Facultad de Derecho
Universidad de La Laguna

Grado en: Derecho

Facultad de Derecho

Universidad de La Laguna

Curso 2018/2019

Convocatoria: Julio

“La nube” como objeto material del delito del art. 197 del CP

“The cloud” as a material object of crime of article 197 of the Penal Code

Realizado por la alumna Mikaela Alejandra Martinez

Tutorizado por el Profesor/a Esteban Sola Reche

Departamento: Disciplinas Jurídicas Básicas

Área de conocimiento: Derecho Penal

ANEXO DE ABREVIATURAS

Art.	Artículo
Cit.	Cita
Coord.	Coordinador
Coords.	Coordinadores
CP	Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
Ed.	Editor
Fj.	Fundamento jurídico
LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
n.	Número
NIST	National Institute of Standards and Technology
p.	Página
pp.	Páginas
S	Sentencia
ss.	Siguientes
TC	Tribunal Constitucional
TICs	Tecnologías de la información y la comunicación
TS	Tribunal Supremo

ABSTRACT

The relevance that cybercrime has acquired today, legislation that leaves gaps in punishability, the difficulty to determine the authorship and the place of commission of the crime and the emergence of a new resource such as cloud computing, have led to our realization the next question:

Is it possible to consider the cloud computing as a material object of the crime of art. 197 of the Spanish Penal Code?

This question has been the "x" that we have tried to clear in the present work. For this we have analyzed and studied the wording of art. 197 of the CP, based on previous studies referring to or linked to the seizure of traditional sources of intimate information. Examining whether it is possible to understand the "cloud" as a document (material object of the crime of Article 197 CP), for which, in turn, we have started from the concept provided by the CP in its art. 26.

Keywords: Cybercrime, cloud computing, material object, art. 197, seizure.

RESUMEN (entre 150 y 350 palabras)

La relevancia que ha adquirido la ciberdelincuencia en la actualidad, una legislación que deja lagunas de punibilidad, la dificultad para determinar la autoría y el lugar de comisión del delito y el surgimiento de un nuevo recurso como es la “nube” han propiciado que nos realicemos la siguiente pregunta:

¿Es posible considerar la “nube” como objeto material del delito del art. 197 del Código Penal Español?

Dicha cuestión ha sido la “x” que hemos intentado despejar en el presente trabajo. Para ello hemos analizado y estudiado la redacción del art. 197 del CP, partiendo de estudios realizados con anterioridad referentes o vinculados al apoderamiento de fuentes tradicionales de información íntima. Examinando si es posible entender la “nube” como documento (objeto material del delito del art. 197 CP), para lo cual, a su vez, hemos partido del concepto que nos proporciona el CP en su art. 26.

Palabras claves: Ciberdelincuencia, “nube”, objeto material, art. 197, apoderamiento.

SUMARIO **Pág.**

1. INTRODUCCIÓN:

1. Internet. *Cloud computing*. *Social networks*. Delito informático. Delito cibernético. Evidencia digital. Todos son términos cuyo común denominador es la Red, entendida como <<ciberespacio virtual>>[1], suponiendo la globalización y popularización de esta, un cambio en el modelo o paradigma de las relaciones[2] políticas, económicas, jurídicas, personales etc. Las Tecnologías de la Información y las Comunicaciones (TICs), las comunicaciones electrónicas y, por ende, la Sociedad de la Información[3], han supuesto una mejora innegable en la calidad de vida, a la par que han traído consigo problemas y situaciones a las cuales hay que darles respuesta y solución.

Para ello, es necesario, entre otros aspectos, un marco legal normativo que se ajuste a la realidad social actual en esta materia, con la finalidad de paliar la inseguridad en la que nos movemos y relacionamos, la cual propicia situaciones carentes de respuestas o que, simplemente se apañan provisionalmente a la espera de una legislación adecuada, que ya debería haber llegado. Si algo debe quedarnos claro es que, el enorme grado de dependencia que tienen los particulares, empresas y la Administración hoy en día con las TICs e internet va *in crescendo*, y no va a parar, dado que la tendencia es que abarque prácticamente todos los aspectos de nuestro día a día y vida real. Por lo tanto, podemos optar por parchear una realidad "nueva" no haciéndole frente, o podemos poner en la mano de la sociedad herramientas para que su vida "virtual" sea más segura y suscite los menores percances posibles.

2. En el presente trabajo trataremos un recurso que, parece haberse consolidado en el 2011[4], el denominado *cloud computing* o computación en la nube, como herramienta de almacenamiento y tratamiento de la información. Centrándonos en si podemos entender la "nube" como objeto material del delito, concretamente del tipo delictivo del artículo 197 del Código Penal Español, cuyo bien jurídico protegido es la intimidad, encontrándose ésta más vulnerable que nunca debido a los medios tecnológicos (medios

[1] El término cyberspace fue creado por William GIBSON en su obra Neuromancer (Editorial AceBooks, Nueva York, 1984). En dicha novela el autor describía una vida paralela a la física, es decir, un mundo virtual separado del real.
[2] BARRIO ANDRÉS*: Ciberdelitos Amenazas criminales del ciberespacio*, pp. 9 ss.
[3] DAVARA FERNÁNDEZ DE MARCOS: *Delitos informáticos*, p.17.
[4] MARTÍNEZ MARTÍNEZ: *Derecho y cloud computing*, p. 15 ss.

técnicos de captación y transmisión de la imagen y del sonido; la acumulación y procesamiento de la información, en concreto de los datos personales[5]). Lo cual ha supuesto el crecimiento de la preocupación por protegerla y, en nuestro caso, analizar si las herramientas jurídicas de las cuales disponemos actualmente la amparan o, por el contrario, necesitarían modificarse para logar una defensa de la misma adecuada y adaptada a la realidad social que vivimos.

2. ¿CONCEPTO DE DELITO INFORMÁTICO?

2.1. Una aproximación "conceptual". Antecedentes y contexto:

1. Debemos tener en cuenta que la delincuencia informática se encuentra dentro de lo que conocemos como "Derecho informático"[6], el cual no se encuentra actualmente configurado como una rama del Derecho, sino como una vertiente más, dentro de cada una de las actuales ramas (civil, administrativa, laboral o penal). No obstante, hay quien considera que dada "la complejidad de las relaciones informáticas, el crecimiento exponencial de las mismas o el hecho de que en el estudio de estas nuevas relaciones se transite de una rama del ordenamiento jurídico a la otra constantemente"[7], es motivo suficiente para reconsiderar la postura de que se debe entender como una nueva rama del ordenamiento jurídico.

A nuestro parecer, y sin entrar de pleno en el asunto, dado que no es objeto de estudio en el presente trabajo, consideramos que actualmente no sería lo más idóneo desvincular las cuestiones asociadas al derecho informático de cada rama del ordenamiento jurídico en las que se encuentran, para crear una rama independiente, lo

[5] DAVARA FERNÁNDEZ DE MARCOS: cit. n. 3, p. 47: "La primera ola de reformas legales surgió en el campo de la protección a la intimidad en los años 70 del siglo XX. Las nuevas tecnologías brindaban la posibilidad de formas de procesamiento, almacenamiento y transmisión de datos inexistentes hasta aquel momento. Datos relativos a las personas aparentemente insignificantes, sin comportar un riesgo a la intimidad personal en caso de encontrarse en manos de otros distintos a su titular, se convertían en una información valiosísima después de ser agrupados, tratados en forma conjunta, interrelacionados y analizados mediante los modernos medios tecnológicos.".

[6] HERNÁNDEZ DÍAZ: *Aproximación a un concepto de derecho penal informático.* p. 31 ss: El Derecho informático "…se define como <<conjunto de normas jurídicas que regulan la utilización de los bienes y servicios informáticos en la sociedad>>, incluyendo como objeto de estudio: 1º el régimen jurídico del software; 2º el derecho de las redes de transmisión de datos; 3º los documentos electrónicos; 4º los contratos electrónicos; 5º el régimen jurídico de las bases de datos; 6º el derecho a la *privacy*; 7º los delitos informáticos; y 8º otras conductas nacidas del uso de los ordenadores y de las redes de transmisión de datos."

