LA PROTECCIÓN PENAL DE LOS MENSAJES DE CORREO ELECTRÓNICO Y DE OTRAS COMUNICACIONES DE CARÁCTER PERSONAL A TRAVÉS DE INTERNET[*]

CARLOS MARÍA ROMEO CASABONA
Catedrático de Derecho Penal
Universidad del País Vasco

PALABRAS CLAVE: Ciberdelincuencia • Protección de las comunicaciones • Derecho Penal e internet

KEY WORDS: Cybercrime • Protection of communications • Penal Law and Internet

[*] Véase más extensamente sobre la materia objeto de este estudio así como en relación con los delitos de descubrimiento y revelación de secretos, en los que se enmarca este estudio, Romeo Casabona, *ComCP II*, Tirant lo Blanch, Valencia, 2004, 591 y ss.

1. LA NECESIDAD DE LA PROTECCIÓN JURÍDICO-PENAL DE LAS COMUNICACIONES A TRAVÉS DE LAS REDES TELEMÁTICAS**

La circulación de información por las redes telemáticas (internet) se ha convertido en un creciente y útil vehículo de comunicación interpersonal, de creación, difusión y acceso a la información.

Al mismo tiempo, el uso de este todavía nuevo procedimiento de comunicación electrónica o telemática comporta la generación de nuevas formas de vulnerabilidad de la intimidad y de los datos de carácter personal en torno a la red, en particular en relación con el anonimato o confidencialidad con que deben estar presididas estas actividades en respecto a terceros ajenos a la comunicación[1], con la integridad de la información producida y con el acceso no consentido a las terminales privadas desde donde los ciudadanos se introducen en la red. Téngase en cuenta, además, que cada acto de recepción o remisión de comunicación o de acceso a sitios de la red deja su huella o traza digital, la cual es susceptible de seguimiento e identificación.

En ocasión anterior he apuntado[2] cómo los bienes jurídicos implicados en las comunicaciones personales a través de las redes telemáticas dignos de protección jurídico-penal no se agotan en la intimidad y los datos personales. Esta consideración me ha llevado a pronunciarme también acerca de la oportunidad político-criminal de proteger penalmente de forma integrada y autónoma el pacifico uso y disfrute de tales redes en las relaciones privadas (sin entrar en su consideración para otro tipo de relaciones) o, dicho de otro modo, la *comunicación pacífica a través de redes telemáticas*, con independencia de las garantías y protección que correspondan a otras formas de manifestación de la intimidad y de los datos de carácter personal.

En efecto, con este nuevo perfil —en cualquier caso, no completamente desconocido para el ordenamiento jurídico español, según se expondrá más adelante—, se quiere llamar la atención sobre la necesidad de ofrecer una protección jurídica más intensa —pero no exclusiva o principalmente penal— a las comunicaciones personales en cuanto tales, así como a las actividades de producción y de consumo de información en las redes, con independencia de que se generen datos personales o no. Posiblemente habría que diseñar la vertebración de cuándo tal protección debería ser asumida por el Derecho Penal y cuándo por otros sectores del ordenamiento jurídico, cuestión sobre la que volveré más adelante.

** Abreviaturas más frecuentes: AAP: Auto de Audiencia Provincial. ADPCP: Anuario de Derecho Penal y Ciencias Penales. AP: Actualidad Penal. CP: Código Penal. CP TR73: Código Penal, Texto Refundido de 1973. D: Decreto. DS: Derecho y Salud. F.j.: fundamento jurídico. JD: Jueces para la Democracia. LGT: Ley General de Telecomunicaciones. LL: La Ley. LO: Ley Orgánica. LOPD: Ley Orgánica sobre protección de datos de carácter personal. O: Orden. PJ: Poder Judicial. PLOCP: Proyecto de Ley Orgánica del Código Penal. RAE: Real Academia Española. RD: Real Decreto. RP: Revista Penal. SAP: Sentencia de Audiencia Provincial. STC: Sentencia del Tribunal Constitucional. STS: Sentencia del Tribunal Supremo. TSJ: Tribunal Superior de Justicia.

[1] Apunta también hacia este nuevo peligro, por cierto, no exento de tensiones con otros intereses de los poderes públicos en relación con la seguridad (así, desde la perspectiva norteamericana), Morales Prats (2002), 71 y s. Véase también, Morón Lerma, 114 y ss.

[2] Romeo Casabona (2001), 209.

Ha de señalarse al menos como objeto de reflexión que habrá que reconsiderar en un futuro próximo la conveniencia de introducir algún delito específico contra ciertos actos de acceso ilegítimo a ficheros o registros ajenos, así como el acceso ilegítimo o interceptación de las comunicaciones telemáticas ajenas, cualquiera que sea el propósito del autor. Es cierto también que en la actualidad esta comunicación pacífica se ve entorpecida cada vez con mayor frecuencia —en ocasiones con efectos muy graves, llegando a alcanzar al propio sistema y a sus archivos—, por la introducción de rutinas —los llamados virus informáticos— precisamente con ocasión y por medio de las comunicaciones telemáticas (p. ej., el correo electrónico), aunque en gran medida estos hechos podrían estar cubiertos por los delitos de daños, bien que se haya demostrado su inoperatividad frente a estos hechos por otros motivos no relacionados con el principio de legalidad (así, las dificultades en la identificación de los autores y la persecución policial, determinación de la competencia jurisdiccional y de la ley penal aplicable, funcionamiento de la entreayuda judicial, etc.).

Antes de adoptar la decisión político-legislativa oportuna habrá que ser consciente de los inconvenientes que puede presentar una solución de esta naturaleza en relación con la difuminación del bien o bienes jurídicos implicados y la lejanía de la referencia de éstos si se configura el nuevo delito como de simple actividad (de peligro abstracto —o de peligrosidad— o de peligro abstracto-concreto —o de acción peligrosa—). La elaboración de un bien jurídico como el que se ha propuesto podría contribuir a paliar parte de estos obstáculos. Además, otro aspecto sobre el que debería reflexionarse antes de tomar una decisión de política legislativa sería la valoración de la posible concurrencia de determinados elementos subjetivos, que podrían dar lugar a un diferenciado desvalor —entre sí— de lo injusto, con su correspondiente repercusión agravatoria del marco punitivo (p. ej., la intención de vulnerar la intimidad de las personas, o secretos industriales o financieros, o relativos a la seguridad del Estado, etc.)[3].

Será necesario asimismo reflexionar sobre si en estos casos el recurso a la tipificación penal estará o no justificado en virtud de los principios de *ultima ratio* y de intervención mínima del Derecho Penal (sobre todo en relación con los accesos ilegítimos sin el propósito de producir ningún daño determinado). En efecto, tampoco aquí debería abusarse del recurso a los instrumentos punitivos, dado que a través de normas extrapenales podrían satisfacerse —al menos en buena medida— las necesidades de tutela jurídica. Si el Derecho Penal está llamado a intervenir, no es menos cierto que de forma paralela habrán de adoptarse otros bloques de medidas y regulaciones jurídicas en el ámbito del Derecho Internacional y del Derecho Procesal o revisar, en su caso, la eficiencia de las ya existentes —tareas que probablemente revisten todavía mayor complejidad—, como garantía para conseguir una *optima ratio* a la intervención de aquél. De lo contrario, es seguro que estará condenado al fracaso.

En cualquier caso, estas reflexiones político-criminales sobre los nuevos escenarios para la intimidad, los datos personales y las telecomunicaciones a través de la red se acrecenta-

[3] Téngase en cuenta que delitos muy próximos a los mencionados en el texto figuran en el Convenio sobre el Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001 (p. ej., el acceso ilegal, art. 2º, y la interceptación ilegal, art. 3º).

rán probablemente a corto plazo, tanto como consecuencia de la presión doctrinal en torno a estos delitos[4] como por los compromisos que se deriven del Derecho Internacional para los poderes públicos españoles.

2. LA PROTECCIÓN PENAL DE LAS COMUNICACIONES A TRAVÉS DE LA RED, EN PARTICULAR DE LOS MENSAJES DE CORREO ELECTRÓNICO

Al consistir los mensajes de correo electrónico y otras telecomunicaciones realizadas a través de las redes telemáticas en una forma de comunicación privada debe reconocérseles en principio el mismo tratamiento jurídico que el ordenamiento reconoce a ésta[5]. Es oportuno mencionar, en primer lugar, la protección constitucional que se garantiza al secreto de las comunicaciones, salvo resolución judicial, en el art. 18.3 CE, y que la misma naturaleza jurídico-constitucional que a las postales, telegráficas y telefónicas que menciona a modo de ejemplo hay que reconocer a cualquier otra forma de comunicación a través de la red, como el acceso a páginas y sitios de la misma, la obtención a través de ella de documentos, datos, imágenes, sonidos, conversaciones escritas u orales instantáneas (chat), etc.

Valga recordar la doctrina del TC sobre el alcance constitucional de la protección de las comunicaciones en general, que abarca tanto al proceso y al soporte de la comunicación como a su contenido mismo: "Rectamente entendido, el derecho fundamental consagra la libertad de las comunicaciones, implícitamente, y, de modo expreso, su secreto, estableciendo en este último sentido la interdicción de la interceptación o del conocimiento antijurídicos de las comunicaciones ajenas. El bien constitucionalmente protegido es así, —a través de la imposición a todos del "secreto"— la libertad de las comunicaciones, siendo cierto que el derecho puede conculcarse tanto por la interceptación en sentido estricto (que suponga aprehensión física del soporte del mensaje —con conocimiento o no del mismo— o captación, de otra forma, del proceso de comunicación) como por el simple conocimiento antijurídico de lo comunicado (apertura de la correspondencia ajena guardada por su destinatario, por ejemplo)"[6].

Con posterioridad el TC ha realizado también una aproximación a la cuestión que nos ocupa en la línea sugerida más arriba, al entender que el referido precepto constitucional ha de extenderse asimismo a las nuevas tecnologías: "Ciertamente los avances tecnológicos que en los últimos tiempos se han producido en el ámbito de las telecomunicaciones, especialmente en conexión con el uso de la informática, hacen necesario un nuevo entendimiento del concepto de comunicación y del objeto de protección del derecho fundamental, que extienda la protección a esos nuevos ámbitos, como se deriva necesariamente del tenor literal del art. 18.3 CE"[7].

[4] V. posiciones doctrinales diferentes sobre esta cuestión: Mata y Martín, 28 y ss.; Morón Lerma, 77 y ss.; Rovira del Canto, Delincuencia informática y fraudes informáticos, Comares, Granada, 2002, 39 y ss. (si bien centrado en el ámbito patrimonial de los delitos informáticos).

[5] Así lo entiende también Morales Prats (2002), 76.

[6] SsTC 114/1984 y 34/1996.

[7] STC 70/2002.

