Presente y futuro

POR **JUAN JOSÉ GONZÁLEZ RUS**

Sobre la base de que el Derecho Penal debe intervenir en la protección de la intimidad ante el uso de la informática, se concluye que nuestro Código Penal y el proyecto de 1992 no aportan una garantía suficiente. La cultura del papel sigue presidiendo la regulación de nuestros delitos. Las carencias que presenta la protección de la intimidad en el Código penal son prácticamente absolutas en relación con los comportamientos ligados con la informática y los bancos de datos de carácter personal, sin que la aplicación de figuras delictivas mediatamente relacionadas con el tema pueda superar la laguna legal.

1. INTIMIDAD E INFORMÁTICA: NECESIDAD Y UTILIDAD DE LA INTERVENCIÓN PENAL

Plantear cómo es y cómo debe ser la intervención penal en la protección de la intimidad ante el uso de la informática y, en particular, en relación con los bancos de datos de carácter personal, presupone aceptar que el Derecho penal debe intervenir en ese más que posible conflicto entre una y otra. Su carácter fragmentario (el Derecho penal sólo debe tutelar los bienes jurídicos más importantes para el mantenimiento del orden social y ante los ataques más graves) y su naturaleza de ultima ratio (el instrumento penal es el último recurso que debe utilizarse para tutelar bienes jurídicos, y sólo debe acudirse a él cuando resulten insuficientes otros medios de actuación y protección social y jurídica), imponen, de una parte, constatar que en la intimidad concurren las tres notas que tradicionalmente se vienen exigiendo a todo bien jurídico como presupuesto de su protección penal: que sea digno de protección, que sea capaz de protección, y que esté necesitado de protección; de otra, que la informática y las nuevas tecnologías relacionadas con el tratamiento de la información constituyen instrumentos idóneos para lesionarla o ponerla en peligro y de la suficiente gravedad para ser objetos de la atención penal.

Hoy, resulta ocioso insistir en que la intimidad es, por su importancia, un bien susceptible de tutela penal (1) y la informática una eventual fuente de graves atentados a la misma. Para confirmar que es un bien digno de protección baste recordar su reconocimiento constitucional como uno de los derechos fundamentales de la persona (art. 18.1 CE) y, por su especial potencial lesivo, la previsión expresa de la limitación legal del uso de la informática para garantizarla (art. 18.4 CE). En realidad, la protección de la intimidad es una vía necesaria para tutelar dere chos que mediatamente aparecen conectados con ella y que pueden verse amenazados con su violación: libertad ideológica, honor, igualdad y derecho a no ser discriminado, derecho al trabajo, etc. Es también capaz de protección, en la medida en que aparecen suficientemente delimitados tanto los elementos materiales en que se sustancia (a los

Fundación Telefónica
Telefónica

efectos que aquí tratamos, los datos personales) como la idoneidad de las conductas infractoras para lesionarla, que resultan, por añadidura, fácilmente identificables.
Para prevenir y sancionar los atentados de que puede ser objeto con el uso de la informática no son suficientes los medios de protección no penales actualmente disponibles, pues a pesar de las infracciones y sanciones previstas en la LORTAD (2), pueden darse agresiones merecedoras, por su gravedad, de la atención punitiva, lo que la convierte en un bien jurídico necesitado de protección penal.
Como consecuencia, puede afirmarse que el Derecho penal debe proteger la intimidad ante eventuales ataques relacionados con la creación, tratamiento y explotación de bancos de datos de carácter personal.