[7] HERNÁNDEZ DÍAZ: cit. n. 6, p. 32.

cual entendemos que acarrearía consigo la creación de un nuevo orden jurisdiccional. Por tanto, creemos que es preferible que cada rama del derecho actual tenga su vertiente de derecho informático, con sus correspondientes especialistas y especialidades. Adoptamos esta postura, puesto que, consideramos que llegará el momento en que la informática, y, por ende, las TICs abarcarán prácticamente toda nuestra vida y día a día suponiendo, probablemente, una regulación muchísimo más exhaustiva que la actual, lo cual sería muy difícil abarcar desde una única rama del ordenamiento jurídico, al igual que mucho más complejo su estudio por los distintos profesionales.

2. Adentrándonos en nuestro objeto de estudio, debemos conocer el contexto a partir del cual se gestó o se comenzó a hablar de un concepto de delito informático en Europa y, por consiguiente, en España. A partir del <<Informe sobre la situación del crimen organizado en Europa>> realizado por el Consejo de Europa[8], se plasmó la evolución de las conductas delictivas (o que deberían ser consideradas como tal) vinculadas con las TICs.

En un momento determinado se empezaron a acumular cantidades descomunales de datos de carácter personal de los ciudadanos por los gobiernos, comenzando así la preocupación en torno al "carácter reservado, la acumulación y el uso que podría hacerse de tales datos"[9].

En la década de los setenta, los ordenadores pasaron a usarse masivamente en el mundo empresarial, de tal forma que la mayoría de las conductas delictivas o que podían llegar a serlo por encontrarse vinculadas a la informática, se daban en su vertiente económica (fraudes, manipulación de datos, espionajes empresariales etc.), lo cual supuso que se partiera de estas modalidades de delincuencia económica para definir lo que se debía entender por delito informático.

A partir de los años ochenta, los ordenadores personales se generalizaron, a la par que surgió la piratería del software, abriéndose paso así las primeras infracciones a la

[8] CONSEJO DE EUROPA, *Organised crime in Europe: the threat of cybercrime. Situation report*, 2004, pp. 84 ss.
[9] HERNÁNDEZ DÍAZ: cit. n. 6, p. 34.

propiedad intelectual y que, además, se van a extender a la música o películas a finales de los años noventa.

Concretamente en 1978, son conocidos por la sociedad los primeros casos de delincuencia informática patrimonial a través de la prensa. En este momento, Bequai considera que "en la definición del delito informático el acento debe ponerse en que los ordenadores pueden ser usados por el autor del delito no sólo como instrumentos para cometer el mismo sino también como objeto del delito"[10].

En España, el concepto de delito informático ("*computer crime*"), surge concretamente a finales de los ochenta, de la mano de Camacho Losa, García Moreno, Ramos Portero[11] o González Rus, aunque todavía en la legislación penal española no se establecía ningún delito o ilícito del ámbito tecnológico.

González Rus, en 1986, consideró imposible agrupar todos los tipos delictivos vinculados con las TICs y subsumirlos en un único concepto de delito, es por ello que clasificó los <<ilícitos informáticos>> "como un conjunto de delitos de carácter heterogéneo que puede dividirse en dos grandes grupos: por un lado, el de las amenazas para la intimidad personal y la esfera privada derivadas de la ingente acumulación de datos; y, por otro, el de los delitos patrimoniales, favorecidos en su comisión por las posibilidades que ofrecen las nuevas tecnologías"[12]. A partir del 2007 y en la actualidad, considera que no puede proponer un único concepto de delito informático[13].

Camacho Losa, en 1987, siendo consciente de que no había una definición de delito informático plenamente grata, entendió que debía considerarse como tal: "toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor, aun cuando no perjudique de forma directa

[10] HERNÁNDEZ DÍAZ: cit. n. 6, pp. 36 ss.
[11] BARRIO ANDRÉS: cit. n. 2. pp. 23 ss.
[12] HERNÁNDEZ DÍAZ: cit. n. 6, pp. 37 ss.
[13] GONZÁLEZ RUS: *Precisiones conceptuales y político-criminales sobre la intervención penal en Internet*, pp. 14 ss.

o inmediata a la víctima y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas"[14].

Con la llegada y expansión de Internet aparece una nueva forma de difundir contenidos ilegales o dañosos (pornografía infantil, discursos racistas o xenófobos etc.), es decir, iban surgiendo nuevas conductas delictivas o ilícitas asociadas a la informática que complicaron aún más la obtención de una definición de delito informático, puesto que estas conductas ya no solo se limitaban estrictamente al patrimonio o a la esfera de la intimidad. Actualmente, prácticamente cualquier delito puede ver favorecida su comisión o incluso cometerse a través de la utilización de las TICs.

Sin embargo, Romeo Casabona, en 1988 ya decía: "…en puridad no puede hablarse de un delito informático, sino de una pluralidad de delitos en los que nos encontramos, como única nota común, su vinculación de alguna manera con los ordenadores, pero ni el bien jurídico agredido es siempre de la misma naturaleza ni la forma de comisión del hecho- delictivo o merecedor de serlo- presenta siempre características semejantes".[15] Por ello, proponía el empleo de otras expresiones como "agresiones realizadas contra medios o sistemas informáticos, o a través de los mismos", al igual que han ido surgiendo otras como, <<criminalidad informática>> o <<delincuencia informática>> separando de esta manera la vertiente criminológica de la penal.

Una corriente minoritaria, siendo uno de sus defensores Davara Rodríguez, consideraba que "la realización de una acción, que reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático, ya sea hadware o software"[16] debe ser entendido como delito informático. Parece ser que dicha definición pone de manifiesto la existencia de acciones pertenecientes ya a una categoría penal,

[14] CAMACHO LOSA: *El delito informático*, pp. 25 ss.
[15] ROMEO CASABONA: *Poder informático y seguridad jurídica. La función tutelar del Derecho Penal ante las nuevas tecnologías de la información.* p. 41.
[16] DAVARA RODRÍGUEZ: *Derecho informático*, p. 302.

pero que son cometidas a través de elementos informáticos o vulnerando los mismos, sin aportación de elementos privativos que sustantiven categorías penales nuevas[17].

Por otro lado, Tiedemann, tras sus primeras definiciones que versaban sobre el aspecto patrimonial, acabó definiendo la criminalidad informática como "todo tipo de acto antijurídico según la ley penal vigente o socialmente perjudiciales y por eso penalizables en el futuro realizado con el empleo de un equipo de procesamiento de datos"[18].

3. En definitiva, tras una detallada lectura de las distintas definiciones de delito informático que se han ido suscitando con los años desde el surgimiento de este tipo de conductas delictivas hasta la actualidad, queda a la vista que no existe un acuerdo o consenso generalizado desde un punto de vista científico-jurídico acerca del concepto de delito informático, por lo que el "significado más utilizado en términos prácticos es aquel que los describe como conductas indebidas e ilegales donde interviene un dispositivo informático como medio para cometer un delito o como fin u objeto del mismo"[19].

2.2. ¿Identidad típica del delito informático?

1. Un sector de la doctrina entiende que no es adecuado hablar de delitos informáticos, en tanto en cuanto no haya una tipificación de un delito informático en la legislación penal española[20], dado que, no existe delito si no hay una ley que lo cree.

Sin embargo, el Código Penal introduce el término <<delitos informáticos>> en el art. 127.1 bis letra c), entendiendo como tales los de los apartados 2 y 3 del art. 197 y los tipificados en el art. 264. Dicho sector entiende que se deduce de la regulación penal actual la no existencia de una tipificación formal del delito informático como tal, sino que se ha regulado de tal forma que, a las acciones y omisiones ya tipificadas y previstas, en su caso, se les ha añadido una modalidad que tipifica y castiga la misma acción u omisión, salvo que esta es llevada a cabo mediante el uso de las TICs.