La Ley General de Telecomunicaciones establece por su parte la protección no penal del secreto de las telecomunicaciones y de los datos personales en el sector[8].

En el art. 197[9] del CP encontramos varias modalidades típicas básicas, una de las cuales gira en torno al apoderamiento de papeles y cartas, en línea muy semejante a su predecesor, aunque incluyendo ahora otros objetos materiales novedosos, tributarios de las nuevas tecnologías de la comunicación, como lo es el correo electrónico, o que simplemente pretenden cumplir una función de escoba o de recogida en relación con los objetos anteriores[10]. Como ya he adelantado, se incluye asimismo la interceptación de las telecomunicaciones de otro, aparte de varios procedimientos técnicos de captación del sonido o de la imagen o de cualquier otra señal de comunicación (expresión confusa por lo que atañe a su naturaleza y contenido, pero que en todo caso pretende asumir de nuevo una función de recogida o de escoba respecto a las innovaciones tecnológicas que puedan surgir en el futuro) (art. 197.1). Finalmente, se incorporan como delito diversas conductas relacionadas con los datos reservados de carácter personal y 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), las cuales presentan en su conjunto la estructura de un tipo básico paralelo pero autónomo, en relación con un bien jurídico en gran medida diferente[11].

Respecto a la naturaleza jurídico-penal de este delito puede calificarse como *de acción peligrosa* (es decir, de peligro abstracto-concreto)[12], pues es preciso que la acción sea en si misma peligrosa para el bien jurídico (de conformidad con el art. 16 CP), es decir, para la intimidad de otra persona. Significa esto que no es necesario que se haya producido la lesión del bien jurídico ni que haya corrido un efectivo peligro (delito de peligro o de peligro concreto). Por consiguiente, es evidente que el tipo básico no es de resultado material[13].

[8] Ley 32/2003, de 3 de noviembre, Capítulo III (arts. 33 y ss.).

[9] Dice así el art. 197.1 del CP: "1. 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 o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses."

[10] De este parecer, en relación con la expresión "cualesquiera otros documentos o efectos especiales", Mata Martín, 127.

[11] Sobre el bien jurídico protegido en este delito y sobre su estructura típica me he ocupado previamente con mayor detenimiento en Romeo Casabona (2001), 288 y ss.; el mismo (2002), 513 y ss.

[12] Como compatibles con la estructura de los delitos de peligro abstracto se pronuncia *Sola Reche* (2001), 214, en nota 40, quien llega a esta conclusión tras la no obstante acertada reflexión de que "no se prevén como delito, o como agravación, las concretas conductas de averiguación de la información pretendida". Sobre la denominación de delitos de peligrosidad, de acción peligrosa y delitos de peligro, que se refieren en el texto, v. Romeo Casabona, "Aportaciones del principio de precaución al Derecho Penal", en *Modernas tendencias en la Ciencia del Derecho penal y en la Criminología*, UNED, Madrid, 2001, 91 y s.

[13] De forma similar, Rodríguez Ramos, *PE II*, 30 lo califica como delito de mera actividad: Sin embargo, Polaino Navarrete, *PE I*, 398, considera este delito como de resultado material, encontrando éste en "la efectiva traslación posesoria de los respectivos documentos a la esfera del autor". Orts Berenguer/Torres Roig, 20, entienden que es necesaria la causación de una ofensa al derecho a la intimidad, "como precisa el legislador al exigir el elemento subjetivo". Lo cierto es que el resultado, para que fuera material, habría que orientarlo a la

3. EL OBJETO MATERIAL DEL DELITO

El objeto material de este delito es múltiple y variado. Todos estos objetos se caracterizan por consistir en soportes físicos con capacidad para recoger, incorporar o reproducir hechos, datos, manifestaciones de voluntad, etc. que constituyan un secreto para alguien y afecten a su intimidad o que sin ser secreto involucren a dicha intimidad; esto es, esos soportes han de incorporar aspectos que afecten a la intimidad de otra persona[14]. Están integrados, en primer lugar, por papeles y cartas, que eran los únicos soportes que señalaba el CP anterior. Además, por mensajes de correo electrónico, documentos y efectos personales. Lógicamente, en este estudio sólo voy a referirme a los mensajes de correo electrónico, mientras que los demás objetos materiales mencionados por la ley únicamente presentan interés en la medida en que son susceptibles de acoger a su vez otros objetos que son fruto de una comunicación telemática personal. Nótese que cualquier mensaje o comunicación telemática que ha sido recogida en un soporte material fuera del sistema informático o telemático constituye ya en cuanto tal un objeto material diferente como papel o carta u otro documento[15] o, en su caso, efecto personal.

El CP no proporciona una definición de mensaje de correo electrónico. Sin embargo, el Derecho comunitario ha incluido una propia, que seguramente será incorporada al Derecho interno una vez que el legislador español haya procedido a la oportuna transposición de la disposición jurídica correspondiente: "Todo mensaje de texto, voz, sonido o imagen enviado a través de una red de comunicaciones pública que pueda almacenarse en la red o en el equipo terminal del receptor hasta que pueda accederse al mismo"[16]. Puede aceptarse la anterior definición a título orientativo, por ejemplo es valiosa la referencia a la modalidad del mensaje, entendido como texto, voz, sonido o imagen, así como la exigencia de la posibilidad de almacenamiento temporal (en la red o en el equipo terminal del receptor) hasta que pueda accederse al mismo. Sin embargo, si atendemos a los propósitos específicos del Derecho Penal, dirigidos a la protección de un determinado bien jurídico, la definición comunitaria que, no debe olvidarse, está subordinada a los propósitos sectoriales en los que se enmarca, puede ser parcialmente inadecuada. En efecto, en cuanto tal definición es al mismo tiempo demasiado restrictiva y demasiado amplia. Lo primero lo encontramos en la limitación a mensajes cursados a través de redes de comunicación públicas y, sin embargo, no debe excluirse la intervención jurídico-penal allí donde existen comunicaciones que deben ser salvaguardadas del alcance ajeno, con independencia del carácter público o pri-

efectiva afectación del bien jurídico protegido y ello no tiene que producirse necesariamente en ninguna de las hipótesis que manejan las dos argumentaciones acabadas de mencionar.

[14] Así, Orts Berenguer/Roig Torres, 20.

[15] Lo que se ve facilitado por la amplia definición de documento que aporta el propio CP: "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" (art. 26).

[16] Art. 2, h de la Directiva 2002/58/CE, sobre privacidad y comunicaciones electrónicas. Esta Directiva ha sido traspuesta parcialmente por la LGT.

vado que tenga la red[17]. Por otro lado, al Derecho Penal sólo interesan las comunicaciones electrónicas que sean personales.

Por consiguiente, y a los solos efectos penales, por mensaje de correo electrónico puede entenderse una modalidad de comunicación, por lo general de carácter personal, que incorpora texto, voz, sonido o imagen y que se sirve de las redes telemáticas como tecnología de transmisión y de los sistemas informáticos (ordenadores y el *software* o sistema lógico correspondiente) como instrumentos de remisión y de recepción entre dos o más comunicantes y, en su caso, de almacenamiento de los mensajes. Conforme a lo indicado más arriba, a los efectos del presente estudio es necesario que la comunicación sea de carácter personal (por tanto, estarían excluidos los mensajes publicitarios o comerciales no individuales o personalizados). En estos casos, la determinación del soporte como objeto material del apoderamiento puede ser más complicada, mientras sólo exista una mera visualización. Estas circunstancias obligarán a un análisis sumamente cuidadoso de la acción típica cuando recae sobre un mensaje de estas características.

Puesto que en el CP vigente —con mayor claridad todavía que en el CP73— las comunicaciones que son abarcadas por el tipo ya no pueden ser entendidas únicamente como las orales[18], hay que concluir en que acoge, por consiguiente, todo tipo de comunicaciones[19], sean orales, escritas, mediante imagen o el sonido u otros signos o la combinación de varios de cualesquiera de ellos. Pero, en segundo lugar, se limita a las comunicaciones a distancia que se valen por ello de procedimientos técnicos de comunicación[20], como telemáticos y otros por cable o inalámbricos[21], bien se realicen estos últimos por medio de ondas radioeléctricas o vía satélite con cualquier receptor de comunicación, p. ej., una radio o un teléfono celular o terminal móvil[22].

La información obtenida ha de tener un contenido de intimidad[23], pero no es necesario que sea en todo caso secreta. El mantenimiento en el tipo del término "secretos" ha sido

[17] De todos modos, la Directiva citada no es ajena a los dos aspectos que se comentan en el texto y viene a coincidir con las preocupaciones allí aludidas, puesto que, por un lado, remite a la Directiva 95/46/CE para la protección de las comunicaciones a través de redes privadas (EM párr. 10), y, por otro lado, señala explícitamente que la Directiva se aplicará al tratamiento de datos personales en relación con las comunicaciones electrónicas (art. 3.1).

[18] Pues, aunque confiriera una cobertura penal residual, el art. 497 bis del CP 73 acogía también las comunicaciones no orales, siempre que se realizaran a través de la línea telefónica o por otro medio que pudiera calificarse como tal. Véase en este sentido, Romeo Casabona (1988), 29 y s.

[19] De acuerdo con la Directiva 2002/58/CE, por comunicación puede entenderse "cualquier información intercambiada o conducida entre un número finito de interesados por medio de un servicio de comunicaciones electrónicas disponibles para el público".

[20] A este sentido genérico aluden Jorge Barreiro, *ComCP*, 567; Muñoz Conde, *PE*, 247; Queralt Jiménez, *PE*, 194.

[21] Véase la SAP Zaragoza de 23 de octubre de 2001, sobre un caso de interceptación y grabación de conversaciones inalámbricas

[22] Véase la STC 34/1996, de 11 de marzo; SAP Almería de 27 de julio de 1992. En la doctrina, Jorge Barreiro, *ComCP*, 567; Morales Prats, *ComCP*, 432.

[23] La mera divulgación de la dirección de correo electrónico de tercero no se adecua a la tipicidad del art. 197.2, según la SAP Madrid 15 de febrero de 2002, ni tampoco forma parte de del cuerpo de un mensaje, podríamos añadir, pero no deja de ser una dato de carácter personal.

objeto de crítica por algún sector doctrinal[24], y con razón, al no ser el secreto en cuanto tal objeto de tutela penal por este delito, pues no presenta en realidad autonomía alguna respecto a la intimidad, que es el bien jurídico protegido. Se tacha la permanencia de este término como fuente de distorsiones interpretativas —dado el sentido polisémico del mismo, que puede aludir a secretos de diversa naturaleza y alcance: secretos industriales o de empresa, de Estado, etc.—, en particular por constituir uno de los dos ejes de la parte subjetiva del tipo. En todo caso, al aludir a los "secretos de otro", es indudable que abarca exclusivamente los secretos de carácter personal[25], lo que viene reforzado por la rúbrica que encabeza el Título en el que se inserta este delito. Esta observación no contradice la garantía que merece el secreto de las comunicaciones.