2. LA PROTECCIÓN EN EL CÓDIGO VIGENTE

Las conductas potencialmente lesivas de la intimidad que pueden producirse en torno a bancos de datos de carácter personal son muy variadas: creación clandestina de bancos de datos; recogida engañosa o fraudulenta de datos; implementación del fichero con datos inexactos, falsos o incompletos; omisiones de actualización que alteran el sentido y significado de los mismos o los convierten en inexactos o erróneos; desatención de las solicitudes de información y, en su caso, rectificación de datos por los sujetos a los que se refiere la información; incumplimiento del deber de secreto de los responsables u operadores del sistema; venta, transmisión, cesión o transferencias ilícitas de datos, etc. En el Código penal vigente, sin embargo, no hay figura delictiva alguna que sancione específicamente tales comportamientos; ni siquiera los más graves -pues no todos, sino solo los más intolerables, deben ser, como queda dicho, competencia del Derecho penal- encuentran en nuestro texto punitivo reflejo expreso.
La intimidad, por otra parte, recibe en el Código penal una protección parcial, a través de figuras provenientes de la era del papel y de momentos en los que eran impensables supuestos de esta naturaleza. Más lamentable es que tampoco se pensara en ello más recientemente; por ejemplo, en 1984,cuando se incorpora al Código el art. 497 bis, que después comentamos, y que al limitarse a las interceptaciones telefónicas y a la utilización de instrumentos o técnicas de captación del sonido, resultó viejo, por insuficiente, desde el mismo momento en que nació. El escaso juego que cabe esperar de las figuras dedicadas a la protección de la intimidad, hace necesario intentar cubrir la laguna legal ensayando fórmulas interpretativas que -si las hubiera- descubran o amplíen posibilidades de aplicación a los casos que nos ocupan en modalidades delictivas dirigidas a la tutela de otros bienes jurídicos (inviolabilidad de la correspondencia, secreto de las comunicaciones, infidelidad en la custodia de documentos, honor, libertad, seguridad del tráfico jurídico o fe pública) que pueden verse incidentalmente lesionados con comportamientos de este tipo.
El camino metódico más adecuado para ello es agrupar los casos posibles en atención al bien jurídico que mediatamente puede verse afectado por los mismos. Sin pretensión exhaustiva, podría hacerse la siguiente clasificación: 1) los supuestos de recogida irregular de datos, divulgación ilícita o incumplimiento del deber de secreto, potencialmente lesivos de la intimidad, con los delitos de descubrimiento y revelación de secretos, y, para cubrir las eventuales lagunas, con la inviolabilidad de la correspondencia y de las comunicaciones y la infidelidad en la custodia de documentos; 2) la introducción de datos falsos, erróneos o inexactos, las omisiones de actualización, informes de conducta o solvencia elaborados sobre la base de los

Fundación Telefónica
Telefónica

mismos y similares, directamente no contemplados, resaltando su posible idoneidad para lesionar el honor, relacionarlos con los delitos de calumnia e injurias; 3) los mismos supuestos, relativos a errores en la recogida, implementación o actualización del fichero, a falta de otra posibilidad mejor, con las falsedades; y 4) en la creación clandestina de bancos de datos o en la utilización ilícita de los mismos, destacando su potencial lesivo de la libertad personal (si sirvieran para obligar al sujeto a realizar lo que no quiere: chantajes, confección de listas negras, registros de impagados tipo RAI, etc.), ver qué posibilidades de punición se ofrecen a traves de los delitos de amenazas y coacciones.

En lo que sigue, pues, con las limitaciones de espacio que la ocasión impone, trataremos de comprobar, de un parte, qué protección puede esperarse de las figuras dedicadas en el Código a la protección de la intimidad; de otra, hasta qué punto unos delitos dispuestos para la tutela de bienes jurídicos que en ocasiones no tienen nada que ver con la intimidad -y que desde luego no han pensado nunca en las aplicaciones informáticas- pueden ser reinterpretados y resultar útiles para castigar comportamientos relacionados con los datos de carácter personal.

1. Observaciones sobre los sujetos activo y pasivo de los eventuales delitos

Debe advertirse que las consideraciones que a continuación se hacen van referidas a datos de carácter personal de personas físicas; únicas, por lo demás, a las que se refiere la LORTAD (art. 1). Aunque penalmente se discuta si las personas jurídicas pueden ser sujeto pasivo de alguno de los delitos aludidos (calumnias e injurias, amenazas y coacciones), y éstas, sin duda, pueden ser titulares de datos susceptibles de ser tratados y manipulados informáticamente, no abordaremos aquí esa cuestión, limitándonos al examen de la perspectiva estrictamente personal, y aceptando de antemano que en lo que sigue sujeto pasivo de los delitos que eventualmente puedan cometerse es una persona física.