[17] BARRIO ANDRÉS: cit. n. 2. p. 26.
[18] HERNÁNDEZ DÍAZ: cit. n. 6. p. 39.
[19] SAIN: *Internet, el cibercrimen y la investigación criminal de delitos informáticos,* p. 8.
[20] DAVARA FERNÁNDEZ DE MARCOS: cit. n. 3 pp. 20 ss.

Davara Fernández de Marcos[21] se muestran muy contundentes al expresar que tras la reforma de 2015 del Código Penal Español no se introduce el delito informático, y de hecho no admiten tan siquiera que exista un delito informático como tal, aceptando dicha terminología por mera conveniencia, y para referirse a "determinadas acciones y omisiones dolosas o imprudentes, penadas por la ley, en las que ha tenido algún tipo de relación en su comisión, directa o indirecta, un bien o servicio informático. En nuestro Derecho no existe como tal el delito informático, porque, como hemos indicado, no está tipificado en el Código Penal, ni se encuentra en ningún otro sitio del ordenamiento que le pudiera encuadrar como legislación penal especial"[22].

2. Consideramos al respecto que, al igual que será prácticamente imposible delimitar lo que debemos entender por delito informático conceptuándolo, tampoco sería lo más idóneo propiciar una regulación específica de los delitos informáticos, como categorías penales nuevas, sino que, y como ya se ha realizado, a las omisiones y acciones existentes tipificadas añadirles su vertiente específica de dicha índole.

3. EL TIPO DEL ARTÍCULO 197 DEL CÓDIGO PENAL ESPAÑOL. ESPECIAL REFERENCIA AL OBJETO MATERIAL DEL DELITO:

1. El artículo 197 -acceso ilícito o no permitido a la intimidad- viene recogido en el T. X del Libro II (<<Delitos contra la intimidad, el derecho a la propia imagen y a la inviolabilidad del domicilio>>) del CP, concretamente dentro del Cap. I, dedicado al <<descubrimiento y revelación de secretos>>, protegiendo el derecho a la intimidad y a la propia imagen.

El presente precepto y, por ende, el capítulo donde se encuentra recogido, ha sido objeto de varias modificaciones, entre las cuales destacamos: la reforma de 1995 que "dotó a la tutela de la intimidad de una unidad y coherencia sistemática que antes no tenía"[23], la modificación por la LO 5/2010[24], de 22 de junio, con el objetivo de

[21] Elena y Laura Davara Fernández de Marcos, a modo de aclaración.
[22] DAVARA FERNÁNDEZ DE MARCOS: cit. n. 3. pp. 23 ss.
[23] ALONSO DE ESCAMILLA: *Tema 10. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio.* p. 217.

transponer lo dispuesto en la Decisión Marco 2005/222/JAI, de 24 de febrero, relativa a los ataques contra los sistemas de información, mediante la cual se introdujo un apartado tercero al art. 197 tipificando conductas de acceso sin autorización a datos o programas contenidos en sistemas informáticos; la LO 1/2015, de 30 de marzo, modificó nuevamente el Capítulo, reordenando las figuras delictivas existentes e introduciendo nuevas modalidades típicas de atentados contra la intimidad y la seguridad en los sistemas informáticos (art. 197.7, 197 bis 2 y 197 ter CP), cumpliendo con lo dispuesto en la Directiva 2013/40/UE, del Parlamento Europeo y del Consejo, relativa a los ataques contra los sistemas de información.

2. Resalta a la vista que la redacción actual del presente artículo referida a los comportamientos de apoderamiento da respuesta a nociones ya superadas por la presente realidad social. Además, el art. 197.2 emplea términos como "modificar" o "alterar" que no son del todo armónicos con la terminología utilizada en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y como dice Romeo Casabona "se abusa de la configuración de tipos agravados en cadena, lo que conduce a penas muy elevadas y a un marco punitivo excesivamente amplio. Por otro lado, la continua aparición de nuevas formas de vulneración de la intimidad por medios tecnológicos genera dudas sobre la eficacia del instrumento penal, dado su permanente riesgo de obsolescencia en relación con este tipo de abusos."[25].

3. Una de estas nuevas formas de vulneración de la intimidad por medios tecnológicos es a través de la "nube", es por ello, por lo que pretendemos analizar si, de la redacción del actual precepto podemos entender la "nube" como objeto material del presente delito.

[24] NÚÑEZ CASTAÑO: *Lección XIV. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio.* p. 335, de la cual hemos extraído las modificaciones expresadas a continuación de la cita.
[25] ROMEO CASABONA: *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio,* p. 254.

3.1. Bien jurídico protegido:

1. Con la regulación de la presente figura delictiva se pretende proteger la intimidad personal o familiar y los datos reservados de personas físicas o jurídicas, para asegurar su confidencialidad y proteger su integridad. Entiende la doctrina que, "… el derecho a la intimidad que establece el art. 197 CP, protege el dominio de la información sobre hechos o circunstancias de la vida personal que, de ser expuestos a la opinión pública, podrían suponer una falta de consideración personal y social del sujeto en cuanto miembro de una comunidad social cohesionada"[26].

2. Sin embargo, ¿qué debemos entender por intimidad? Si acudimos al art. 12 de la Declaración Universal de Derechos Humanos[27] o al art. 18 de la Constitución Española[28], de su lectura podemos verificar que se refiere a ésta como un derecho inherente de la personalidad, de hecho la STC 231/1988, de 2 de diciembre, en su fj 3, refiriéndose al honor, la intimidad y la propia imagen, pero más específicamente a la intimidad, así lo afirma: "aparecen como derechos fundamentales estrictamente vinculados a la propia personalidad, derivados sin duda de la dignidad de la persona que reconoce el artículo 10 de la Constitución Española, y que implican la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario -según las pautas de nuestra cultura- para mantener una calidad mínima de la vida humana. Se muestran así estos derechos como personalísimos y ligados a la misma existencia del individuo".

Es decir, entenderemos por intimidad todas aquellas manifestaciones sobre la personalidad individual o familiar reservadas a su titular o sobre las cuáles, éste, ejerce algún tipo de control cuando intervienen terceros (particulares o poderes públicos).

---

[26] ALONSO DE ESCAMILLA: cit. n. 23. p. 218.

[27] Declaración Universal de Derechos Humanos, artículo 12: *"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques."*

[28] Constitución Española, artículo 18: *"1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito. 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."*

A su vez, debemos distinguir el concepto de privacidad y el de intimidad, "la privacidad es más amplia que la intimidad, <<pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo-, la privacidad constituye un conjunto más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas en tres sí, arrojan como precipitado un retrato de la personalidad del individuo que este tiene derecho a mantener reservado. Y si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 de la Constitución y por las leyes que los desarrollan, la privacidad puede resultar menoscaba por la utilización de las tecnologías informáticas de tan reciente desarrollo>>"[29].

Por lo tanto, el concepto de intimidad al que se refiere nuestro actual Código Penal parte de la regulación y definición que nos proporciona la Constitución Española, la jurisprudencia del Tribunal Constitucional y la doctrina.

3. Hogaño, existen voces doctrinales que creen conveniente la creación de una nueva categoría jurídico-penal que abarque las conductas delictivas informáticas que ya no solo lesionan bienes jurídicos tradicionales, sino que lesionan nuevos intereses que deben ser objeto del Derecho Penal. De esta forma se habla de la seguridad informática como bien jurídico colectivo a titular; la integridad, confidencialidad y disponibilidad de los datos y sistemas informáticos; y la <<intimidad informática>>[30], en la cual nos centraremos dado el objeto de estudio de este trabajo.

De lo anteriormente expuesto podemos observar las enormes dificultades que se nos presentan a la hora de conceptuar la intimidad como bien jurídico objeto de tutela penal, encontrándonos además con su relatividad como característica innegable que no ayuda a la hora de definirla[31].