4. LA ADECUACIÓN TÍPICA DE LAS DIVERSAS MODALIDADES COMISIVAS

El CP de 1995 introdujo de forma expresa como delito el apoderamiento de los mensajes de correo electrónico, así como la interceptación de las telecomunicaciones de otra persona. Sin perjuicio de las precisiones que se introducirán más abajo, puede adelantarse ya que en el primer caso se trata de conductas que pueden afectar al mensaje de correo electrónico o a cualquier otra comunicación a través de la red asimilable que se encuentra en una situación estática, esto es, guardados en un fichero una vez recibido, pendiente de recepción y guardado en el sistema del prestador de servicios o guardado en el terminal de remitente cuando se halla pendiente de remisión. Mientras que las segundas —las telecomunicaciones— se refieren a conductas que afectan a cualquier mensaje u otra forma de comunicación telemática semejante mientras se encuentran en el proceso de transmisión (y, en ocasiones, de creación), es decir, en "movimiento". Sin perjuicio de que comporten situaciones diferentes, en todas ellas puede accederse a la comunicación privando a su destinatarios o a alguno de ellos de su contenido o sin privar del mismo.

Las acciones de privación del mensaje o de cualquier otra comunicación a través de la red mediante su obstrucción, alteración o destrucción estarían más próximas en todo caso a los delitos de daños que a la finalidad que anima al tipo de descubrir los secretos o vulnerar la intimidad de otro, que difícilmente puede verse afectada por meros actos obstructivos o impeditivos de la comunicación entre terceras personas. De todos modos, en su caso, podría verse afectada la integridad de los datos de carácter personal, y puesto que éstos constituyen un bien jurídico autónomo, podría dar lugar a la aplicación del delito establecido en el art. 197.2 del CP, donde se protegen estos datos frente a su alteración o modificación no autorizada en perjuicio de terceros, además de frente a su acceso o utilización también no autorizados.

[24] Morales Prats, *ComCP*, 324.
[25] Así también, Morales Prats, *ComCP*, 424.

4.1. El apoderamiento de mensajes de correo electrónico

La primera acción típica en la que vamos a detener nuestra atención está constituida por el apoderamiento de mensajes de correo electrónico y de otras formas de telecomunicación. Para tal propósito habrá que abordar el alcance que tiene la acción de apoderarse en el conjunto del tipo en el que se inserta.

La acción típica viene expresada en el art. 197.1 del CP como *apoderarse* de los objetos que se enumeran en el tipo, entre ellos los mensajes de correo electrónico. Esta expresión proviene del CP73 (art. 497) y continúa presentando en la actualidad semejantes y al mismo tiempo nuevos problemas interpretativos y mereciendo por ello las mismas críticas que entonces, como tendremos ocasión de comprobar a continuación. En efecto, tradicionalmente el término ha dado lugar a varias interpretaciones posibles sobre su significado, algunas de las cuales son compatibles entre si; pero no quiere decirse con ello que este criterio haya encontrado aceptación generalizada, pues en realidad la mayor parte de los autores conciben algunas de tales interpretaciones como excluyentes. En todo caso, es indudable que este término ha experimentado un proceso de idealización o espiritualización que no puede desconocerse (en algún caso, incluso no puede prescindirse de esa depuración, pues, como se verá, es una exigencia taxativa del tipo), por lo que uno de los problemas más importantes radica en decidir hasta qué grado es admisible tal espiritualización sin que suponga un desvío no permitido del principio de legalidad de los delitos (analogía *in malam partem*).

La primera acepción, que gira en torno a su expresión literal, consiste en entender que el acto de apoderamiento comporta el desplazamiento o *traslación física de la cosa* —del soporte en el que se encuentra la información o el hecho secreto o íntimo— por parte del sujeto activo del delito a su propio ámbito de dominio o de control, en sentido similar, en consecuencia, al que suele interpretarse esta misma expresión en los delitos contra el patrimonio de apoderamiento (el hurto, en el que se utiliza la palabra "tomar", pero en especial el robo, con el que coincide la de "apoderarse"). Sin embargo, sin perjuicio de que parece razonable aceptar que no puede desconocerse el parentesco que guardan en su forma de comisión ambos grupos de delitos, precisamente por utilizar el mismo vocablo para definir la acción típica, no debe olvidarse en ningún momento la diferente orientación de cada uno de ellos en relación con el bien jurídico que están llamados a proteger los respectivos delitos. En consecuencia, esa traslación física en el delito de descubrimiento y revelación de secretos habrá que entenderla como suficiente —típica— desde el momento en que capacita al sujeto activo para acceder —no que acceda efectivamente— al contenido del objeto material trasladado a su control. La acción típica quedaría plenamente realizada con el mero hecho material descrito, sin que sea precisa la captación o aprehensión intelectual del contenido del soporte de la información o circunstancia íntima (que, ciertamente, puede llegar a producirse). Esta interpretación es casi unánime en la doctrina[26] y debe aceptarse como una interpretación válida.

[26] Así, p. ej., Carbonell Mateu/González Cussac, *PE*, 286; Higuera Guimerá (2002), 774; Jorge Barreiro, *ComCP*, 566 y s.; Lozano Miralles, PE, 210; Mata y Martín, 127 y s.; Morales Prats, *ComCP*, 427; Muñoz Conde,

Otro significado es fruto del criterio jurisprudencial, ya antiguo, del que se hacen eco algunos autores, conforme al cual el apoderamiento también puede verse encarnado en la retención de lo recibido por error (en concreto, una carta postal remitida por error a un destinatario equivocado por parte del servicio de correos). En el tema que nos ocupa aquí consistiría, por ejemplo, en la recepción de un mensaje de correo electrónico enviado por el remitente a persona distinta del destinatario al que se quería dirigir en realidad (p. ej., al copiar del listado de direcciones incorrecta pero inadvertidamente la dirección de otra persona) y su subsiguiente apertura por el receptor[27]. La jurisprudencia ha matizado, respecto a los supuestos de cartas remitidas a un destinatario equivocado por correo postal, que no basta con la simple inactividad o pasividad respecto a la retención, pues en coherencia con el sentido de la palabra apoderamiento es necesaria una acción positiva por parte de quien recibe la cosa para que ésta quede bajo su dominio[28]. Desde luego, debe aceptarse que la apertura y subsiguiente aprehensión de su contenido ha podido ser accidental como consecuencia de un error inicial ajeno, con mayor motivo si se trata de un mensaje telemático, en el que el autor del error será normalmente el propio remitente. En tales situaciones (tanto de comunicaciones telemáticas como postales) es aceptable la exclusión del dolo en relación con lo realizado, según se verá más abajo, y considerar consecuentemente atípico el hecho. Sin embargo, cabría preguntarse si el tipo quedaría constituido si el receptor accidental procede a la copia del mensaje con el fin de vulnerar la intimidad de tercero (p. ej., para divulgarlo), una vez descubierto el error, dado el sentido que asigno más abajo a la acción de copiar.

Como efecto de estos argumentos y de las propias características semánticas de la acción típica, podemos extraer dos conclusiones: una, que ya no es necesario en todos los casos que el acto de traslación haya sido realizado por el sujeto activo o por un tercero que obre con dolo (ni en relación con esto último tampoco se trataría de un instrumento no doloso, dado que la acción inicial relativa al envío erróneo no ha sido generada o provocada por el presunto sujeto activo)[29], basta con un acto de dominio —eso sí, positivo— sobre el soporte, una vez que éste ha llegado a su esfera de acción. Asimismo, está excluida la comisión de estos hechos por omisión. Ambas conclusiones han de ser igualmente asumidas.

El siguiente paso en este proceso de espiritualización del acto de apoderarse se construye a partir de la aceptación de que a la conducta de apoderamiento hay que asimilar,

PE, 251; Polaino Navarrete, *PE*, 398; Serrano Gómez, *PE*, 251; Sola Reche (2001), 214. Sin embargo, mantienen un criterio contrario, que comentamos más abajo, Anarte Borrallo, 54; Queralt Jiménez, *PE*, 194.

[27] La doctrina y la jurisprudencia se han ocupado tan sólo del caso de la apertura de una carta tras su remisión indebida por parte del servicio postal (u otro privado semejante) y es al que aplican la solución que se menciona en el texto: Anarte Borrallo, 54; Bajo Fernández/Díaz Maroto, PE, 161; Carbonell Mateu/González Cussac, *PE*, 286; Lozano Miralles, *PE*, 210; Muñoz Conde, *PE*, 251, y SsTS de 6 de octubre de 1967, 25 de noviembre de 1969 y 8 de marzo de 1974.

[28] SsTS de 6 de octubre de 1967 y 25 de noviembre de 1969.

[29] La SAP Madrid 11 de mayo de 2001, considera que no constituye divulgación ni dolo de divulgación el hecho de presentar a juicio de separación las cartas de correo electrónico obtenidas por un envío anónimo.

según los casos, el hecho de copiar (mensaje de correo o de fax electrónicos)[30], fotocopiar o fotografiar el soporte material (papel, documento o efecto personal)[31] en el que se encuentra la información secreta o íntima, o incluso únicamente el contenido del soporte y no éste (piénsese, p. ej., en el mensaje de correo electrónico que es impreso en papel o copiado en un disquete, disco compacto u otro soporte informático), si por ese medio aquélla —la información— se hace accesible. Ésta es una exigencia derivada de una interpretación teleológica a partir del bien jurídico protegido y del hecho de que el acto de apoderamiento es instrumental (medio idóneo para poder acceder a una información, etc., íntima, pero no para su mera apropiación material), de acuerdo con la interpretación primera que de este término acabamos de ver, y lo que ha de permitir es el acceso al contenido del soporte que se pretende descubrir, pero no el soporte en cuanto tal, que por lo general será irrelevante para la intimidad del sujeto pasivo.

Una ulterior acepción de la acción típica —ciertamente, ya con un alto grado de espiritualización— incluiría el conocimiento del contenido del documento o efecto personal sin que esté precedido o acompañado por el apoderamiento material de dicho soporte. Ahora bien, incluso en este caso cabe contemplar varias hipótesis diferentes. La primera de ellas se refiere a cuando el sujeto activo necesita realizar un acto previo que le permita la visualización del contenido

Así, extraer de un sobre abierto la carta o documento para volverlos a depositar en su sitio una vez leídos; o meramente levantar un papel u otro objeto que impide la visión de otro que se encuentra tapado debajo; o encender el terminal del ordenador, acceder a la carpeta donde figuran los mensajes ya leídos —o no— por su destinatario y visualizarlos a continuación. Esta nueva propuesta de comprensión del tipo comporta, una vez más, una ampliación del concepto de apoderamiento a un conjunto de supuestos en los que el sujeto ha de realizar una acción tendente a remover, aunque sea de forma temporal y en todo caso no irreversible, cualquier obstáculo —por insignificante que sea éste— que impida la visualización del contenido que incorpora el soporte. A este respecto es significativo el acto de colocar un obstáculo, por muy leve que sea éste, por parte del sujeto pasivo al eventual acceso visual de terceros (apagar la pantalla del terminal, cerrar la puerta del despacho, etc.), pues constituye un reflejo *objetivo* de la voluntad de aquél de guardar o proteger el secreto o de mantenerlo fuera del alcance de otros, por lo que de acuerdo con esta interpretación cualquier acto encaminado a levantar o remover ese impedimento se adecuaría a las exigencias del tipo.

