado establece que no es necesario que se trate de imágenes o grabaciones con contenidos sexuales, sino referidas a la intimidad.

Destacando el derecho a la propia imagen, en la Sentencia 437/2011, de 29 de junio, se establece que: "*es de especial interés lo resuelto en la STS de 11 de abril de 1987, citada en otras posteriores, según la cual el Derecho a la propia imagen consiste en la facultad exclusiva del interesado a difundir o publicar su propia imagen y por ende su*

Derecho a evitar su reproducción; se trata de un Derecho de la personalidad y se entiende por imagen la representación gráfica de figura humana mediante un procedimiento mecánico o técnico de reproducción."

3. PRUEBAS DIGITALES

Es posible definir doctrinalmente la prueba tecnológica como aquel archivo informático que contine metadatos, esto es, aquella información oculta sobre su contenido almacenada en forma de ceros y unos (código binario) y que necesita, por tanto, de su transformación en información legible.

Estas pruebas, son evidencias de la realidad que cuentan con una mayor información sobre su contenido y que podrán aportarse al proceso.

Para la aportación de pruebas nos regimos por las reglas establecidas en los articulo 785.1 y 786.2 de la Ley de Enjuiciamiento Criminal, la posibilidad para las partes de aportar prueba documental al inicio de las sesiones del juicio oral. Aunque existen momentos anteriores en los que es posible aportar ese tipo de prueba.

La Sentencia del Tribunal Supremo 197/2018, establece que:

"*Ahora bien, esta Sala debe fijar claro que sobre la proposición de prueba documental al inicio del juicio oral no existe la denominada proposición de prueba sorpresiva por las partes, concepto que, desde una construcción procesal es inadmisible, dado que admitida procesalmente la posibilidad de proponer prueba documental al inicio del juicio oral, no puede aludirse al "factor sorpresa" en su aportación al inicio de las sesiones del juicio oral para rechazar la prueba que se propone, dado que es un derecho de la parte llevarlo a cabo, y por ser al inicio de las sesiones cuando, también, las partes pueden llevarlo a cabo, tanto documental, como pericial o testifical. Otra cuestión distinta es la relevancia de esa aportación, o no, al objeto de alterar el proceso de convicción que pueda haber llevado el Tribunal tras el examen de la prueba practicada. Pero la viabilidad procesal de su aportación y su admisibilidad dependerá de otros factores en torno a los conceptos de "necesidad", o pertinencia", pero no acerca de un "carácter sorpresivo" de su aportación, dado que ello no puede predicarse de una vía de proposición de prueba al inicio de las sesiones del juicio oral.*"

Cabe destacar, la Sentencia del Tribunal Supremo 300/2015, de 19 de mayo, se ha generalizado el convencimiento de las pruebas tecnológicas son fácilmente manipulables, lo que provoca cierto rechazo hacia las mismas por parte de los operadores jurídicos.

Esta resolución dice: "*la posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación la identidad de los interlocutores y, en fin, la integridad de su contenido.*"

Pese a la existencia del riesgo de alteración de las pruebas, tal como existen de las demás; las posibles soluciones para su tratamiento ya están previstas por el ordenamiento.

Por ello, hay que destacar que uno de los medios mas utilizados para aportar al proceso una prueba tecnológica es vía documento privado o público.

La LEC regula el medio de prueba documental en los artículos 317 a 334.

También ha cogido importancia la prueba documental digital, vía pericial de experto informático. Esto lleva a entrar en el análisis pormenorizado tanto de IP, metadatos o lo que viene siendo lo mismo, el análisis del lugar donde se ejecutaron los hechos, que medio se empleó (teléfono, tablet u ordenador).

El otro medio de para aportar la prueba documental es por vía de documento privado, o lo que viene siendo el uso de "pantallazos", como medio de prueba documental, una cuestión muy controvertida, puesto que es relativamente sencillo la manipulación de las conversaciones de WhatsApp.

Es la Sentencia del Tribunal Supremo, de la Sala de lo Social, 706/2020, de 23 de julio, la que sostiene que: "*el avance tecnológico ha hecho que muchos documentos se materialicen y presenten a juicio a través de los nuevos soportes electrónicos, lo que no debe excluir su naturaleza de prueba documental, con las necesarias adaptaciones. Si no se postula un concepto amplio de prueba documental, llegará un momento en que la revisión fáctica casacional quedará vaciada de contenido si se limita a los documentos escritos, cuyo uso será exiguo. En consecuencia, debemos atribuir la naturaleza de prueba documental a los citados correos electrónicos obrantes a los folios 730, 731 y 505 de las actuaciones. Ello no supone que todo correo electrónico acredite el error fáctico de instancia, al igual que sucede con los documentos privados. Para ello será necesario valorar si se ha impugnado su autenticidad por la parte a quien perjudique; si ha sido autenticado, en su caso; y si goza de literosuficiencia".*

Y por último, señalar la posibilidad de aportar la prueba documental, vía documento notarial. En este caso, es un medio de aporte de prueba documental, donde el interesado irá a una notaría, acompañado de su abogado, donde se levantará un acta donde conste los datos del aparato electrónico, así como una descripción y aporte de fotografías siempre efectuadas por el propio Notario, para dar fe de la veracidad del documento, y así poder considerarlo como un documento público, y gozar de la especial protección de que deriva esta posibilidad.