[29] SOLA RECHE: *La protección penal de los datos personales genéticos en el derecho español*, p. 209.
[30] HERNÁNDEZ DÍAZ: cit. n. 6. pp. 44 ss.
[31] En este sentido, SOLA RECHE, Esteban: *La protección penal de la intimidad informática*, pp. 179 ss.

4. En 1991, Sola Reche, ya nos advertía que nuestro ordenamiento tenía pendiente una legislación que recogiese "la protección penal de intimidad frente a la utilización abusiva de la informática, que ya recogieron las legislaciones de otros países"[32]. Si bien es cierto, que actualmente existe una regulación que pretende proteger la intimidad frente a dichos abusos, lo que debemos plantearnos es si realmente, en la práctica, es efectiva y funcional.

El concepto o término <<intimidad informática>> se crea por parte de la doctrina a raíz de los múltiples medios que surgen como consecuencia de la aparición de la informática, para vulnerar la esfera íntima. Y es que, como ya dijo Pérez Luño: "La dimensión cuantitativa de las informaciones que pueden ser almacenadas y transmitidas es de tal magnitud que ha dado lugar a un auténtico cambio cualitativo, que obliga a considerar el problema de las relaciones entre intimidad e información bajo un nuevo prisma."[33].

En este punto conviene hacer alusión al <<Habeas data>>, "que comprende el derecho de la persona a estar informado de su inclusión en un banco de datos y de los datos que le afectan, así como el acceso a ellos; derecho a la supresión de determinados datos -datos sensibles- o a su cancelación (lo que implica también la fijación de una limitación temporal de la validez de los mismos); derecho a la rectificación de los datos erróneos; derecho a conocer el uso a que van a ser dedicados los datos personales; derecho a la confidencialidad; limitaciones tanto en la recogida como en la utilización de los datos; adopción por el banco de datos de medidas que garanticen el no acceso a los datos por parte de personas no autorizadas, a la vez que aseguren su no destrucción o modificación, etc."[34]

[32] SOLA RECHE: cit. n. 31. p. 186.
[33] PÉREZ LUÑO: *Nuevas Tecnologías, Sociedad y Derecho. El impacto socio-jurídico de las Nuevas Tecnologías de la información,* p. 87.
[34] SOLA RECHE: cit. n. 31. p. 187. Información que cita y extrae de CARLOS-MARÍA ROMEO CASABONA, *La Reforma Penal ante las nuevas tecnologías de la información en "Informática e Diritto",* septiembre-diciembre 1987, p. 126.

3.2. Tipos básicos alternativos del art. 197.1 del CP:

A continuación, analizaremos la estructura del art. 197 del CP, objeto de estudio. Comenzaremos por los distintos tipos básicos alternativos[35] que se establecen en el art. 197.1, por lo que, desde que se realice uno de ellos la conducta sería típica.

1. Como primer tipo básico, nos encontramos con el apoderamiento de secretos documentales[36] cuyos elementos del tipo objetivo son, en primer lugar, el objeto material[37] constituido por papeles (incluidas ilustraciones), cartas[38], mensajes de correo electrónico, cualesquiera otros documentos[39] o efectos personales[40].

En segundo lugar, la conducta típica consistirá en apoderarse de los objetos materiales anteriormente enumerados[41].

En tercer lugar, en cuanto a los sujetos, por un lado, tenemos al sujeto activo que, al tratarse de un delito común, podrá ser cualquier persona (física o jurídica), y, por otro lado, tenemos al sujeto pasivo que será el titular de los secretos, mensajes de correo electrónico, papeles, documentos o efectos personales que serán el objeto de apropiación.

---

[35] ROMEO CASABONA: cit. n. 25, p. 257.

[36] Artículo 197.1 inciso 1º del Código Penal Español: "El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales".

[37] Debemos entender como objeto material del delito, aquel sobre el cual recae la acción delictiva, diferenciándolo del bien jurídico protegido, que como sabemos se trata de aquel interés protegido por la ley penal.

[38] ROMEO CASABONA: cit. n. 25, p. 258: *"cartas (<<comunicaciones escritas, dirigidas a un destinatario concreto, determinado y existente, de carácter personal, con comunicación de ideas, sentimientos, propósitos y noticias>>)".*

[39] El art. 26 del Código Penal Español nos proporciona una definición de lo que debemos entender por documento, la cual citamos: *"A los efectos de este Código se considera documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica.".*

[40] ROMEO CASABONA: cit. n. 25, p. 258: *"Mucho más arduo resulta precisar qué debe entenderse por efectos personales, pues es una expresión anfibológica y puede ampliar de hecho el tipo en exceso; teniendo en cuenta el bien jurídico protegido, habrá que entender cualquier objeto personal que posea un contenido secreto o intimidad (posible concurso de delitos con el hurto, identificable por la intencionalidad que anime el sujeto).".* En este sentido, y a modo de ejemplo, la STS 6201/1997 de 20 de octubre de 1997 determinó que se podría considerar como tal el contenido de un paquete postal que excediese del volumen de una carta.

[41] Sobre esta cuestión regresaremos y la relacionaremos con el objeto material (epígrafe 4 del trabajo), con el objetivo de fundamentar nuestra postura al respecto.

En cuanto a los elementos del tipo subjetivo, el dolo debe abarcar todos los elementos objetivos del tipo, siendo además necesario que concurra un elemento subjetivo de lo injusto <<la finalidad de descubrir los secretos o vulnerar la intimidad de otro>>[42].

2. El segundo tipo básico es el referente a la interceptación de las telecomunicaciones[43], cuyo objeto material estará constituido por las telecomunicaciones de otro[44] y cuya acción típica consistirá en "Interferir o captar una telecomunicación ajena, tanto si se impide la llegada del mensaje o intercambio de mensajes a su destino (desviando la comunicación y privando de ella a los comunicantes) como no (la comunicación es intervenida y captada, pero no se priva de ella a los comunicantes, p. ej., intercambio instantáneo de mensajes por diversos procedimientos de chat); así como cualquiera otras comunicaciones reservadas llevadas a cabo a través de la red, por telefax y otros recursos similares."[45].

En lo referente a los sujetos nos remitimos a lo ya expuesto para el tipo básico del art. 197.1 inciso 1º del CP, al igual que para los elementos del tipo subjetivo.

---

[42] NÚÑEZ CASTAÑO: cit. n. 24, p. 339. Respecto de la consumación, ROMEO CASABONA: cit. n. 25, p. 259: *"2. No es preciso para la consumación del delito que se haya producido la efectiva vulneración del secreto o de la intimidad. Es por ello por lo general un delito mutilado de dos actos, quedando el segundo de ellos ya fuera del tipo (SAP Granada sec. 2 667/2012 de 30 de noviembre; es de resultado cortado para Rueda Martín pp. 50 s.)."*.

[43] Art. 197.1 inciso 2º del CP: *"intercepte sus telecomunicaciones"*. En lo referente a los sujetos (activo y pasivo) y al tipo subjetivo nos remitimos a lo ya explicado para el primer tipo básico alternativo. Otro aspecto que debemos tener en cuenta es que, si bien es cierto hemos seguido la estructura de los tres tipos básicos alternativos que presenta ROMEO CASABONA (cit. 25), haremos alusión a NÚÑEZ CASTAÑO (cit. 24), autora que engloba en el tipo que lleva por título *"Interceptación de las comunicaciones"*, las dos conductas que disemina ROMEO CASABONA en: *"Interceptación de las telecomunicaciones de otro"* y *"Utilización de artificio técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación"*, lo cual, a nuestro parecer, es más esclarecedor y facilita su estudio.