Del mismo modo, y con independencia de que la LORTAD haga recaer la responsabilidad administrativa sobre la figura del responsable del fichero (salvo en las violaciones del deber de secreto: artículos 42 y 10, respectivamente), basada en una especie de presunción de culpa in vigilando o in eligendo respecto de sus subordinados, el carácter personal de la responsabilidad penal obliga siempre a identificar al autor material de la conducta delictiva; lo que constituye una dificultad añadida a las derivadas de la interpretación de los respectivos preceptos, dadas las dificultades que ello ofrece en tareas y procesos en los que usualmente intervienen (o pueden intervenir) numerosas personas. Desde luego, identificado el autor material del delito, éste será el que responda, aunque no sea el responsable del fichero, pues las limitaciones o atribuciones de autoría que puedan hacer las normas administrativas no tienen valor alguno en el campo penal.

2. Descubrimiento y revelación de secretos, e inviolabilidad de la correspondencia y de las comunicaciones

Los tipos relativos al descubrimiento y revelación de secretos (art. 497 y ss.), secreto de Abogados, Procuradores (art. 360) y funcionarios (art. 367 y ss.) sólo podrán abarcar, obviamente, los datos calificables de secreto, entendiendo por tal la información de conocimiento restringido que su titular quiere mantener oculta. Por consiguiente, la mayor parte de la información que se recoge en los bancos de datos de carácter personal (relativas casi siempre a aspectos académicos, laborales o profesionales, hábitos de vida o consumo, situación económica, gastos, domicilio, etc.), relacionados más con la privacidad que con la intimidad -como reconoce la propia EM de la LORTAD-, quedan en principio extramuros de la protección penal. Sólo los llamados datos sensibles, relativos al origen racial, salud, vida sexual y creencias religiosas o ideológicas, y que en la LORTAD son objeto de atención especial,

Fundación Telefónica
Telefónica

podrían -en una determinación que deberá hacerse caso por caso- entrar dentro del concepto de secreto. Las posibilidades de incluir en alguno de estos delitos la recogida irregular de datos para su tratamiento informático son, sin embargo, limitadas si se consideran los términos de las correspondientes conductas típicas.

En el art. 497 (3) resulta imprescindible el apoderamiento (en principio, coger, cualquiera que sea la forma, o no devolver lo recibido por error) de los papeles o cartas del titular del secreto, de manera que si se llega al descubrimiento del mismo por otro procedimiento, no cabrá su apreciación. Los secretos han de ser, además, del propietario de los documentos, pues si fueran de un tercero la conducta es igualmente atípica. Aunque la cuestión sea debatida, creo que puede entenderse que concurre el apoderamiento cuando haya un acceso ilícito a la información, que pasa a estar a disposición de otro, o se produzca la captación intelectual del contenido de los papeles o cartas, aunque no se tome materialmente el escrito. Ello permitiría entender presente el requisito típico cuando se copia un fichero informático, se interfiere una trasmisión de datos o simplemente se visionan por pantalla, si no fuera porque la alusión a papeles o cartas obliga restringir la conducta a documentos escritos, con exclusión, por ejemplo, del cada vez más frecuente correo informático.

Las cartas que aquí se contemplan son las propias de la correspondencia epistolar, al contrario que en los supuestos en los que se protege la libertad de las comunicaciones, en donde se comprende también la correspondencia no escrita. En todo caso, es preciso que el apoderamiento se haga para descubrir los secretos, elemento subjetivo del injusto, que impide la comisión culposa y que hace que si la intención fuera otra no pueda estimarse este delito. Que todos estos elementos concurran conjuntamente en una recogida de datos, por muy irregular que sea, presumiblemente ocurrirá sólo en supuestos excepcionales, lo que muestra la escasa virtualidad del precepto para procurar una adecuada tutela de la intimidad personal en este ámbito. En todo caso, los delitos quedan consumados cuando se descubren los secretos, se incorporen o no posteriormente a algún banco de datos, evidencia de lo alejados que están los preceptos de los casos que contemplamos (4).