La otra hipótesis o paso quedaría integrado cuando el sujeto accede directamente a la visualización del contenido, sin necesidad de eliminar o remover impedimento alguno, ni

[30] Sin embargo, traslada estos supuestos al último inciso "o de cualquier otra señal de comunicación" (sobre esta expresión típica véase más abajo), Muñoz Conde, *PE*, 254. En mi opinión es innecesario acudir a esta modalidad típica, pues el fax electrónico y cualquier otro medio similar de comunicación presentan idénticas características y condicionamientos técnicos que los mensajes de correo electrónico, aparte de la definición que hemos propuesto para éste último, radicando su única diferencia en el formato de presentación al usuario.

[31] En este sentido, la STS de 14 de septiembre de 2000: "para que concurra el apoderamiento exigido basta su aprehensión virtual, esto es, que el sujeto activo del delito se haga con su contenido de cualquier forma técnica que permita su reproducción posterior, como por ejemplo, mediante su fotografiado".

tan siquiera de tocar físicamente el objeto, ni, por supuesto, de desplazamiento ilegítimo. Por ejemplo, leyendo el documento de un tercero situado a la vista sobre la mesa de éste mismo, o un texto —un mensaje de correo electrónico que haya sido impreso previamente— o imagen visualizables sobre la pantalla de un terminal de ordenador.

Para que sea admisible la conclusión de la adecuación típica de esta diferente dimensión de la referida expresión de apoderarse es preciso reconocer a la misma un significado o alcance todavía más espiritualizado que en los supuestos mencionados con anterioridad, pues supone un notable alejamiento de la interpretación que resulta más evidente, como traslación física del soporte del secreto o información íntima (p. ej., un papel o carta) desde el círculo de su propietario al autor del hecho, quedando desposeído aquél de dichos objetos; supone entender la acción típica, además —pero no siempre—, como la pura y simple aprehensión intelectual del contenido que aquéllos incorporan, así como los comportamientos intermedios. Por consiguiente, el último criterio interpretativo apuntado resulta ya discutible desde el punto de vista de su adecuación típica, pues es dudoso que se pueda forzar tanto el proceso de "desmaterialización" —espiritualización— del tipo, pues éste exige en todo caso —probablemente con dudoso acierto— un comportamiento material vinculado con los soportes que menciona[32]. En cualquier caso, es revelador señalar que la doctrina se encuentra muy dividida sobre este particular[33].

Incluso en sentido estricto, pero siempre desde la perspectiva interpretativa propuesta, la mera captación intelectual del contenido tampoco sería necesaria para sostener la tipicidad, pues el sujeto activo podría retener en su memoria el texto visualizado sin llegar a comprender su significado (p. ej., por hallarse escrito en un idioma desconocido para aquél, o consistir en signos —p. ej., matemáticos, criptográficos— únicamente comprensibles por un experto).

Sin perjuicio de las consideraciones hermenéuticas presentadas hasta el momento en este trabajo, en las que ya se ha podido comprobar las singularidades de especial relieve de las que son tributarios los mensajes de correo electrónico, y se han ofrecido respecto a ellos algunas propuestas específicas, el apoderamiento de los mismos requiere todavía un examen detallado[34]. Para algunos autores el hecho típico está caracterizado por el acto de apoderarse del correo electrónico de otro, por ejemplo, del mensaje una vez impreso sobre papel o soporte similar[35]. Cierto que no presenta la menor duda la adecuación típica de tal conducta, pero en realidad quedaría ya plenamente cubierta a través de los demás objetos

[32] En una línea argumental similar, Orts Berenguer/Roig Torres, 26, estiman que es necesario que el autor realice una acción física dirigida a obtener los datos secretos.

[33] Por el criterio afirmativo se decantan Jorge Barreiro, *ComCP*, 566 y s.; Morales Prats, *ComCP*, 427; Polaino Navarrete, *PE*, 398. En sentido contrario, exigen el apoderamiento material o físico del objeto, pues de lo contrario no concurriría el tipo objetivo, Higuera Guimerá (2002), 774, 776 y s.; Muñoz Conde, *PE*, 251. Como puede apreciarse, en el texto defiendo una postura diferente a las anteriores y tal vez intermedia (y semejante a la de Orts Berenguer/Roig Torres, véase nota anterior): es necesario remover un obstáculo para acceder a la información –sin verdadera traslación física del objeto-, pero no es suficiente con la mera visualización de aquélla.

[34] En Romeo Casabona (2001), 298 y ss., se mantenían ya las posiciones que se incluyen aquí, respecto a las cuales se han reforzado ahora las líneas argumentales sostenidas entonces.

[35] Así, Morales Prats, *ComCP*, 427.

materiales que han sido estudiados más arriba, dado que a ese mensaje impreso no se le puede negar la condición de 'papel', 'carta' o 'documento', o de los tres objetos al mismo tiempo. Sin embargo, no me parece suficiente, pues esto no es lo específico y diferencial del mensaje de correo electrónico, y en consecuencia no puede ser el motivo que impulsara al legislador a incluirlo expresamente en la ley. El legislador supuestamente debió pretender cubrir alguna posible laguna de la descripción típica del CP anterior, y ya se ha visto cómo no sería éste el caso si lo limitamos al supuesto acabado de mencionar sugerido por un sector doctrinal, pues sin la menor duda sería ya típico incluso con la deficiente redacción del CP derogado. Algo semejante podría decirse de los telefaxes y teletextos, así como de los mensajes de voz, sonido, texto o imagen intercambiados por medio de terminales móviles. Por consiguiente, es preciso buscar otras propuestas más acordes con el verdadero sentido de la ley.

a) Acceder al mensaje que se visualiza directamente sobre la pantalla de un terminal, sin realizar ningún tipo de maniobra: en coherencia con lo apuntado anteriormente sobre otros documentos informáticos diferentes al mensaje de correo electrónico, debe excluirse tal conducta del ámbito de la tipicidad de este delito[36].

b) Abrir una carpeta no destinada en principio a estos mensajes: el hecho inicial, de ser accidental, sería también atípico, pero de aprovechar tal circunstancia persistiendo en la captación de la información, sería típica, por concurrir ya en este supuesto el dolo. De no ser accidental el acceso, se trataría de un supuesto asimilable al que se estudia a continuación.

c) Acceder al buzón —informático— de un tercero, en el que se encuentran almacenados todos los correos electrónicos recibidos por un mismo destinatario (p. ej., abrir e introducirse en la llamada "bandeja de entrada" del programa de correo electrónico), captando así el autor el contenido de los mensajes, pero sin desposeer de ellos a su titular: configura un supuesto similar a los mencionados más arriba como subsumibles en el tipo, en los que se remueve un obstáculo con el fin de poder acceder a los mensajes ya recibidos y archivados sin que se produzca un desplazamiento físico ilegítimo de los mismos.

En esta última hipótesis y en la señalada en segundo lugar podría operarse tanto desde el equipo terminal del sujeto pasivo, como desde el terminal del sujeto activo o de un tercero, pudiendo incluso trasladar una copia a otro terminal, aspecto este que sería irrelevante para la configuración de este tipo. En todo caso, el acceso al equipo terminal del sujeto pasivo introduciendo para ello la clave que da entrada a dicho equipo, habiendo sido obtenida por cualquier medio sin el consentimiento de aquél o con dicho consentimiento pero más allá de los límites de autorización, es un procedimiento concluyente de haber vencido el obstáculo que previene cualquier acceso no deseado, como lo es también el desbloqueo de dicha clave.

Ahora bien, en mi opinión la literalidad del art. 197.2 impone admitir que en la tercera de las hipótesis planteadas se produciría al mismo tiempo el apoderamiento de datos reservados personales en ficheros o soportes informáticos y otros, a los que se refiere este precepto. Estaríamos ante un concurso de leyes, cuya resolución es irrelevante, al llevar consi-

[36] De opinión contraria, Morales Prats, *ComCP*, 427*; Jorge Barreiro*, *ComCP*, 567 (siguiendo al autor anterior).

go la misma pena (pero, con todo en este caso seria ley especial el art. 197.1, al referirse específicamente al correo electrónico, frente a otros ficheros mas genéricos que menciona el art. 197.2).

Para poder llegar a las sucesivas conclusiones y propuestas interpretativas que se han ido exponiendo respecto a la palabra apoderarse, algunas de las cuales me parecen razonables y defendibles, es preciso recordar las siguientes puntualizaciones con propósitos de recapitulación: a) la palabra apoderamiento guarda una estrecha proximidad semántica con aquellos delitos contra el patrimonio en los que se recurre a dicho término para describir la acción típica, pero que al ir orientados a finalidades diferentes (a la protección de bienes jurídicos diversos), su coincidencia no es total: en los delitos de descubrimiento de secretos no comporta necesariamente un desplazamiento o traslación física del objeto material ni tiene por qué tener efectos posesorios o intelectivos[37]; b) debe reconocerse que entender compatible con la palabra apoderarse las conductas de retener un documento (carta), primero, y de copiar el contenido del soporte, después, supone el inicio de un proceso de espiritualización de dicho término; c) en la misma dirección se inscriben los supuestos de remoción de obstáculos para acceder a la información; d) el propio CP de 1995 ha dado un paso más allá hacia la espiritualización del término estudiado cuando incorpora explícitamente como objeto material los mensajes de correo electrónico. En efecto, la inclusión de este objeto material en el delito aporta un argumento intrasistemático adicional, en el sentido de que si abre razonablemente las puertas a una comprensión más dinámica de la palabra apoderarse, tal interpretación no debe estar cerrada a los demás objetos materiales incluidos en el tipo, si por su propia naturaleza admiten y requieren al mismo tiempo una interpretación de este tenor.

Cualquier otro comportamiento que no incluya algún acto de desplazamiento o de acceso a lo inicialmente oculto se sitúa al margen de este delito.