[44] NÚÑEZ CASTAÑO: cit. n. 24, p. 339: *"esto es, las comunicaciones personales que se realizan a distancia a través de medios tecnológicos (teléfono, fax comunicaciones por satélite, radio o medios informáticos, como chat, redes sociales, etc.)."*, en este sentido también, ROMEO CASABONA: cit. n. 25, p. 259: *"2. Las comunicaciones abarcadas por el tipo (objeto material) son muy variadas: orales, escritas o por signos; simultáneas o diferidas. Por consiguiente, acoge todo tipo de telecomunicaciones, por cable (teléfono fijo) o inalámbricas (terminal móvil, radio); éstas pueden realizarse por medio de ondas radioeléctricas o vía satélite utilizando cualquier receptor de comunicación (sobre esta amplitud de recursos ya la STC 34/1996, de 11 de marzo)."*.

[45] ROMEO CASABONA: cit. n. 25, p. 259.

3. Como tercer tipo básico, nos encontramos con la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación[46], cuyo objeto material estará formado por medios técnicos, excluyéndose por lo tanto los naturales (sentidos), para captar el sonido, imagen o señal de comunicación[47].

Por lo que respecta a la conducta típica, consistirá en la utilización de artificios o medios técnicos de escucha, grabación, reproducción etc., no siendo suficiente para su consumación únicamente su instalación, sino que será necesario que la imagen, sonido o señal se capte efectivamente[48].

En cuanto a los sujetos y tipo subjetivo nos remitimos a lo ya expuesto para el tipo básico del art. 197.1 inciso 1º del CP.

3.3. Datos reservados o de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos o en cualquier otro tipo de archivo o registro público o privado (art. 197.2):

Tal y como expone el art. 197.2 del CP, se castigará con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses al que: "sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier

[46] Art. 197.1 inciso 3º del CP.

[47] A modo de ejemplo, la SAP Granada sec. 2 667/2012, de 30 de noviembre, que versa sobre la grabación mediante un MP3 a la esposa manteniendo relaciones sexuales con otro hombre. En el mismo sentido la STS 872/2001, de 14 de mayo, sobre la instalación de mecanismos de grabación y escucha en el domicilio conyugal porque el esposo sospechaba que su esposa le era infiel. En ambos casos esos medios técnicos a los cuales hemos hecho alusión constituyen el objeto material del delito. En lo referente al objeto material de dicho tipo básico, RUEDA MARTÍN: *Protección penal de la intimidad e informática*, p. 46, ya nos advierte que, con el objetivo de prever lagunas de punibilidad, deberíamos conectar la referencia que realiza el CP al decir *"cualquier otra señal de comunicación*" con cualquiera que presente características tecnológicas comunes o similares conocidas o por descubrir.

[48] NÚÑEZ CASTAÑO: cit. n. 24, p. 340. Además, deberán de desarrollarse en lugares privados cerrados, dado que las captaciones en lugares privados abiertos o en lugares públicos quedan circunscritos al ámbito civil.

medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero".

A priori, dado que la redacción del precepto 197 es confusa e innecesariamente complicada, y, por ende, muy deficiente[49], quizás no nos demos cuenta de que estamos ante un tipo básico diferente de los tipos básicos alternativos del art. 197.1, pero que a su vez comparten la misma intensidad punitiva y estructura, en lo referente a los tipos agravados (a partir del art. 197.3 CP) y autónomos (art. 197.3 pfo. 2º y 197.7 pfo. 1º del CP).

3.3.1. Precisión del bien jurídico protegido y del objeto material del delito[50]:

1. Es cierto, que al iniciar el tercer epígrafe del presente trabajo hemos tratado el bien jurídico protegido, en líneas generales, del art. 197 del CP. No obstante, llegados a este tipo delictivo debemos realizar matizaciones al respecto.

Cuando el CP se refiere a las conductas de <<apoderarse, utilizar>> o <<acceder y utilizar>> está delimitando acciones típicas que entendemos suponen un atentado a la intimidad del sujeto pasivo, mientras que, cuando utiliza las acepciones <<modificar>> o <<alterar>> configurando otras conductas típicas, cuando éstas se realicen se atentará a un bien jurídico diferente, que se conoce por identidad informática, integridad de los datos o libertad informática[51].

2. El objeto material serán los datos reservados de carácter personal o familiar de otro, por lo tanto, es requisito indispensable que los datos pertenezcan a un sujeto pasivo que no puede coincidir con el activo.

Entenderemos por datos de carácter personal, tal y como establece el art. 3 a) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, "cualquier información concerniente a personas físicas identificadas o

[49] ROMEO CASABONA: cit. n. 25, p. 261.
[50] NÚÑEZ CASTAÑO: cit. n. 24, p. 340, denomina el presente tipo delictivo como "Apoderamiento de secretos informáticos" o ALONSO DE ESCAMILLA, Avelina: cit. n. 23, p. 221 los denomina "Los delitos cometidos a través de medios informáticos".
[51] ROMEO CASABONA: cit. n. 25, p. 260.

identificables", añadiendo que también pueden pertenecer al ámbito familiar. A pesar de que dicho precepto haga alusión a las personas físicas únicamente, tal y como entiende Romeo Casabona, la información podrá ser concerniente a cualquier persona física o jurídica, dado que como establece el art. 200 del CP, también se protegen los datos reservados de la última[52].

A su vez, esos datos personales también deberán ser reservados, y por reservados vamos a entender "de acceso limitado para terceros ajenos al fichero, aunque no sean íntimos en sentido estricto; significa que no están al alcance de terceras personas ajenas a su tratamiento autorizado."[53] Excluyéndose de este concepto aquellas fuentes a las cuales podamos acceder todos como público (art. 3.j de la LOPD) o no sea necesaria autorización o consentimiento del interesado para que podamos acceder y conocer los mismos.

Además, dichos datos deberán encontrarse contenidos en archivos o soportes físicos, electrónicos o telemáticos, siendo por lo tanto la particularidad, el hecho de que se encuentren contenidos en soportes informáticos[54].

En este sentido, también sería interesante tener en cuenta la definición que realiza el Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001, que España firmó el 23 de noviembre de 2001, manifestó su consentimiento el 03 de junio de 2010 ratificándolo y entró en vigor en España el 01 de octubre de 2010, sobre lo que se entiendo por sistema informático[55] y por datos informáticos[56].

---

[52] ROMEO CASABONA: cit. n. 25, p. 260, y para un mayor detalle pp. 279 ss, en las cuales explica como las personas jurídicas pueden ser sujetos pasivos de los tipos delictivos del art. 197 del CP, tras establecerlo de manera explícita el art. 200 del CP, aclarando que la protección de los datos reservados de las personas jurídicas fue una decisión político-criminal que se adoptó en 1995, en su opinión favorable, a pesar de que suscite problemas interpretativos.

[53] ROMEO CASABONA: cit. n. 25, pp. 260 ss.

[54] NÚÑEZ CASTAÑO: cit. n. 24, p. 340.

[55] *"A los efectos de este Convenio, un "sistema informático" es un dispositivo que consta de hardware y software cuya función es el tratamiento automatizado de datos digitales. Puede incluir facilidades de entrada (input), salida (output) y almacenamiento. Puede funcionar de forma independiente o estar conectado a una red con otros dispositivos similares."*.

[56] *"La definición de "datos informáticos" se basa en la definición de datos de la ISO. Esta definición contiene palabras "que se preste a tratamiento informático". Esto significa que los datos están en un formato tal que pueden ser procesados directamente por un sistema informático. Con el fin de aclarar que en el presente Convenio el término "datos" debe entenderse como datos en formato electrónico u*

3.3.2. Elementos del tipo objetivo y subjetivo:

1. Se desprende de la redacción del precepto que se abarcan distintas modalidades referentes a la conducta típica: acceso, alteración, apoderamiento, uso o modificación de los datos contenidos en los soportes informáticos.[57]

El art. 197.2 presenta una estructura de conductas alternativas[58], por lo tanto, la acción típica consistirá en realizar la acción sobre los datos de otra persona con intención de perjudicar a un tercero (donde interaccionan tres sujetos: el sujeto activo del hecho delictivo, el titular de los datos y el tercero perjudicado- distinto del anterior-) o sobre los datos de otra persona con el fin de perjudicar a esa misma persona (coindicen titular de los datos y perjudicado).