Otro tanto cabe decir del art. 498 (5), referido a secretos, documentales o no, que se conocen por concretas personas sometidas a especiales deberes de sigilo (administrador, dependendiente o criado). Aunque ni se precisa que los secretos estén recogidos en escritos -lo que permite incluir los contenidos en ficheros informáticos o los captados en transmisiones de datos, que quedaban fuera del 497- ni se requiere ninguna conducta de apoderamiento ni se contempla ningún ánimo especial, no es mucho mayor la virtualidad aplicativa que cabe esperar de esta modalidad delictiva en relación a los casos que comentamos. En todo caso, no basta el descubrimiento del secreto, sino que se requiere su divulgación y que el mismo se conozca precisamente por la relación de subordinación que media entre el titular y el sujeto activo, resultando atípicos aquellos en los que el secreto se conoce en virtud de otra relación o éste no se divulga.

Consideraciones semejantes pueden hacerse del art. 360 (6), de estructura similar a la del 498, y del art. 367 (7), manifestación, por lo demás, de la parca representación que tiene el incumplimiento del secreto profesional en nuestro Código, y capaces, a lo sumo, de prestar una protección marginal y ciertamente accidental en los supuestos que nos ocupan; especialmente en hipótesis de facilitación de datos para su inclusión en el fichero o de incumplimiento del deber de reserva (si el responsable del fichero fuera un funcionario, art. 367). Obsérvese, no obstante, que la responsabilidad criminal podría exigirse al Abogado, Procurador o funcionario que, inclumpliendo los deberes que sobre él pesan, facilitara la información que se introduce en el banco de datos, pudiendo alcanzar la punición a los responsables u operadores del fichero, a

Fundación Telefónica
Telefónica

lo sumo, como partícipes.
La interceptación de comunicaciones telefónicas o la utilización de técnicas de captación del sonido previstas en el artículos 497 bis (8), ofrecen, en principio, un mayor campo de acción, al ir referidas no sólo a los secretos, sino también a la intimidad de otros, lo que permite acoger informaciones y datos personales que no pueden calificarse de secreto en sentido estricto. Además de los captados o conocidos mediante los instrumentos o artificios técnicos de escucha, podrán incluirse los que se capten interfiriendo transmisiones telefónicas. Discutida es la posibilidad de considerar típica la interceptación de transmisiones telefónicas de datos (telex, fax, datos informáticos vía modem, redes especiales de transmisión de datos), por quienes entienden que se contemplan sólo comunicaciones entre personas y no entre personas y máquinas o de máquinas entre sí; cuestión que personalmente creo que debe resolverse en sentido afirmativo. No quedan protegidas, en cambio, las transmisiones que se produzcan por procedimientos no reconducibles a la telefonía (radio, satélite, imagen, redes informáticas internas) ni, por la exigencia del elemento subjetivo del injusto para descubrir, las que se produzcan con otra finalidad o son captados y descubiertos de forma accidental. Con la salvedad de no requerir esta finalidad específica, semejante es la interpretación que cabe hacer del art. 192 bis (9), relativo a conductas realizadas por autoridades y funcionarios.
Más tangencial aún es la relación de las figuras que, en relación a funcionarios públicos, tipifican los registros ilegales (art. 191) y la inviolabilidad de la correspondencia, ya cometida por funcionarios (art. 192), ya por particulares (art. 249); preceptos en cierto modo complementarios del art. 497 bis, en la medida en que por correspondencia debe entenderse la comunicación que no consista en conversaciones en presencia.
Las posibilidades que ofrece la reinterpretación de las figuras examinadas para sancionar la recogida irregular de datos de carácter personal para integrarlos en bancos de datos es, pues, ciertamente limitada; casi anecdótica, podría decirse. Sólo el incumplimiento del deber de secreto por responsables del fichero que sean funcionarios públicos podría encontrar acomodo sin grandes dificultades en los artículos 367 y 368. Ello hace que la única tutela que puede producirse en este campo venga de las infracciones y sanciones previstas en la LORTAD.