En conclusión, no constituye una interpretación analógica en perjuicio del reo, contraria a las estrictas exigencias del principio de legalidad, entender que la palabra apoderamiento admite la traslación física o material del soporte, la reproducción de éste junto con el contenido que incorpora, la reproducción únicamente del contenido sobre un soporte diferente o, incluso, la captación directa de su contenido, siempre que haya un comportamiento previo que facilite el acceso al objeto material. Cualquiera de las variantes analizadas integra la acción típica que estamos estudiando. De todos modos, esta conclusión no impide insistir en el desacierto de mantener la expresión legal comentada —apoderarse—, puesto que ofrece un rendimiento muy trabajoso para lograr cubrir la variedad de aspectos —nuevos y no tan nuevos— mediante de los cuales puede presentarse la acción en la vida real.

A la vista de las reflexiones y propuestas anteriores se comprenderá lo excesivamente rígida y angosta —y por ello rechazable— que resulta la hipótesis, defendida minoritariamente por la doctrina[38], de que el tipo exige no sólo apoderarse del objeto o soporte que

[37] Véase, sin embargo, Polaino Navarrete, *PE*, 298, quien califica el apoderamiento como una "traslación posesoria cognitiva".

[38] Sostenida por Anarte Borrallo, 52; Queralt Jiménez, *PE*, 194.

contiene la información secreta, sino además que llegue a conocerse también su contenido. Esta interpretación cuenta con un soporte legal todavía menos claro que del que pudiera disponer alguna de las anteriores propuestas interpretativas y, desde luego, no se compadece con la evolución inherente a este tipo en atención en parte, precisamente, a los nuevos objetos materiales que incorpora.

4.2. La interceptación de las telecomunicaciones de otro a través de la red

La segunda variante típica está constituida por la interceptación de las telecomunicaciones de otro. Puesto que sobre el significado del objeto material (las telecomunicaciones) ya me he ocupado más arriba, queda ahora centrarnos en el alcance dela acción típica: interceptar.

La palabra *interceptar* es polisémica. En primer lugar, y según lo expuesto, puede entenderse como "apoderase de una cosa antes de que llegue al lugar o a la persona a la que se destina" (según la RAE). Asimismo, como obstruir una vía de comunicación. Finalmente, acceder a la comunicación de otros sin obstruir o interrumpir esa comunicación. En resumen, interceptar desde un punto de vista lingüístico puede consistir en desviar, obstruir o acceder, en este caso a una telecomunicación, pero en atención a la estructura compleja que presenta el art. 197.1 y al bien jurídico protegido, procede realizar varias precisiones.

En efecto, la primera acepción debe ser descartada de todo punto en este lugar, puesto que de lo contrario no permitiría establecer ninguna forma de distinción con el primer inciso del art. 197.1 del CP, ya estudiado, al menos por lo que se refiere a la acción típica. A semejante conclusión debe llegarse por lo que respecta al sentido obstructivo de la palabra, puesto que ya quedó apuntada más arriba su desvinculación con la protección de la intimidad y de la confidencialidad de las comunicaciones.

Nos queda, por consiguiente, como significado más conforme con la naturaleza del delito el de acceder a la comunicación de otros sin interferir en su prosecución. En consecuencia, satisfaría los requerimientos de este segundo inciso ('interceptar' como equivalente a intromisión) y no del primero ('apoderarse'), en virtud de lo ya argumentado, si el sujeto activo logra acceder a un mensaje de correo electrónico durante el proceso de su transmisión, mientras está circulando por la red, captando su contenido sin desviarlo de su destino. Sería aplicable entonces este segundo inciso del art. 197.1 del CP. Ahora bien, si el sujeto activo lograra reenviar una copia a su propia terminal, podría incluirse en ambos incisos del art. 197.1 indistintamente, dado que hemos admitido como adecuadas típicamente al primero de ellos las acciones de copiar un documento sin privar al mismo tiempo de él a su propietario o tenedor[39].

Es indiferente asimismo que se utilicen medios técnicos aptos para la interceptación de la comunicación o comunicaciones sucesivas de una o de varias personas entre si o de un

[39] Este supuesto de copia o grabación lo entiende subsumible únicamente en el segundo inciso Morales Prats, *ComCP*, 427.

conjunto de ellas inicialmente indiferenciado (p. ej., técnicas de barridos aleatorios de las comunicaciones)[40].

En conclusión, en relación con el objeto de interés de este estudio es típica conforme al inciso segundo del art. 197.1 del CP la acción de interceptar los mensajes de correo electrónico o cualquier otra forma de comunicación telemática sostenida a través de la red en el sentido de acceder a la comunicación realizada por terceros, siempre que esto se sustancie sin impedir la llegada del mensaje a su destino o el efectivo intercambio de mensajes.

4.3. LA DESVIACIÓN DE UNA TELECOMUNICACIÓN

La acción puede consistir, finalmente, en la desviación del mensaje a un tercer terminal (p. ej., desde el que opera el sujeto activo o a otro diferente) durante el período de transmisión desde el equipo terminal del remitente al del destinatario, siempre que se prive a éste de su recepción. Nos encontramos aquí con una conducta que participa de elementos de los dos tipos referidos en los apartados anteriores, puesto que se actúa en el proceso de la transmisión, pero se priva al mismo tiempo de su recepción al destinatario o destinatarios. Entiendo que será punible de acuerdo con el primer inciso del art. 197.1, en el sentido de apoderamiento que he propuesto más arriba, pues si el mensaje llegase a pesar de ello a su destino estaríamos ante el supuesto de interceptación de las comunicaciones de otro que menciona el segundo inciso del art. 197.1, como voy a tratar de demostrar a continuación.

En efecto, lo que aquí ocurre es que se intercepta un mensaje de correo electrónico, en el sentido de "apoderase de una cosa antes de que llegue al lugar o a la persona a la que se destina" que le otorga la RAE (dentro de las diversas acepciones que admite el vocablo "interceptar"), sin acceder necesariamente al contenido del mensaje. La acción se asemeja con cierta fidelidad —incluso etimológicamente— al efecto traslativo que adjudicamos inicialmente a la palabra apoderarse, pero con la significativa diferencia —tributaria de las propias características tecnológicas de las que se vale este correo virtual— de que no se produce el traslado material de ningún soporte, sino del contenido mismo del mensaje. Consecuentemente, la adecuada interpretación de "apoderarse de… mensajes de correo electrónico" no ha de limitarse al sentido material o físico de los supuestos analizados con anterioridad, incluso los entendidos más laxamente, porque el estado "natural" de estos mensajes que estamos analizando ahora —los mensajes de correo electrónico— es virtual, sin ningún soporte material que los contenga (a salvo del propio equipo terminal, si ya se encuentra en él, o del servidor, si está pendiente de recepción por el destinatario). Por otro lado, la posibilidad de acceder a un mensaje de correo electrónico desde diferentes puntos o terminales, y no sólo —ni de forma excluyente— desde el terminal habitual abunda a favor de esta propuesta interpretativa. A partir de aquí podría sostenerse el mismo criterio respecto a otros mensajes que se valen de instrumentos y procedimientos tecnológicos semejantes (p. ej., el telefax cuando se envía a un terminal informático).

Debe dejarse claro inmediatamente que, por consiguiente, la palabra interceptar según se está utilizando ahora no guarda relación semántica con la que se utiliza en el segundo

[40] Alude expresamente en sentido afirmativo a esta posibilidad, Muñoz Conde, *PE*, 253.

inciso del art. 197.1 ("interceptar las telecomunicaciones de otro"), y por ello no puede ser integrada en esa modalidad del tipo, sino en la de apoderamiento, pues como se indicó más arriba, en aquella estructura típica no se produce una traslación-privación del dominio de la comunicación, que es lo que ocurre en nuestro caso, sino una mera intromisión cognoscitiva en la comunicación de terceros[41].

En conclusión, la anterior interpretación sí parece responder más certeramente a las características propias de los mensajes virtuales y probablemente también a la preocupación del legislador por despejar cualquier duda sobre la incriminación de las conductas mencionadas, recurriendo por ello a la mención explícita de estos mensajes en la descripción de los objetos materiales sobre los que puede recaer la acción típica.

4.4. El apoderamiento de trazas de acceso a la red

Como es sabido tanto las comunicaciones a través de la red como el mero acceso a determinados sitios de la misma (páginas *web*), suele dejar huellas de los mismos (páginas visitadas, hora de acceso, etc.), como ocurre en el propio historial de la navegación efectuada por la red, así como con los llamados *cachés*, pues ambos quedan registrados en el equipo terminal. En particular, algunos sitios de la red introducen en el equipo terminal como condición previa a permitir el acceso al mismo un fichero (*cookie*) que suministra información sobre el propio usuario. Sin entrar ahora en el estudio de este procedimiento, que requeriría un abordaje específico, lo cierto es que accediendo a las *cookies*, como también a los demás rastros, se puede obtener también información sobre los accesos realizados por el usuario, lo que afecta sin duda a su vida privada[42]. ¿Cómo podría calificarse entonces si alguien accede al terminal de un tercero y se apodera o copia dichas *cookies* u otros rastros de las sucesivas navegaciones?

Lo cierto es que el objeto material a duras penas encaja en las previsiones actuales del CP, pues aunque podría aceptarse que el acto constituye un apoderamiento típico, no se trata de papel o carta, ni es un mensaje de coreo electrónico ni tampoco un efecto personal y es al menos discutible que constituya documento en el sentido del CP (art. 26). Por otro lado, el hecho no tiene por qué comportar la interceptación de una comunicación (aunque podría serlo), por lo que surgen en un primer plano dudas sobre la tipicidad del acceso o apoderamiento de estas informaciones.

La cuestión es si cabe considerar dichas informaciones como dato reservado de carácter personal, pues en ese caso al abarcar el art. 197.2 del CP como objeto material esos datos bastará con que estén registrados en soportes informáticos, electrónicos o telemáticos, que es lo que ocurre con la hipótesis que nos ocupa (esta información se halla en el equipo terminal u ordenador del usuario; también puede encontrarse parte de ella en el sistema del

[41] Sin embargo, Morales Prats, *ComCP*, 427 y 431, considera que este hecho queda abarcado en los supuestos de interceptación de las telecomunicaciones, esto es, el segundo inciso del art. 197.1. En mi opinión, según se defiende en el texto, éste es un caso evidente de apoderamiento en el primer sentido de traslación material, aunque lo sea por otros procedimientos, en todo caso virtuales; para la conducta típica de interceptación quedan otros supuestos diferentes al que propone este autor, de los que también me ocupo en el texto.