No obstante, Romeo Casabona habla de una tercera conducta, la acción ejercitada por el propio titular de los datos sobre los suyos propios con intención de perjudicar a un tercero[59], que entiende no es punible dado que la acción típica debe recaer sobre datos ajenos al sujeto activo del tipo.

2. Debemos de tener en cuenta que, el precepto está regulado y redactado de tal forma que toda gira en función de la posición subjetiva de los intervinientes, dado que, titular de los datos podrá serlo únicamente aquel cuyos datos se puedan ver afectados perjudicándole a él o a un tercero[60].

---

otro formato que se preste a tratamiento informático directamente, se introduce el concepto de "datos informáticos. Los datos que se procesan automáticamente pueden ser objeto de uno de los delitos definidos en el presente Convenio, así como el objeto de la solicitud de una de las medidas de investigación definidas en el presente Convenio.".

[57] A modo de ejemplo, véase la STS de 10 de enero de 2018, en la cual se estima el recurso parcialmente, dado que, en el caso concreto consideró que procedía rebajar en dos grados la pena al concurrir dos circunstancias atenuantes (entre ellas la obcecación), de especial intensidad. Se considera culpable y castiga a un profesional de la sanidad por acceder en más de cien ocasiones (demostrado mediante periciales) a los historiales clínicos del padre de sus nietos y la esposa de éste, con la finalidad de verificar el estado de salud y la evolución de sus adicciones y poder utilizarlo en el procedimiento de regulación de las relaciones paternofiliales de los niños.

[58] ROMEO CASABONA: "Del descubrimiento y revelación de secretos", p. 754.

[59] ROMEO CASABONA: cit. n. 58, p. 756: (p. ej., alterar los datos personales relativos a méritos profesionales, situándose así en una posición de ventaja en relación con otros profesionales potenciales competidores)

[60] ROMEO CASABONA: cit. n. 25, p. 261. En relación, véase art. 3 letra e) de la LOPD.

Respecto al sujeto pasivo, será aquél que es titular de los datos afectados por la conducta típica, por lo tanto, siempre se corresponderá con el titular del bien jurídico. Pudiendo coincidir el sujeto pasivo con el perjudicado o no. Se excluyen del sujeto pasivo los menores e incapaces, cuyos datos sean de protección especial (art. 197.5 CP). También debemos distinguir el titular de los datos del titular del fichero, que será el <<responsable del fichero>>, dado que así se establece en la ley.

Respecto del sujeto activo, podrá ser *intraneus*, es decir una persona inicialmente autorizada o legitimada para acceder al fichero, o *extraneus o extranei*, personas ajenas al fichero y por tanto no legitimadas inicialmente. [61] No obstante, quien estando autorizado a acceder al fichero y se excede de dicha autorización incurre en el tipo.

Además, tendremos que distinguir el acceso autorizado del no autorizado. El primero, el autor del hecho está legitimado para acceder al fichero, en cambio en el segundo será culpable quien no estando autorizado para acceder a los datos lo hace <<por cualquier medio>>, siendo suficiente con la captación intelectual de los datos, simple visionado, no siendo requisito indispensable la aprehensión física[62].

4. En relación con el tipo subjetivo será necesario el dolo en cualquiera de sus formas, siendo necesario además la concurrencia de un elemento subjetivo de lo injusto como es <<obrar en perjuicio de…>>, encontrándonos ante un delito de intención y de resultado cortado[63].

3.4.Tipos agravados:

Como ya anticipábamos, el legislador al redactar el precepto en cuestión, tras el art. 197.2, recoge tipos agravados encadenados que dificultan mucho más la comprensión del precepto y que, por supuesto, no ayudan a su esclarecimiento.

Por todo ello, tras haber leído y analizado distintas clasificaciones doctrinales, en cuanto a la estructura, nos hemos decantado por la establecida y utilizada por Romeo Casabona, citado a lo largo del trabajo. No obstante, no nos detendremos excesivamente

[61] ROMEO CASABONA: cit. n. 58, pp. 746 y ss.
[62] ROMEO CASABONA: cit. n. 25, pp. 262 y ss.
[63] RUEDA MARTÍN: cit. n. 47, p. 81.

en este punto por no ser el tema central del presente estudio, haciendo alusión a los aspectos que consideramos más esenciales de los mismos y que pueden tener relación con el problema a tratar en cuestión.

1. Por revelación de la información obtenida (Art. 197.3, pfo. 1º del CP[64]): Nos encontramos con una acción alternativa, lo cual supone que podrá el sujeto activo difundir, revelar o ceder a terceras personas los datos o hechos descubiertos o las imágenes captadas[65].

2. Por razón de la calidad o condición del sujeto activo (Art. 197.4 letra a) y art. 198 del CP), podemos dividirlo a su vez en:

-Cometidos por personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros (art. 197.4 letra b) del CP):

Del propio título podemos desprender que se trata de un delito especial impropio, dado que el sujeto activo debe de reunir una calidad, es decir, ser responsable o encargados de los ficheros etc.[66]

Dentro del presente agravante podemos distinguir tres posibilidades: La realización del tipo del art. 197.1, agravándose por lo dispuesto en el art. 197.4 letra a); la del tipo del art. 197.2, agravándose por lo dispuesto en el art. 197.4 letra b); o la del tipo delictivo super agravado del art. 197.4 último párrafo, consistente en difundir, ceder o revelar la información a la cual se ha podido acceder.

-Cometido por funcionario o autoridad (art. 198 CP):

Respecto a los elementos del tipo objetivo destacables, en primer lugar, haremos alusión al sujeto activo, el cual deberá reunir la condición de autoridad o funcionario

[64] *"Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores."*.
[65] Bastaría con transmitir los datos a una sola persona. Sin embargo, para un mayor detalle recomiendo la lectura de ALONSO DE ESCAMILLA: cit. n. 23. pp. 222 ss., en las cuales explica la diferencia entre cada una de las alternativas de acción y sus especialidades.
[66] Para determinar que debemos entender por responsable del fichero acudiremos al art. 3. d) de la LOPD: *"Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento."*. No obstante, no existe una coincidencia entre la LOPD y el CP, véase ROMEO CASABONA: cit. n. 25, pp. 264 ss.

(con lo que respecta a su definición nos remitimos al art. 24 del CP), encontrándonos ante un delito especial.

En cuanto a la acción típica, cierto es que el CP se remite al artículo anterior, pero tras la reforma del 2015, el art. 197 (al cual se refiere) ya no es en sentido estricto justo el anterior, sin embargo, no cabe duda de que hace referencia al 197, quedando la incertidumbre si también se refiere a los anteriores y, en su caso, a cuáles[67].

3. Por la especial vulnerabilidad del sujeto pasivo (Art. 197.5 -inciso final- del CP[68]):

Entenderemos por menor de edad el que lo sea de acuerdo con la actual legislación civil, es decir, inferior a 18 años, y persona con discapacidad necesitada de especial protección[69] será aquella que cumpla con lo establecido en el art. 25 pfo. 2 del CP, al cual nos remitimos.

4. Por razón de la calidad o vulnerabilidad de la información (Art. 197.5 y 197.4 b) del CP), podemos dividirlo a su vez en:

Datos sensibles que requieren de una especial protección (art. 197.5):

Se trata de datos referentes o que revelen la ideología, religión, creencias, salud, origen racial o vida sexual. Es decir, el hecho que dichos datos se conozcan o se utilicen por terceros puede suponer que el titular de éstos pase a encontrarse en una situación de mayor vulnerabilidad. Por ello, se consideran datos hipersensibles lo cual supone establecer unas garantías para reforzar su protección, como puede ser, por ejemplo,

[67] ROMEO CASABONA: cit. n. 25, p. 266, considera que al ser delitos heterogéneos debe despejarse dicha duda en favor del acusado, respetando la prohibición de la analogía *in malam partem* no aplicando la agravación en los demás delitos.