3. Calumnias e injurias

Los bancos de datos de carácter personal pueden contener datos capaces de lesionar el honor del sujeto al que se refieren, por lo que interesa explorar también las posibilidades de tutela que pueden proporcionar los delitos de calumnia e injurias. Como consecuencia de errores en la recogida de datos o en la implementación del fichero, inexactitudes, lagunas u omisiones en la actualización de los datos, puede producirse la «falsa imputación de un delito de los que dan lugar a procedimiento de oficio», reconducible al ámbito de la calumnia (art. 453), o la atribución de hechos, comportamientos, condiciones, vicios o faltas de moralidad o actitudes susceptibles de integrar un delito de injurias (art. 457 y 458) (10). Con la particularidad, además, de que el distinto papel que en un delito y otro cumple la exceptio veritatis hace que si en la calumnia el delito imputado ha de ser falso (o lo que es lo mismo: el dato ha de ser erróneo), en las injurias puede producirse el delito aunque lo imputado al sujeto sea cierto (11), con tal de que objetivamente suponga la deshonra, el descrédio o el menosprecio de otra persona y subjetivamente esté presente el animus inuriandi que, como elemento subjetivo del injusto (común a la calumnia), se considera imprescindible para la comisión del delito.
Precisamente la exigencia de este ánimo será la dificultad principal que encuentre la estimación de ambos delitos en casos como los que nos ocupan. Aunque la jurisprudencia viene entendiendo implícito el ánimo de injuriar en los comportamientos que ya objetivamente aparecen como gravemente injuriosos, sólo excepcionalmente se producirá esta circunstancia

Fundación Telefónica
Telefónica

en los datos de carácter personal que usualmente integran los ficheros de datos. Como en la recogida de datos o en la implementación de la base muy probablemente intervendrán distintas personas, sería necesario, primero, identificar quiénes suministraron, introdujeron o trataron la información que se considera calumniosa o injuriosa y, después, que lo hicieron con el propósito de injuriar al titular de la misma. Las dificultades que ello presenta son obvias; más, si se considera que para la formación de bancos de datos tanto la recogida como la introducción de los mismos suele ser indiscriminada y no referida a sujetos concretos. Pensar que, en tales casos, hay un propósito genérico e indiscriminado de injuriar a todos los titulares afectados por el error, la inexactitud o el dato injurioso sólo sería viable si la información tuviera en sí misma la gravedad objetiva suficiente, lo que, como ya se ha dicho, no ocurrirá más que en casos excepcionales. Por otra parte, aunque doctrina y jurisprudencia coinciden en que el animus inuriandi puede concurrir con cualesquiera otros (de informar, criticar, narrar, etc.), pudiendo apreciarse el delito si el que prevalece es el primero (cuestión a determinar en función de las características de cada caso), lo más frecuente será también que predomine alguno de los otros propósitos, lo que supondría la desaparición de ambos delitos (12).

También aquí, por consiguiente, las posibilidades que se ofrecen para lograr la punición por vía indirecta están severamente limitadas por los requisitos que precisan los delitos contra el honor.

4. Falsedades

Las carencias de tutela que presenta la solución anterior pueden intentar solventarse acudiendo a los delitos de falsedades. Para ello, aceptado que los datos recogidos en el registro o fichero sean falsos, será preciso poder calificar al soporte informático en que se contienen de documento penalmente relevante en orden a los delitos de falsificación (13).

Salvo las previsiones de los artículos 1216 CCiv. y 596 LECiv. sobre el documento público, en el ordenamiento jurídico español no existe un concepto general de documento capaz de servir de soporte a sus distintas clases. Ello, obliga a reconstruir su noción sobre la base de los criterios doctrinales y jurisprudenciales, que, en síntesis, vienen exigiendo al mismo los requisitos de materialidad, fijeza y preconstitución probatoria. En definitiva: instrumentos escritos, atribuibles a una persona, en los que se recogen una o varias manifestaciones de voluntad, que hacen nacer o reconocen un derecho o un hecho de relevancia jurídica en el desarrollo de las actividades humanas (SSTS de 24 de noviembre de 1983, 29 de mayo de 1985, entre muchas).

Además de que los registros y ficheros informáticos no gozan de esa materialidad y fijeza reclamada para los documentos, los bancos de datos de carácter personal, por lo general, resultan ser un medio de información que no genera derecho ni obligación jurídica alguna, que no tienen eficacia probatoria y que, por consiguiente, no pueden ser considerados como documento, lo que hace inviable de principio la aplicación de los delitos de falsedad a los casos que analizamos. Sólo certificaciones impresas que fueran capaces de producir o probar hechos con trascendencia jurídica y en las que se produjera alguna de las alteraciones previstas en el art. 302 podrían integrar el delito; lo que raramente se dará en los casos que comentamos.