[42] En este sentido, Hernández Guerrero, 346 y ss.; Morales Prats (2002), 73 y ss.

proveedor de acceso a la red, como se verá más abajo). La LOPD define los datos de carácter personal como cualquier información concerniente a personas físicas identificadas o identificables (art. 3, a). Por consiguiente, a partir de una definición tan amplia (en este caso en relación con la expresión "cualquier información concerniente a"), y al no ser preciso que formen parte de un fichero en sentido estricto cuando se encuentran registrados en un soporte como el indicado, éste sería entonces el camino para sancionar penalmente el acceso a esta clase de información residual pero tan reveladora potencialmente de la intimidad del sujeto que ha generado esa información en su propio equipo terminal. Esta interpretación sería alternativa de persistir la duda sobre la existencia de documento, como se apuntaba más arriba, si bien no me parece que deba descartarse en todo caso, por lo que podría producirse un concurso de leyes en relación con el inciso primero del art. 197.1

4.5. REALIZACIÓN DEL HECHO SIN EL CONSENTIMIENTO DEL INTERESADO

En todas las variantes examinadas es necesario que el sujeto activo realice la acción correspondiente sin el consentimiento del sujeto pasivo. Por consiguiente, el consentimiento de cada uno de los participantes en la comunicación se configura como el eje sobre el que se vertebra el marco de licitud de aquélla en relación con terceras personas.

El consentimiento del interesado excluye, desde luego, la tipicidad del hecho, es decir, de las diversas conductas que han sido estudiadas más arriba[43]. En este delito el consentimiento opera como causa de exclusión del tipo y no de la antijuricidad, porque cuando se produce la mediación del mismo (previa o simultáneamente al hecho) no se sustancia ningún menoscabo fáctico del bien jurídico. Esto es así porque este delito pertenece al grupo en los que junto al bien jurídico en cuanto tal se protege la libre disposición del mismo por parte de su titular[44].

Cuando se trata de la comunicación simultánea entre dos o más personas y una de ellas revela a terceros ajenos a tal comunicación el contenido de la misma o procede a su grabación o registro mediante artificios técnicos o a copiar una imagen, de consistir en un procedimiento audiovisual de comunicación, no concurre el tipo, puesto que el interlocutor es cotitular de la información reservada y está legitimado para hacer uso de ella, salvo que a su vez tenga una obligación previa de secreto laboral o profesional, pero entonces se trataría de un tipo delictivo diferente (art. 199 CP). En este sentido, la jurisprudencia entiende que

[43] Las posiciones doctrinales sobre la naturaleza jurídica del consentimiento en este delito son divergentes. En el sentido del texto (excluye el tipo), Anarte Borrallo, 51; Carbonell Mateu/González Cussac, *PE*, 288; Higuera Guimerá (2002), 775; Jorge Barreiro, *ComCP*, 566; Serrano Gómez, *PE*, 256. Por el contrario, consideran que es causa de justificación Lozano Miralles, *PE*, 205; Muñoz Conde, *PE*, 254 (al menos, así lo plantea en relación con la interceptación de comunicaciones); Queralt Jiménez, *PE*, 197.

[44] Véase sobre ello ya Romeo Casabona, *El Médico y el Derecho Penal (Licitud y responsabilidad) I. La actividad curativa*, Bosch, Casa Ed., Barcelona, 1981, 325 y ss.; el mismo, "El consentimiento en las lesiones en el Proyecto de Código Penal de 198", en *CPC*, nº 17, 1982, 35 y ss. Se adhiere a ello en este delito, Higuera Guimerá (2002), 775.

no se produce la vulneración del art. 18.3 de la CE ni, por consiguiente, el tipo del art. 197.1 del CP[45].

Más clara me parece la respuesta al supuesto de captaciones del sonido o la imagen de otro u otros por una persona ajena a la comunicación, pero que cuenta para ello con el consentimiento de uno o varios de los interlocutores. En estos casos, tal consentimiento no excluye la tipicidad, puesto que el partícipe en la comunicación está involucrando a un tercero sin que tal circunstancia sea conocida por los demás, y pueda ser consentida implícitamente, como se deduce del hecho de que al iniciar una comunicación con varios interlocutores previamente identificados —aunque no necesariamente de forma nominal— se está aceptando implícitamente el acceso de todos ellos. Es decir, los participes captados no se encuentran en condiciones de poder asumir en esta situación el riesgo de un comportamiento desleal por parte de alguno de ellos[46].

4.6. El tipo subjetivo

El tipo subjetivo está comprendido, en primer lugar, por el dolo en cualquiera de sus variantes (directo de primer o segundo grado o eventual)[47], el cual implica la conciencia y voluntad de la realización de todos los elementos objetivos del tipo.

Además, es necesaria la concurrencia de un específico elemento subjetivo de lo injusto, como elemento típico común —al igual que el dolo— para las diversas modalidades típicas ya estudiadas en su vertiente objetiva, consistente en la intencionalidad de "[para] descubrir los secretos o vulnerar la intimidad de otro". Sobre el alcance de ambos componentes subjetivos, que se presentan como exigencia típica alternativa, por lo que se refiere a "descubrir", alude a la captación intelectual del contenido del soporte, a su conocimiento, pero en este caso tal captación ha de recaer sobre un secreto de carácter personal, esto es, sobre un hecho que su titular ha querido dejar fuera del alcance de los demás o tan sólo accesible a un número limitado de personas. En el segundo caso ha de concurrir la intención de vulnerar la intimidad de un tercero, aunque no afecte a un secreto ajeno, conclusión que abunda en la idea de lo superfluo de la referencia expresa al secreto y a su descubrimiento, pues bastaba con la segunda —vulnerar la intimidad de otro—, que se proyecta explícitamente sobre el bien jurídico protegido y en ella quedaría ya incluida la primera.[48]

Es por ello un delito de intención mutilado de dos actos, el primero de los cuales configura ciertamente la acción típica —apoderarse, interceptar, etc.—, pero quedando el segundo de ellos ya fuera del tipo (el efectivo descubrimiento del secreto o vulneración de la

[45] A este respecto señala la STC 114/1984, de 29 de noviembre: "El derecho al "secreto de las comunicaciones... salvo resolución judicial" no puede oponerse, sin quebrar su sentido constitucional, frente a quien tomó parte en la comunicación misma así protegida". Similar, la STS 8 de junio de 2001.

[46] De esta opinión Muñoz Conde, *PE*, 254, para quien el interlocutor podría ser coautor o –más plausiblemente- partícipe punible por estos hechos.

[47] Admite únicamente el dolo directo, sin aparente justificación, Morales Prats, *ComCP*, 428.

[48] Véanse planteamientos críticos semejantes en Morales Prats, *ComCP* 428; siguiéndole, Jorge Barreiro, *ComCP*, 569.

intimidad)[49], cuya comisión quedará en principio en manos del sujeto activo, sin perjuicio de que se pretenda que el descubrimiento lo realice un tercero al que se entrega el soporte correspondiente sin haber entrado en conocimiento de su contenido[50], lo que podrá dar lugar a su vez a un tipo delictivo distinto (art. 197.3 CP).

Si concurriese una finalidad distinta a las dos señaladas, no existirá este delito, sin perjuicio de que pueda dar lugar a la comisión de otro, siempre que a su vez concurran sus propios requisitos de tipicidad (p. ej., hurtos, daños)[51]. En conclusión, este elemento subjetivo —al igual que ocurre con otros delitos con una estructura típica semejante— puede producir un doble y tal vez antagónico efecto: adelantar la intervención del Derecho Penal, al no ser necesario que el sujeto haya adquirido un conocimiento efectivo del contenido secreto o íntimo; pero al mismo tiempo, excluye del delito aquéllos comportamientos que objetivamente pueden dar lugar a una vulneración de un secreto o de la intimidad, pero no se hallan animados por tal intención.

La comisión por imprudencia no está tipificada expresamente, por lo que no resulta punible, de acuerdo con la exigencia del art. 12 del CP. Desde una perspectiva político-criminal es acertada esta exclusión punitiva, y al mismo tiempo resulta coherente con la en principio incriminación excepcional de la imprudencia por la que optó el legislador en el CP vigente.

La impunidad de la imprudencia tiene relevancia para el error sobre el tipo (p. ej., si una persona se apodera de un papel creyendo equivocadamente que no posee ningún contenido relevante para la intimidad, siendo que el dolo ha de abarcar el conocimiento de tal circunstancia)[52], pues tanto sea el error invencible (porque así lo establece el art. 14.1, primer inciso, del CP), como vencible (en cuyo caso se prevé su sanción por imprudencia, art. 14.1, segundo inciso), el hecho será impune, al no existir la tipicidad imprudente para estos delitos.

Asimismo, las intromisiones accidentales quedan fuera de la cobertura de este delito[53], lo que puede hacer problemática la incardinación en algún tipo delictivo el uso posterior de lo aprehendido o interceptado.[54]

[49] Estiman asimismo que se trata de un elemento subjetivo del tipo, Jorge Barreiro, *ComCP*, 569; Morales Prats, *ComCP*, 427 y s., quien, no obstante, se muestra muy crítico con la exigencia de tal elemento; Sola Reche (2001), 214.

[50] Muñoz Conde, *PE*, 252.

[51] Muñoz Conde, *PE*, 252. Considera que estos elementos subjetivos introducen una restricción para otras formas de intrusismo no animadas por ningún elemento subjetivo especial, Morón Lerma, 50 y s.

[52] Anarte Borrallo, 53.

[53] En este sentido, la STS 8 de julio de 1992 ha señalado que "no basta con la mera u ocasional escucha producida cuando el usuario de un determinado teléfono oye casualmente una conversación de otros dos interlocutores debido a defectos técnicos de la infraestructura telefónica o por las especiales características del tipo de teléfono utilizado […] la acción de comunicar la conversación así escuchada a una tercera persona puede ser reprochada social y éticamente como un acto indirecto y maledicente, pero no tiene un específico encaje legal en el tipo".

[54] Sobre este particular Sola Reche (2001), observa que no son típicos los hechos consistentes en descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, cuando hacerse con papeles, etc., no constituya apoderamiento, y el acceso a las telecomunicaciones no signifique su interceptación, lo que además, hace

5. Accesos legítimos a las comunicaciones de terceros a través de la red

La presencia de causas de justificación en estos delitos puede ser muy amplia, pero al mismo tiempo de una excepcional complejidad[55]. Por lo general, sin perjuicio de la casuística con que se presenten, la mayor parte de las causas de justificación cuya concurrencia puede dar lugar a discusión gira en torno al ejercicio legítimo de un derecho[56], al cumplimiento de un deber (nº 7º del art. 20) y, probablemente con menos frecuencia, el estado de necesidad.

Como quedó dicho y argumentado más arriba, el consentimiento del interesado (art. 197.1) no opera como una causa de justificación, sino de exclusión de la tipicidad misma. Sería absurdo pensar que, p. ej., cuando alguien señala a otro un documento con información íntima y le solicita que lo tome y lea con el fin de que le de su consejo, está incurriendo ya en el tipo, pero de forma lícita. Insistamos en que la voluntad del titular del contenido íntimo es decisiva para determinar hasta dónde puede llegar la intervención del Derecho Penal, dada la amplia disponibilidad del bien jurídico reconocida a su titular.

A semejante conclusión llegamos también en relación con las conductas de acceso, alteración, utilización, etc., de datos personales cuando han sido autorizadas por quienes tengan competencias para ello y dentro de las operaciones que la ley prevé para el tratamiento y gestión de los datos[57].