[68] *"Igualmente, cuando… la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior."*. ROMEO CASABONA: cit. n. 25, p. 266, estima que no siempre se justifica dicha agravación dado que la vulnerabilidad de ambos sujetos pasivos *".no presupone necesariamente un injusto mayor del hecho, que haya incidido en la comisión del delito".*

[69] Hasta la LO 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre del Código Penal, se utilizaba la denominación de <<incapaz>>.

prohibir el acceso a la información y su tratamiento en archivos automatizados sin que medie el consentimiento del afectado, entre otros[70].

Utilización de datos personales de la víctima (art. 197.4 letra b) del CP):

Será requisito necesario realizar alguno de los tipos del art. 197.1 o 2 del CP, agravándose la pena cuando se utilicen los datos obtenidos, por ejemplo, del apoderamiento de los secretos del sujeto pasivo[71].

5. Cometer el delito con fines lucrativos (Art. 197.6 del CP):

Realmente nos encontramos ante dos tipos delictivos agravados cuando la acción esté presidida por el ánimo de lucro[72], cuando los hechos se hayan realizado con fines lucrativos; y cuando, además de realizarse con fines lucrativos, afecten a datos "sensibles" del art. 197.5 del CP (tipo hiperagravado).

Tras haber analizado todos los tipos agravados, hemos de decir que el art. 197 también presenta tipos autónomos, los cuales no entraremos a detallar. Véase art. 197.3 pfo. 2º y 197.7 del CP.

4. LA "NUBE" COMO OBJETO MATERIAL DEL DELITO DEL ART. 197:

Llegados a este punto, y, tras haber realizado un análisis pormenorizado de los aspectos que hemos considerado más importantes y especialmente relevantes para dar una respuesta al problema que se nos plantea, debemos, en primer lugar, cuestionarnos ambas posibilidades (si entendemos la nube como objeto material, o si, por el contrario, entendemos que no puede ser objeto material del art. 197) y sus efectos. Finalizando con las conclusiones y propuesta.

1. La generalidad de los usuarios de este recurso si tuviesen que dar una definición sobre qué entienden por "cloud computing", la describirían como un espacio

[70] Para una mayor explicación recomiendo la lectura de ROMEO CASABONA: cit. n. 25, pp.266 ss.
[71] A modo de reflexión, en relación con los tipos del art. 197.1 del CP, ¿podrían todos los objetos materiales subsumirse y entenderlos como datos, inclusive los efectos personales?
[72] No será necesario para su consumación que se haya obtenido efectivamente un lucro (delito de resultado cortado), es decir, que como elementos del tipo subjetivo nos encontraremos con el dolo y el ánimo de lucro (bastando por tanto una finalidad lucrativa), ROMEO CASABONA: cit. n. 25, p. 268.

virtual en el que se pueden almacenar multitud de archivos, documentos, fotos, videos, datos etc. Cierto es, no obstante, es mucho más que eso.

El NIST[73] ha definido el fenómeno como: "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.".

Por lo tanto, aunque la "nube" sea algo más que un espacio donde almacenar información, datos etc., a efectos del presente trabajo, nos importa esta primera definición aproximativa.

2. Si entendemos que la "nube" puede ser objeto del tipo del art. 197.1 inciso 1º del CP, tendríamos que entenderla subsumida dentro de lo que el código determina como "cualesquiera otros documentos". Por tanto, al entenderla como objeto material, en concreto, como un documento, desde el momento que se acceda a la misma (independientemente de si finalmente dentro hay datos, información, etc., que contengan secretos con los que vulnerar la intimidad) sin el consentimiento o autorización debida, estaríamos cometiendo el tipo del art. 197.1 inciso 1º (dándose además todos los restantes elementos del tipo objetivo y subjetivo), porque entenderíamos que se estaría apoderando el sujeto activo del objeto material en cuestión, el cual contiene el secreto, con independencia, de que llegue a conocer la información dado que, recordemos, no es requisito para su consumación.

Podría darse entonces un intento de acceso, de tal forma que, si se demuestra el mismo, estaríamos ante una tentativa del tipo del art. 197.1 inciso 1º del CP.

A pesar del razonamiento anterior, si entendemos la "nube" como objeto material del delito del art. 197, dado que lo subsumimos en "cualesquiera otros documentos", es

[73] "Final Version of NIST Cloud Computing Definition Published", disponible en https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published.

decir, que la consideraríamos documento, no podemos olvidar que el CP, en su art. 26 nos proporciona una definición, a la cual ya hemos hecho referencia con anterioridad, pero que conviene traer a colación en este punto. Y es que, a efectos del CP: "se considera documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica", es decir, ¿realmente la "nube" es un soporte material? Porque si no la entendemos como tal no podríamos subsumirla en "cualesquiera otros documentos" por lo que, no la podríamos entender como objeto material del delito, dada la actual redacción del precepto.

Sin embargo, si vamos más allá y consideramos que el concepto de documento del CP no es afín a la realidad tecnológica que vivimos, no obstante defendemos la postura de que, si bien es cierto el *cloud computing*, a pesar de ser inherente- dado que se trata de un espacio virtual-, su acceso debe de realizarse desde un ordenador o dispositivo electrónico que como tal es un soporte material, la nube y el contenido de la misma se va a plasmar en dicho soporte, porque de lo contrario no podríamos siquiera acceder al mismo.

3. En cambio si no entendiésemos la "nube" como objeto material del delito del art. 197 del CP, sino que, por ejemplo, la viésemos como el medio para llegar a esos documentos, datos etc., susceptibles de apoderarse, surgirían los siguientes problemas a los cuáles habría que dar respuesta:

-El acceso no permitido o autorizado quedaría impune o ¿en qué tipo se podría subsumir dicha conducta? En tal caso, ¿el intento de acceso demostrado quedaría impune también?

-Al entender que la "nube" no es objeto material, con el acceso no estaríamos incurriendo en el tipo delictivo del art. 197.1 inciso 1º del CP, por lo que, si accedemos y leemos información, pero no nos apoderamos de ella, ¿estaríamos incurriendo en el tipo delictivo?

En este punto deberíamos hacer alusión a lo expuesto por Romeo Casabona: "El tipo objetivo comprende la acción típica de apoderarse de los objetos materiales que se

indican. Sin embargo, esta expresión se ha quedado angosta en la actualidad respecto a la materialidad de los objetos susceptibles de apoderamiento, por lo que su sentido se ha ido espiritualizando. Por ello suele aceptarse que también forma parte del tipo conocer el contenido del documento, efecto personal o mensaje de correo electrónico sin apoderase materialmente de su soporte."[74]. Es decir, si aceptamos dicha postura, realmente podríamos entender que, no es necesario apoderarse materialmente del documento, carta etc.[75], para entender consumado el tipo delictivo, sino que bastaría con, en ese supuesto, haber llegado a acceder a la información sin que sea necesaria dicha aprehensión del elemento material, pudiendo utilizarlo también como argumento a favor para considerar la "nube" como objeto material.

No habría problema si se accediese a la "nube" y se demostrase que se ha apoderado de documentos, etc., incurriendo en el tipo delictivo del art. 197.1 inciso 1º del CP.

5. CONCLUSIONES Y PROPUESTA:

Si bien es cierto que, de la redacción actual del precepto no parece quedar reflejada la "nube" como objeto material del delito, no basta para decir que no podríamos entenderla como tal.

Reconozco mayores razones para entenderla como objeto material del delito, dado que, como he expuesto anteriormente, no comprenderla como tal supondría dejar la posibilidad de que conductas que se realizan hoy en día queden impunes por no considerarlas ilícitas y, por ende, penadas por el CP.