5. Amenazas y coacciones

Si la creación del banco de datos o la utilización que se hace del mismo se dirige a presionar a los titulares de la información para obligarles a realizar lo que no quieren (chantajes, confección de listas negras, registros de impagados o solvencia tipo RAI, etc.), nos encontraremos dentro del campo de acción de los delitos de amenazas y coacciones.

Cuando se conminara al sujeto con hacer pública la información que sobre el mismo se tiene

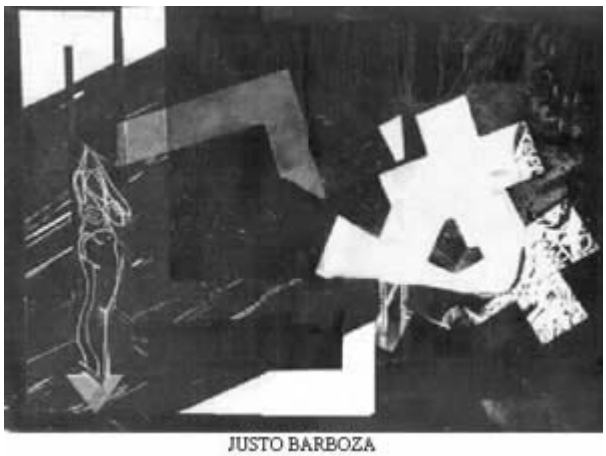
Fundación Telefónica

en el banco de datos, imponiéndole o no alguna condición,y con independencia de que, si se hubiera impuesto, ésta fuera lícita o ilícita, podrá integrarse sin dificultad alguna un delito de amenazas (artículos 493 y 494). El soporte en el que se encuentre la información no ofrece aquí particularidad alguna en orden a la apreciación del delito, que, si concurren los elementos típicos, podrá estimarse del mismo modo que cuando la información no está recogida en ficheros informáticos.
Distinto es, en cambio, el caso de las coacciones (art. 496: sin autorización legítima y con violencia, obligar a otro a hacer lo que la ley no prohíbe o compelerle a efectuar lo que no quiera, sea justo o injusto; por ejemplo: inclusión en listas negras para presionar al sujeto al pago de sus deudas). Y ello, porque su estimación requeriría probar: (1) que concurre la violencia reclamada por el precepto legal, lo que, aún aceptando el concepto amplio de la jurisprudencia (fuerza física, presión o costreñimiento moral o intimidación en las personas o fuerza en las cosas, directa o indirecta, y de una cierta intensidad) no será fácil ni aún en los bancos de datos de presumible finalidad conminatoria (a lo sumo podría integrarse la falta del 585.4º); y (2) que la finalidad real del banco de datos es la de limitar la capacidad de obrar del sujeto, o que, aún concurriendo también el propósito informativo, predomina la intención coactiva. Como ni uno ni otro extremo serán de fácil constatación en la mayoría de los casos que comentamos, también aquí las posibilidades de protección que cabe esperar son, pues, reducidas.

3. LA PROTECCIÓN EN EL FUTURO CODIGO PENAL

Frente a lo que pudiera pensarse, el Proyecto de Código penal de 1992 no alteraba sustancialmente el panorama expuesto. Siguiendo la lógica que inspira los actuales tipos de descubrimiento y revelación de secretos, junto a una más amplia concepción del secreto profesional (art. 199), se preveía el castigo de quien descubriera y/o revelara secretos o informaciones reservadas de carácter personal o familiar, apoderándose de sus papeles o documentos, ficheros, archivos o registros informáticos o utilizando instrumentos técnicos de captación del sonido, la imagen o cualquier otra señal de comunicación (art. 198.1, 2 y 3); agravándose las respectivas penas si el autor fuera el responsable del soporte informático o archivo (art. 198.4). Previsiones que se hacían extensivas a los «datos reservados de personas jurídicas» (art. 200).
Todo lo relativo a bancos de datos clandestinos, recogida o cesión irregular, engañosa o fraudulenta de datos, incluso sensibles, introducción y mantenimiento de datos erróneos o falsos, quedaba para la LORTAD, cuyo régimen de infracciones y sanciones (art. 42 ss.) era el único recurso aplicable. Del mismo modo, es dudoso que en la regulación penal que se proponía quedaran comprendidos los casos en que no hay apoderamiento de los datos, sino utilización ilegítima de los mismos, o la captación mediante el simple visionado por pantalla. La responsabilidad penal por hechos de ese tipo, por consiguiente, debería seguir planteándose como ahora, ensayando la eventual aplicación de los delitos contra el honor, amenazas, coacciones, etc.