A continuación se estudian algunos supuestos más frecuentes y, por lo general, también más problemáticos[58].

5.1. La prevención y la persecución de los delitos

El acceso a correos electrónicos y a otras formas de comunicación y a datos de carácter personal en la red con el fin de prevenir la comisión de delitos a través de la misma (pornografía infantil, incitación a la xenofobia, terrorismo) y de su persecución, en su caso, ha despertado un particular interés en los últimos años. En ocasiones puede constituir un deber intervenir las comunicaciones efectuadas a través de la red. En efecto, el nuevo régimen legal establecido sobre los servicios de la sociedad de la información[59] impone a los proveedores de acceso y a los prestadores de servicios en la red ciertas obligaciones que podrían afectar a la protección de los datos personales y en concreto dar lugar a la realización de alguna de las conductas típicas estudiadas con anterioridad.

---

notar el autor, puede plantear dificultades de encaje de algunos tipos que guardan dependencia con éste (en concreto, el art. 197.3 CP).

55 De semejante parecer, Anarte Borrallo, 55; Muñoz Conde, *PE*, 252 y s.

56 Cfr. SAP Madrid de 11 de enero de 2002.

57 Y por lo que entonces se expuso, es mucho más absurdo conferir al consentimiento del titular de los datos una relevancia que en realidad no tiene, a salvo de hipotéticos supuestos excepcionales.

58 V. más ampliamente sobre accesos legales, Hernández Guerrero, 391 y ss.

59 Véase la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

En relación con las competencias y obligaciones de los prestadores de servicios se plantean dos clases de problemas. En primer lugar, determinar qué comportamientos pueden verse afectados por los tipos delictivos que están siendo objeto de este estudio, o bien por otros tipos delictivos; y, en segundo, lugar, qué naturaleza jurídico—penal tienen dichas conductas, a la vista de que actuarán o deberán actuar de acuerdo con lo previsto en la ley, es decir, estando autorizados, mientras que el tipo del art. 197.2 requiere actuar "sin estar autorizado". Por consiguiente, aunque este segundo aspecto lo entiendo como una cuestión de tipicidad, lo trataremos aquí de forma autónoma, a la vista de las características más peculiares que presenta. Por otro lado, no debe olvidarse que el delito exige que el objeto material sobre el que recae la acción han de serlo los datos reservados de carácter personal y familiar, circunstancia que no siempre tiene por qué concurrir en los datos que pueden hallarse involucrados en relación con estos hechos. Sin embargo, respecto al correo electrónico y otras comunicaciones hemos visto cómo únicamente el consentimiento en cualquier forma de acceso en los mismos excluye el tipo y que en estos casos es, sin embargo, la ley la que puede legitimar tales accesos por los prestadores de servicios.

En primer lugar, los prestadores de servicios de la sociedad de la información tienen la obligación de interrumpir la prestación o de retirar los datos que vulneren ciertos principios que se enumeran en la ley[60]. Estas conductas en si mismas consideradas no comportan en absoluto actos de apoderamiento de datos. Por lo que en relación con este delito la acción es atípica, sin perjuicio de que pudiera constituir un delito de daños (art. 264.2 del CP —daños sobre datos, programas o documentos electrónicos contenidos en sistemas informáticos, si los datos se destruyen, alteran o inutilizan, a lo que, por cierto, no alude la ley como parte del comportamiento obligado).

En segundo lugar, corresponde a estos mismos profesionales el deber de retención de datos de tráfico relativos a las comunicaciones electrónicas por un período máximo de doce meses (art. 12 Ley 34/2002)[61]. Es indudable que el hecho se enmarca dentro de la conducta típica de apoderamiento, del art. 197.1 del CP, aunque la acción se limite a guardar una copia de dichos datos.

[60] De conformidad con lo que prevé el art. 8.1 de la Ley 34/2002. Los principios aludidos en el texto, que se enumeran en dicho precepto, son: a) La salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional. b) La protección de la salud pública o de las personas físicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores; c) El respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social, y d) la protección de la juventud y de la infancia". Es oportuno destacar que se añade en el mismo precepto que cuando esté normativamente previsto que las actuaciones que han sido mencionadas en el texto hayan de ser intervenidas por la autoridad judicial competente, a ésta corresponderá entonces la adopción de tales medidas.

[61] La Directiva 2002/58/CE, ya citada, indica qué debe entenderse por datos de tráfico, así como por datos de localización: "Datos de tráfico; cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma. Datos de localización: cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal del usuario de un servicio de comunicaciones electrónicas disponibles para el público" (art. 2, letras b y c, respectivamente).

No obstante, con el fin de dejar sentado el alcance de esta obligación, sus límites, sus finalidades y el hecho de tener que cederse a terceros, debe completarse aquí la exposición de parte de esta normativa: "2. Los datos que, en cumplimiento de lo dispuesto en el apartado anterior, deberán conservar los operadores de redes y servicios de comunicaciones electrónicas y los proveedores de acceso a redes de telecomunicaciones serán únicamente los necesarios para facilitar la localización del equipo terminal empleado por el usuario para la transmisión de la información. Los prestadores de servicios de alojamiento de datos deberán retener sólo aquellos imprescindibles para identificar el origen de los datos alojados y el momento en que se inició la prestación del servicio. En ningún caso, la obligación de retención de datos afectará al secreto de las comunicaciones. Los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios a que se refiere este artículo no podrán utilizar los datos retenidos para fines distintos de los indicados en el apartado siguiente u otros que estén permitidos por la Ley , y deberán adoptar medidas de seguridad apropiadas para evitar su pérdida o alteración y el acceso no autorizado a los mismos. 3. Los datos se conservarán para su utilización en el marco de una investigación criminal o para la salvaguardia de la seguridad pública y la defensa nacional, poniéndose a disposición de los Jueces o Tribunales o del Ministerio Fiscal que así lo requieran. La comunicación de estos datos a las Fuerzas y Cuerpos de Seguridad se hará con sujeción a lo dispuesto en la normativa sobre protección de datos personales" (art. 8º, Ley 34/2002).

Como es obvio, la concurrencia del tipo objetivo (más exactamente, de la acción típica mencionada) no exime del análisis del resto de los elementos, en concreto ahora, del subjetivo. En otro lugar me he decantado a favor de que "en perjuicio de tercero", frente a la posición jurisprudencial y de algún sector doctrinal (que lo conciben, incorrectamente en mi opinión, como un elemento objetivo), debe entenderse como un elemento subjetivo de lo injusto que debe añadirse a la presencia del dolo[62]. En consecuencia, y conforme a este criterio, me parece dudoso que el prestador de servicios actúe en los casos en los que se lo impone la legislación vigente animado por la antedicha intención, por lo que por esta vía podría quedar ya incompleto —y excluido— el tipo.

De todos modos, queda pendiente de valoración el sentido que en este contexto tan particular cabe otorgar a "sin estar autorizado" (art. 197.2 del CP). No cabe duda de que la Ley citada otorga una autorización para realizar las conductas mencionadas más arriba en relación con la sociedad de la información. Sin embargo, a diferencia de las actividades de las personas a quienes corresponde las tareas de tratamiento y gestión de los datos con la finalidad de que éstos puedan cumplir su función normal a la que están destinados sin que se produzca en principio ninguna interferencia que afecte al titular de los datos, en los supuestos que nos ocupan ahora los datos que son objeto de captación, eliminación (alteración o modificación), etc., con propósitos de seguridad en la red, están realizando conductas que, en sentido estricto, van más allá de lo que correspondería a al tratamiento funcional de los mismos (esto es, servir de intermediarios para la difusión de los datos a través de la red), por lo cual, sin dudar de la importancia que dichas operaciones pueden comportar en beneficio de los demás usuarios de la red y de terceras personas, y por ello de su

[62] Véase Romeo Casabona, *ComCP II*, 671 y s.

legitimidad, entiendo que tales comportamientos pueden traspasar el ámbito de la tipicidad, constituyendo así la autorización (o imposición normativa: cumplimiento de un deber) una causa de justificación.

Como acaba de comprobarse, la ley autoriza a determinados profesionales a que de forma sistemática procedan a registrar y conservar durante un período de tiempo legalmente establecido los datos de tráfico de todos los usuarios, con el fin de poder localizar, si ello fuera necesario, el equipo terminal empleado para la transmisión, así como identificar el origen de los datos alojados y el momento en el que ese inició la prestación del servicio, sin que tales retenciones puedan afectar al secreto de las comunicaciones. Cabe preguntarse entonces si los agentes de la autoridad (los miembros de los cuerpos y fuerzas de seguridad) estarán legitimados al acceso directo a tal información o incluso al contenido de las comunicaciones si tienen indicios o sospechas de la comisión de algún delito.

A este respecto debe recordarse previamente que las conductas tipificadas como delito en el art. 197 configuran otros tipos agravados cuando el hecho es cometido por autoridad o funcionario público fuera de los casos permitidos por las leyes (art. 198 del CP). Aunque las leyes procesales no hacen mención de los mensajes de correo electrónico, no cabe duda de que, como he venido apuntando en pasajes anteriores, constituyen una forma de correspondencia y a ella hay que asimilar su tratamiento jurídico, en este caso el relativo al derecho de interferir en estos mensajes por parte de la autoridad o un funcionario público. En consecuencia, son aplicables a las interceptaciones o accesos a los mensajes de correo electrónico las misma excepciones justificantes y con los mismo requisitos que marca la ley.

No tan fácilmente asimilable es el control o revisión de los accesos a internet cuando éstos no consistan tan sólo en comunicaciones directas con otras personas (chat oral o escrito), por ejemplo, el acceso a determinadas páginas o sitios de la red. En cualquier caso, y sin perjuicio de la actualización que requiere de forma general el ordenamiento jurídico en relación con las diversas manifestaciones y aplicaciones de las tecnologías de la información y la comunicación, no veo obstáculo para aplicar las prescripciones que se refieren a las comunicaciones, tanto en lo relativo a su protección como cuando se trata de acceder legítimamente a ellas mediante la en todo caso necesaria autorización judicial.

5.2. LAS COMUNICACIONES EN EL LUGAR DE TRABAJO

En el seno de la empresa se plantean varios problemas en relación con el acceso a los mensajes de correo electrónico de los empleados y a otros accesos y comunicaciones semejantes a través de la red realizadas por aquéllos. En resumen, se trata de hipotéticos comportamientos en los que se plantea el acceso al correo del trabajador para comprobar si está utilizando el servicio de correo electrónico y el acceso a la red con fines particulares u otros abusivos.