4. CONCLUSIONES

Como he podido transmitir a lo largo de esta breve comunicación, las conductas criminales han cambiado en muy poco tiempo, y algo que solía decir mi profesora de Derecho Penal, la Profesora Doctora Doña Elena Núñez, era que el criminal siempre iba mas adelantado al Derecho Penal.

He intentado acercar dos conductas que se han convertido en algo común en los juzgados, llevando a crear fiscalías especializadas en delitos informáticos, así como innumerables apoyos doctrinales y jurisprudenciales, que apoyan las actuaciones y que dan la importancia debía a tan magno problema.

Es cierto que he elegido estos delitos, y la relación con la aportación de prueba documental, porque la línea de defensa o la acusación que se puedan ejercer, dependiendo que operador jurídico eres; es importante. Tanto para la aportación, como para la posible impugnación o para poder tener el principio de contradicción de las pruebas en el proceso.

El uso de la analogía, o del buen saber y hacer del tribunal, ante la falta de medios legislativos que describan un marco donde nos podamos amparar, es otra de las comunes reacciones que nos encontramos a lo largo de todo el proceso.

Aunque haya intentado nombrar el proceso penal, es equiparable a los demás procesos, tanto a un procedimiento de divorcio de menores, donde la aportación de WhatsApp es muy común, incluso el uso de audios de menores en procedimientos de filiación.

En el caso de la jurisdicción social, tenemos el uso del correo electrónico corporativo. Eso daría no solo para una pequeña comunicación, sino para una tesis doctoral, puesto que el uso del correo electrónico como correo privado, la vigilancia y control del correo corporativo por parte de la empresa a espaldas del trabajador sin preaviso, o la transmisión de información corporativa por medio del correo corporativo al correo particular.

Nuevamente citando a la jurisdicción social, también tenemos los reiterados casos del uso de aplicaciones de mensajería instantánea (*WhatsApp*) para hacer efectivos los despidos, reiteradas sentencias de nuestros tribunales ya han podido calificar este medio, como un medio valido de notificación del despido. Algunas añaden que será necesaria una notificación formal de manera posterior, pero que sirva de referencia que el empleado ha dejado de prestar servicios para la empresa.

Volviendo a la jurisdicción penal, es claro y manifiesto que el uso de las nuevas tecnologías, así como todo el entorno que lo acompaña, esta siendo un reto muy importante para el legislador penal y procesal penal. La capacitación de medios para poder enjuiciar hechos, que puedan ser calificados de hechos delictivos, puede vulnerar el principio acusatorio, el principio de legalidad o el principio de tipicidad, dando por si una clara vulneración de los derechos fundamentales del ciudadano, que dependiendo del momento procesal pueda tener la calificación de investigado o acusado.

Por todo lo anteriormente expuesto, y debido a la brevedad del trabajo, me gustaría finalizar exponiendo la gravedad del asunto, no solo del medio probatorio; sino del perfil criminal que esta siendo objeto de las condenas, así como de las victimas de los delitos derivados de uso de medios informáticos, y de la especial complejidad que llevan amparada, tanto para su instrucción, así como del enjuiciamiento y posterior condena.

5. BIBLIOGRAFIA

5.1 Constitución Española

5.2 Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal

5.3 Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

5.4 Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

5.5 Real Decreto de 14 de septiembre de 1882 por el que se aprueba la ley de Enjuiciamiento Criminal.

5.6 Circular 3/2017, de 21 de septiembre, sobre la reforma del Código Penal operada por la Ley Orgánica 1/2015, de 30 de marzo, en relación con los delitos de descubrimientos y revelación de secretos y los delitos de daños informáticos.

5.7 Sentencias

5.7.1 Sentencia del Tribunal Supremo, Sala Segunda de lo Penal, 437/2011, de 29 de junio.

5.7.2 Sentencia del Tribunal Supremo, Sala Segunda de lo Penal, 300/2015, de 19 de mayo.

5.7.3 Sentencia del Tribunal Supremo, Sala Segunda de lo Penal, 342/2013, de 17 de abril

5.7.4 Sentencia del Tribunal Supremo, Sala Segunda de lo Penal, 324/2017, de 8 de mayo.

5.7.5 Sentencia del Tribunal Supremo, Sala Segunda de lo Penal, 554/2017, de 12 de julio.

5.7.6 Sentencia del Tribunal Supremo, Sala Segunda de lo Penal, 197/2018 de 25 de abril.

5.7.7 Sentencia del Tribunal Supremo, Sala Segunda de lo Penal, 379/2018, de 23 de julio.

5.7.8 Sentencia del Tribunal Supremo, Sala Cuarta de lo Social, 706/2020 de 23 de julio.