Fundación Telefónica
Telefónica



JUSTO BARBOZA

La cultura del papel, poco explicable en un legislador de fines de siglo, presidía igualmente la regulación de los delitos de infidelidad en la custodia de documentos y violación de secretos (art. 394 ss.), resultando también discutible que la redacción de las falsedades documentales (art. 376 ss.), exigiendo papel o soporte material como presupuesto del concepto de documento, permitiera acoger los datos almacenados en registros magnéticos. Todo ello mostraba, además de precipitación en la elaboración de los tipos, que el legislador español continúa muy alejado de los problemas que plantea la informática y que no hay unas directrices político-criminales claras en torno al tema.

4. CONCLUSIONES GENERALES

A tenor de lo expuesto, pueden extraerse las siguientes conclusiones:
1. Las relaciones intimidad-informática tienen la importancia suficiente como para merecer la atención del Derecho penal.
2. En el Código penal vigente no hay precepto alguno que contemple los atentados a la intimidad que puedan realizarse con ocasión de la creación, implementación y explotación de bancos de datos de carácter personal.
3. Las modalidades delictivas reconducibles a la protección de la intimidad (fundamentalmente los delitos de descubrimiento y revelación de secretos), ajenos por completo a la realidad de la informática y de las nuevas tecnologías, podrían ser aplicables, a lo sumo, a supuestos marginales y poco frecuentes en la dinámica usual de conductas relacionadas con los bancos de datos.
4. Las posibilidades que ofrecen otras figuras delictivas para ofrecer una tutela indirecta en estos casos (calumnia, injurias, inviolabilidad de la correspondencia, libertad de las comunicaciones, infidelidad en la custodia de documentos, falsedades y amenazas y coacciones) son escasas y, desde luego, insuficientes para una adecuada contemplación penal del tema.
5. La propuesta de regulación que se contenía en el Proyecto de Código penal de 1992, aún mejorando la situación vigente, no suponía tampoco una respuesta correcta, evidenciando la falta de criterios político-criminales claros en la materia.
En definitiva: estamos ante un tema en el que, permítaseme la expresión coloquial, el legislador «ha oído campanas …, pero no sabe bien por dónde». Y ese, en los tiempos que corren -y, más aún, en los que se avecinan-, es un lujo que la sociedad española no puede permitirse.