En cuanto al acceso al correo electrónico privado del trabajador la cuestión es ciertamente compleja. No cabe duda de que, como se vio más arriba, a él se extiende el derecho al secreto de las comunicaciones[63]. En resumen, se trata de información personal de carác-

[63] También en este sentido, Ruiz Marco, 57.

ter reservado que puede entrar asimismo en el ámbito de protección de la norma penal que estamos estudiando (art. 197.1 o 2 del CP, según los casos). Por su parte, el empresario puede estar movido por diversos intereses aparentemente legítimos para acceder al correo electrónico de sus empleados, como podría serlo la obtención de elementos de prueba para un despido, o con el fin de comprobar si el trabajador está haciendo uso privado del correo electrónico, y además si lo hace en horas de trabajo, aspectos ambos que podrían comportar un perjuicio económico para la empresa, o cuando sospecha que el correo está siendo usado para la comisión de un delito (distribución de mensajes xenófobos, pornografía, etc.). Entonces se trata de ver si el empresario puede actuar amparado por una causa de justificación, en concreto la del ejercicio legítimo de un derecho (art. 20 nº 7 del CP).

La escasa jurisprudencia existente sobre estas situaciones, en todo caso no penal, ha exigido como primer requisito la proporcionalidad entre el objetivo buscado por el empresario y el acceso al correo del empleado, habiendo negado su concurrencia cuando aquél únicamente pretendía acopiar pruebas para fundamentar como procedente un despido[64].

Por lo que se refiere a los accesos de inspección o revisión del correo para comprobar la naturaleza privada o laboral-profesional del correo, debe añadirse que para determinar si por parte del trabajador hay un comportamiento abusivo que pueda ser causa de despido, habrá de estarse a lo pactado entre el empresario y los trabajadores sobre el uso de ese servicio. En todo caso, no se estima en la actualidad razonable una exclusión absoluta al trabajador del acceso al correo electrónico, dada su utilidad y el hecho de que no puede privarse a las personas de acceder a nuevos recursos tecnológicos, siempre que se usen con moderación y comporten, cuando se hace durante el horario laboral, un uso con repercusiones inapreciables en relación con la actividad laboral a la que está obligado a prestar el trabajador[65]. En consecuencia, para que el comportamiento sea lícito, el acceso al correo del trabajador bajo sospecha por parte del empresario deberá hacerse de acuerdo con las formalidades de la normativa laboral[66] o abstenerse en otro caso. Los controles, monitorizaciones o revisiones rutinarias a toda la plantilla de empleados sólo podrán realizarse si hay una norma legal que lo autorice.

La Dirección General del Mercado Interno de la Unión y el Grupo de trabajo de la Comisión Europea sobre protección de datos[67] se han pronunciado sobre este asunto, admitiendo la posibilidad de acceso a los mensajes de correo de los trabajadores, siempre y cuando se den una serie de garantías entre las que destacan: a) la necesidad de un propósito especificado, explícito y legítimo; b) que la supervisión sea una respuesta proporcionada sobre un patrón de riesgo, y c) la mínima repercusión sobre los derechos a la intimidad de los trabajadores afectados[68].

[64] Sentencia del Juzgado de lo Social nº 12 de Barcelona de 16 de septiembre de 2002.

[65] Así, la sentencia TSJ de Madrid de 12 de junio de 2001 y sentencia del Juzgado de lo Social nº 12 de Barcelona de 16 de septiembre de 2002.

[66] En este sentido, Ruiz Marco, 60, apunta al art. 18 del ET de 1995, conforme al cual deberá hacerse en presencia de un testigo (un enlace sindical o, en su defecto, otro trabajador).

[67] Opinión 8/2001 y Resolución 29 de mayo de 2002, respectivamente.

[68] En estos documentos y en la vulneración del art. 18.3 CE y 11 LOPJ se funda la STSJ Cataluña de 11 de junio de 2003, para considerar ilícitos el bloqueo, acceso y copia del correo electrónico y las trazas (*cookies*) de

Si existe la sospecha de que el trabajador está cometiendo un delito por medio del correo electrónico u otras comunicaciones por medio de la red deberá ser la autoridad judicial quien tome la decisión de autorizar la intervención de esta correspondencia o comunicación.

Respecto al control de los accesos a páginas *web* a través de internet, al consistir en comunicaciones privadas, está sometido en términos generales a un régimen similar.

6. BIBLIOGRAFÍA CITADA

AA.VV., *Internet y derecho penal*, *Cuadernos de Derecho Judicial*, Consejo General del Poder Judicial, Madrid, 2002.

Anarte Borrallo, "Consideraciones sobre los delitos de descubrimiento de secretos (I). En especial, el artículo 197.1 del Código Penal", en *JD*, nº 43, 2002.

Bajo Fernández/Díaz Maroto PE, *Manual de Derecho penal. Parte Especial. Delitos contra la libertad y seguridad, libertad sexual, honor y estado civil*, 2ª ed., Ed. Centro de Estudios Ramón Areces, Madrid, 1991.

Carbonell/González Cussac PE, Vives/Boix/Carbonell/González Cussac, *Derecho Penal. Parte Especial*, 3ª ed., Ed. Tirant lo Blanch, Valencia, 1999.

Fernández López, "La nueva regulación de la protección de datos personales en España a partir de la Ley Orgánica 15/1999, de 13 de Diciembre", en *«Ius & Law»*, nº 1 y 2, 2001.

Hernández Guerrero, "La intervención de las comunicaciones electrónicas", en *Estudios Jurídicos. Ministerio Fiscal*", III-2001, Centro de Estudios de la Administración de Justicia, Madrid, 2001.

Higuera Guimerá (1986a), "Los delitos de colocación ilegal de escuchas telefónicas en el Código penal español", en *BIMJ*, nºs 1414 y 1415, 1986.

Higuera Guimerá (2002), "El descubrimiento y la revelación de secretos", *AP*, nº 31, 2002.

Jorge Barreiro ComCP, *Comentarios al Código Penal* (dir. Gonzalo Rodríguez Mourullo, coord.. Agustín Jorge Barreiro), Civitas, Madrid, 1997.

Lozano Miralles, PE: Bajo Fernández, *Compendio de Derecho Penal (Parte Especial)*, II, Madrid, 1998.

Mata y Martín, *Delincuencia informática y Derecho Penal*, Edisofer, Madrid, 2001. Morales Prats (2001), La intervención penal en la red. La represión penal del tráfico de pornografía infantil: estudio particular, en Zúñiga Rodríguez, Méndez Rodríguez y Diego Díaz-Santos (Coords.), "Derecho Penal, sociedad y nuevas tecnologías", Ed. Colex, Madrid, 2001.

Morales Prats ComCP, *Comentarios a la Parte Especial del Derecho Penal* (dir. Gonzalo Quintero Olivares, coord. Fermín Morales Prats), 3ª ed., Aranzadi, Pamplona, 2002.

Morales Prats (2002), "Internet: riesgos para la intimidad", en «*Internet y derecho penal», Cuadernos de Derecho Judicial*, Consejo General del Poder Judicial, Madrid, 2002.

Morón Lerma, *Internet y Derecho Penal: Hacking y otras Conductas Ilícitas en la Red*, Aranzadi, Pamplona, 1999.

Muñoz Conde PE, *Derecho penal. Parte Especial*, 14ª ed., Ed. Tirant lo Blanch, Valencia, 2002.

Orts Berenguer/Roig Torres, *Delitos informáticos y delitos comunes cometidos a través de la informática*, Tirant lo Blanch, Valencia, 2001.

acceso a otras páginas web por parte de una trabajadora realizados por su empresa para justificar un despido disciplinario, que el Tribunal considera improcedente.

Queralt Jiménez PE, *Derecho penal español. Parte Especial, 3ª ed. corregida y puesta al día*, J.M. Bosch Editor, Barcelona, 1996.

Polaino Navarrete, PE I, *Curso de Derecho Penal español. Parte Especial*, I (dir. Manuel Cobo del Rosal), Marcial Pons, Madrid, 1996.

Rodríguez Fernández, "La intervención telefónica como restricción al derecho fundamental a la intimidad", en *RP*, nº 5, 2000.

Rodríguez Ramos PE II, *Derecho Penal, Parte Especial*, II, Serv. De Publicaciones de la Facultad de Derecho, Universidad Complutense, Madrid, 1997.

Romeo Casabona (1988), *Poder informático y seguridad jurídica (La función tutelar del Derecho Penal ante las nuevas tecnologías de la Información)*, Fundesco, Madrid 1988.

Romeo Casabona (1993), "Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías", en *PJ*, nº 31, 1993 (publicado también en *Revista del Foro Canario*, nº 87, 1993).

Romeo Casabona (2001), "La protección penal de la intimidad y de los datos personales en sistemas informáticos y en redes telemáticas (internet)", en *Estudios Jurídicos. Ministerio Fiscal*, Centro de Estudios Jurídicos de la Administración de Justicia, Ministerio de Justicia, Madrid, III-2001.

Romeo Casabona (2002), "La intimidad y los datos de carácter personal como derechos fundamentales y como bienes jurídicos penalmente protegidos", en *Libro en memoria del Profesor Lidón*, Universidad de Deusto, Bilbao, 2002.

Ruiz Marco, *Los delitos contra la intimidad. Especial referencia a los ataques cometidos a través de la informática*, Ed. Colex, Madrid, 2001.

Seoane Rodríguez, "De la intimidad genética la derecho a la protección de los datos genéticos. La protección iusfundamental de los datos genéticos en el Derecho español (A propósito de las SSTC 290/2000 y 292/2000, de 30 de noviembre) (Parte I)", en *Rev Der Gen H*, nº 16, 2002.

Serrano Gómez PE, *Derecho Penal. Parte Especial*, 3ª ed., Dykinson, Madrid, 2002.

Sola Reche (2001), "La protección penal de los datos personales genéticos en el Derecho español", en Carlos María Romeo Casabona (Ed.), *Genética y Derecho Penal. Previsiones en el Código Penal Español de 1995*, Cátedra Interuniversitaria Fundación BBVA – Diputación Foral de Bizkaia de Derecho y Genoma Humano, Universidad de Deusto y Universidad del País Vasco – Ed. Comares, Bilbao – Granada, 2001.

De Vicente Remesal, "Descubrimiento y revelación de secretos mediante escuchas telefónicas", en *PJ*, 1990.

RESUMEN: La rápida y enorme expansión lograda por las comunicaciones personales a través de internet, en particular el correo electrónico, ha generado al mismo tiempo abusos contra la confidencialidad y el anonimato con el que deben estar presididas aquéllas en relación con terceros. Se trata en el presente estudio de comprobar si los instrumentos jurídico-penales actuales son suficientes para prestar la protección adecuada a dichas comunicaciones.

ABSTRACT: The quick and enormous expansion achieved by personal communications through Internet, especially via e-mail, has developed, at the same time, abuses against confidentiality and anonymity, principles which must rule those communications with third parties. The goal of this study is to verify if the current juridical and criminal instruments are enough to provide the necessary protection to such communications.