Ahora resulta más que evidente que debemos de hacer una interpretación extensiva de lo dispuesto en el art. 197 y del concepto de documento del art. 26 del CP, para entenderla como tal. No obstante, dicha interpretación no puede ser duradera en el tiempo, quiero decir con esto que, no debe servir de pretexto o fundamento para no

[74] ROMEO CASABONA: cit. n. 25, p. 257 y RUEDA MARTÍN: cit. n. 47 pp. 42 ss.
[75] En este sentido, SOLA RECHE: cit. n. 29, p. 214: "Obsérvese que con el objetivo de salvaguardar la intimidad la incriminación se adelanta hasta castigar conductas que *aún* no suponen el *descubrimiento* de los secretos o la *vulneración* -en el sentido del precepto- de la esfera íntima: el delito se consuma sin necesidad de acceder, de llegar a conocer la información reservada o íntima… permanecen al margen del tipo penal las intromisiones no provocadas (accidentales)".

modificar el Código Penal de tal forma que quede predeterminada la "nube" como objeto material del delito. No teniendo, por tanto, que acudir a interpretaciones que muchas veces generan inseguridad jurídica repercutiendo negativamente en la ciudadanía que obtiene por parte de los tribunales soluciones contradictorias partiendo de una misma regulación.

A medida que iba investigando y realizando el presente trabajo he podido comprobar que la redacción y regulación actual del precepto en cuestión es ardua, complicada y da la sensación, en multitud de ocasiones, que han intentado partir de una excesiva casuística por el afán de prever todas las situaciones posibles- imposibilidad en la delincuencia informática más que lógica- logrando lo que precisamente parece que pretendían evitar, la posibilidad de la impunidad de conductas que deberían estar penadas.

Por todo ello, considero que debería ser reformada la actual regulación del precepto, no pretendiendo delimitar en exceso y minuciosamente el tipo delictivo, dado que, en la delincuencia informática o cibernética la realidad muta constantemente y a una velocidad que no puede ni va a alcanzar la regulación jamás. Reformas encadenadas, regulaciones complejas y enrevesadas intentando delimitar al máximo una realidad más lejos de la precisión que nunca, solamente va a propiciar una impunidad constante. Y es que, si ya es complejo determinar lo que entendemos por delito informático (incluso habiendo autores citados a lo largo del presente trabajo que consideran imposible hoy en día dicha labor), una regulación que tiene como base la especificidad no va a permitir los objetivos pretendidos. Es por ello que, la regulación en estos tipos delictivos debería de ser lo suficientemente genérica para poder abarcar las nuevas formas delictivas que puedan ir surgiendo a medida que avanzan los medios tecnológicos y las TICs que se utilizan cada vez con mayor frecuencia en la sociedad.

No obstante, considero que este aspecto el legislador debería de haberlo previsto, dado que, como ya hemos hecho alusión, el recurso del *cloud computing* data de 2011 según las fuentes consultadas, y la última reforma del Título X del Libro II del CP donde se encuentra recogido el art. 197 (objeto también de reforma) se realizó en 2015.

6. BIBLIOGRAFÍA

ALONSO DE ESCAMILLA, Avelina (2018), "Tema 10. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio" en LAMARCA PÉREZ (coord.), Dykinson, S.L., Madrid.

BARRIO ANDRÉS, Moisés (2017), "Ciberdelitos: Amenazas criminales del ciberespacio", Reus, Madrid.

CAMACHO LOSA, Luis (1987), "El delito informático", Góndor, Madrid.

DAVARA FERNÁNDEZ DE MARCOS, Elena y Laura (2017), "Delitos informáticos" en DAVARA RODRÍGUEZ (coord.), Aranzadi, Navarra.

DAVARA RODRÍGUEZ, Miguel Ángel (1993), "Derecho informático", Aranzadi, Madrid.

DAVARA RODRÍGUEZ, Miguel Ángel (2017), "Delitos informáticos", Aranzadi, Navarra.

DE LA CUESTA ARZAMENDI, José Luis y DE LA MATA BARRANCO, Norberto J. (2010), "Derecho Penal Informático", Thomson Reuters, Navarra.

DÍEZ RIPOLLÉS, José L. y ROMEO CASABONA, Carlos María (2004), "Comentarios al código penal. Parte especial II. Títulos VII-XII y faltas correspondientes", Tirant lo Blanch, Valencia.

GÓMEZ RIVERO, M.ª del Carmen (2018), "Nociones fundamentales de derecho penal. Parte especial", Tecnos, Madrid.

GONZÁLEZ RUS, Juan José (2007), "Precisiones conceptuales y político-criminales sobre la intervención penal en Internet", *en Cuadernos penales José María Lidón*, 4, 2007.

GUZMÁN, Carlos A./FERNANDA FERREYRO, María (2017), "Delitos informáticos. Investigación criminal, marco legal y peritaje", B de F Montevideo-Buenos Aires, Buenos Aires.

HERNÁNDEZ DÍAZ, Leyre (2010), "Aproximación a un concepto de derecho penal informático" en DE LA CUESTA ARZAMENDI (director)/DE LA MATA BARRANCO (coord.), Thomson Reuters, Navarra.

LAMARCA PÉREZ, Carmen (2018), "DELITOS. La parte especial del Derecho penal", Dykinson, S.L., Madrid.

MARTÍNEZ MARTÍNEZ, Ricard (2012), "Derecho y cloud computing", en MARTÍNEZ MARTÍNEZ (editor) Aranzadi, Navarra.

MARTÍNEZ MARTÍNEZ, Ricard (2012), "Derecho y cloud computing", Aranzadi, Navarra.

NÚÑEZ CASTAÑO, Elena (2018), "Lección XIV. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en GÓMEZ RIVERO (directora), Tecnos, Madrid.

PÉREZ LUÑO, Antonio-Enrique (1987), "Nuevas Tecnologías, Sociedad y Derecho. El impacto socio-jurídico de las Nuevas Tecnologías de la información", Fundesco, Madrid.

ROMEO CASABONA, Carlos María (1988), "Poder informático y seguridad jurídica. La función tutelar del Derecho Penal ante las nuevas tecnologías de la información", Fundesco, Madrid.

ROMEO CASABONA, Carlos María (2001), "Genética y derecho penal. Previsiones en el código penal español de 1995", Comares, Granada.

ROMEO CASABONA, Carlos María (2004), "Del descubrimiento y revelación de secretos", en DÍEZ/ROMEO (coords.), Tirant lo Blanch, Valencia.

ROMEO CASABONA, Carlos María/ SOLA RECHE, Esteban/ BOLDOVA PASAMAR, Miguel Ángel (2016): "Derecho penal. Parte especial. Conforme a las leyes orgánicas 1 y 2/2015, de 30 de marzo", Comares, Granada.

ROMEO CASABONA, Carlos María (2016): "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en ROMEO/SOLA/BOLDOVA (coords.), Comares, Granada.

RUEDA MARTÍN, Mª Ángeles (2004): "Protección penal de la intimidad e informática", Atelier, Barcelona.

SAIN, Gustavo (2017): "Internet, el cibercrimen y la investigación criminal de delitos informáticos", en GUZMÁN/FERNANDA FERREYRO (directores), B de F Montevideo-Buenos Aires, Buenos Aires.

SOLA RECHE, Esteban (1991): "La protección penal de la intimidad informática", en Anales de la Facultad de Derecho de la Universidad de La Laguna, Nº 11, Canarias Futura, Tenerife.

SOLA RECHE, Esteban (2001): "La protección penal de los datos personales genéticos en el derecho español", en ROMEO CASABONA (ed.), Comares, Granada.

7. TABLA DE JURISPRUDENCIA CITADA:

Tribunal, Sala y Fecha	**Referencia**	**Magistrado Ponente**
STC, 02.12.1988	231/1988	Gloria Begué Cantón
STS, Sala de lo Penal,1, 20.10.1997	6201/1997	Eduardo Moner Muñoz
STS, Sala de lo Penal, 14.05.2001	3910/2001	Diego Antonio Ramos Gancedo
STS, Sala de lo Penal, 10.01.2018	15/2018	Andrés Palomo del Arco