Fundación Telefónica

(1) La distinción entre intimidad y privacidad a la que se refiere la E.M. de la LORTAD, y cuál debe ser la que integre el bien jurídico protegido en relación con el uso de la informática no la abordaremos aquí. Sobre ello, vid. ROMEO CASABONA, «Infracciones administrativas y penales en relación con la protección de datos», recogido en esta misma publicación, y LUCAS MURILLO, «La protección de los datos personales ante el uso de la informática en el Derecho español», en Estudios de Jurisprudencia, 1992, núm. 3, págs. 15 y ss. Sobre el concepto de intimidad y su tutela penal, vid. GÓMEZ PAVON, La intimidad como objeto de protección penal, Akal, Madrid, 1989, passim y GARCIA VITORIA, El derecho a la intimidad en el Derecho penal y en la Constitución de 1978, Aranzadi, Pamplona, 1983, págs. 17 y ss. Para una aproximación más específica a las relaciones entre informática e intimidad y situación del derecho comparado, vid. «III Congreso Iberoamericano de Informática y Derecho. Resumen de Comunicaciones», en Informática y Derecho, 1992, núm. 3, passim.
(2) Que representa actualmente el núcleo central de la protección en este ámbito, complementado por la tutela marginal que puede derivarse de otras disposiciones como la Ley 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, la Ley de Estadística, etc.
(3) «El que para descubrir los secretos de otro se apoderare de sus papeles o cartas y divulgare aquéllos será castigado con las penas de arresto mayor y multa de 100.000 a 2.000.000 de pesetas». «Si no los divulgare, las penas serán las de arresto mayor y multa de 100.000 a 500.000 pesetas».
(4) Vid. con mayor detalle, GONZALEZ RUS, «Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos», en Revista de la Facultad de Derecho de la Universidad Complutense de Madrid, 1986, monográfico núm. 12, págs. 144 y ss.
(5) Art. 498: «El administrador, dependiente o criado que en tal concepto supiere los secretos de su principal y los divulgare será castigado con la penas de arresto mayor y multa de 100.000 a 500.000 pesetas». El art. 499 va referido a secretos industriales y no a datos de carácter personal.
(6) Art. 360: «Será castigado con las penas de suspensión y multa de 100.000 a 500.000 pesetas el Abogado o Procurador que, con abuso malicioso de su oficio, o negligencia o ignorancia inexcusable, perjudicare a su cliente o descubriere sus secretos, habiendo tenido conocimiento de ellos en el ejercicio de su profesión».
(7) Art. 367, párr. 1º: «El funcionario público o autoridad que revelare los secretos o cualquier información de que tenga conocimiento por razón de su oficio o cargo y que no deban ser divulgados será castigado con las penas de suspensión y multa de 100.000 a 200.000 pesetas». Párr. 3º: «Si se tratare de secretos de un particular, las penas serán las de arresto mayor y multa de 100.000 a 500.000 pesetas». A efectos de pena se distingue según que se cause o no grave daño a la causa pública (párr. 2º). Fuera de consideración queda el art. 368, que tiene una dimensión económica que lo aleja, en principio, de los supuestos a que nos referimos. Sólo en casos verdaderamente excepcionales (datos de carácter personal de particulares contenidos en documentos o papeles confiados a funcionarios públicos por razón de su cargo) podrá tener interés considerar los artículos 364, 365 y 366, relativos a la infidelidad en la custodia de documentos.
(8) Art. 497 bis: «El que para descubrir los secretos o la intimidad de otros sin su consentimiento interceptare sus comunicaciones telefónicas o utilizare instrumentos o artificios técnicos de escucha, transmisión, grabación o reproducción del sonido será castigado con las penas de arresto mayor y multa de 100.000 a 500.000 pesetas. Si divulgare lo descubierto

Fundación Telefónica
Telefónica

incurrirá en las penas de arresto mayor en su grado máximo y multa de 100.000 a 2.000.000 de pesetas».
(9) El art. 192 bis castiga comportamientos similares a los contemplados en el art. 497 bis, realizados por «La autoridad, funcionarios públicos o agente de estos» que realizaren la conducta «sin la debida autorización judicial, salvo, en su caso, lo previsto legalmente en desarrollo del artículo 55.2 de la Constitución».
(10) Art. 457: «Es injuria toda expresión proferida o acción ejecutada en deshonra, descrédito o menosprecio de otra persona». Graves se consideran las que se recogen en el art. 458, entre las que se mencionan la imputación de un delito de los que no dan lugar a procedimiento de oficio, las de un vicio o falta de moralidad que pueda perjudicar considerablemente la fama, crédito o interés del agraviado, las que, por sus características, puedan ser tenidas como afrentosas y las que racionalmente merezcan la calificación de graves.
(11) Mientras que «El acusado de calumnia quedará exento de toda pena probando el hecho criminal que hubiere imputado» (art. 456), en la injuria la prueba de la verdad sólo se admite para eliminar la responsabilidad criminal cuando las imputaciones vayan dirigidas «contra funcionarios públicos sobre hechos concernientes al ejercicio de su cargo, o cuando tenga derecho a perseguir el delito imputado…» (art. 461).
(12) Mayores posibilidades tendría la aplicación de la Ley de 5 de mayo de 1982, ya aludida, por cuanto si bien las conductas capaces de integrar el delito de calumnia o injurias (vía penal) coinciden objetivamente con las intromisiones ilegítimas que contempla la Ley, la aplicación de ésta no precisa del animus inuriandi.
(13) Sobre el particular, vid., CARRASCOSA LOPEZ/BAUZA REILLY/GONZALEZ AGUILAR, «El derecho de la prueba y la informática. Problemática y perspectivas», en Informática y Derecho, 1991, núm. 2, págs. 57 y ss.

Fundación Telefónica