

FERMIN MORALES

**Profesor Titular de Derecho Penal
Universidad de Barcelona.**

Problemática jurídico-penal de las libertades informáticas en España tras diez años de vigencia de la Constitución de 1978

I. El presente trabajo (*) constituye una profundización de otros que sobre esta materia publiqué años atrás (1); una década de vigencia de la Constitución de 1978, sin que se haya producido el desarrollo legislativo de la previsión que contempla el art. 18.4 CE, la paralización de la Propuesta de Anteproyecto de Nuevo Código Penal de 1983 (PANCP), que prevé la creación de delitos informáticos, y la creciente informatización de datos en nuestro país, justifican una nueva reflexión sobre la pertinencia y alcance de respuestas penales frente a los abusos informáticos en la esfera de los bienes de la personalidad.

La necesidad de redefinir los bienes de la personalidad y, en particular, la intimidad frente al uso y desarrollo de la informática, ha puesto en cuestión la tradicional distinción entre derechos individuales y dere-

(*) El presente trabajo se corresponde básicamente con la ponencia presentada al Seminario Hispano-alemán sobre Informática y Derecho Penal, celebrado en la Facultad de Derecho de la Universidad de Barcelona en abril de 1988.

(1) *La tutela penal de la intimidad: "privacy e informática"*, Barcelona, 1984; "Privacy y Reforma Penal: La Propuesta de Anteproyecto de Nuevo Código Penal de 1983", en *Documentación Jurídica*, núm. 37/40 (Monográfico dedicado a la Propuesta de Anteproyecto del Nuevo Código Penal", vol. 1, Madrid, 1983, pp. 575 ss.; "Presupposti politico-criminale per una tutela della riservatezza informatica", en *Il Diritto dell'informazione e dell'informatica*, Anno 2, núm. 2 (Mayo-Agosto), 1986.

chos sociales, entre derechos participativos y libertades-límite, así como la esquemática dicotomía entre lo público y lo privado (2). Incluso determinados sectores doctrinales mantienen que estamos ante la génesis de derechos y libertades de “tercera generación”, que constituirían una respuesta a la “contaminación de las libertades” (*‘liberties’ pollution*) o erosión de los derechos fundamentales en la sociedad tecnológica (3). En tal medida parece conveniente abandonar el empleo de la locución *intimidad* en favor de otras denominaciones como la de “*privacy*” (se emplea el término anglosajón pues todavía la Real Academia de la Lengua no ha admitido el término “privacidad”), para designar estas nuevas necesidades de tutela en la esfera de los bienes de la personalidad. La “*privacy*” no puede ser definida, según los viejos patrones del bien jurídico *intimidad*, como aquella esfera individual en la que se constata un “*grado cero*” de sociabilidad, pues de la misma dimanar no sólo facultades de exclusión de terceros, sino también facultades de control sobre los datos personales informatizados que circulan en los circuitos telemáticos (4). Parece pues que la “*privacy*” no delimita

(2) Al respecto Vid. Morales Prats, F., *La tutela...*, op. cit., pp. 16 ss.; Pérez Luño, A.E., *Nuevas tecnologías: sociedad y derecho*, Madrid, 1987, p. 125; Matteucci, N., “Introduzione pubblico e privato”, en *Privacy e banche dei dati*, AA.VV., Bologna, 1981, pp. 19 ss.; Frosini, V., *L'uomo artificiale (Etica e Diritto nell'era planetaria)*, Milano, 1986, pp. 135 ss.

(3) Así Pérez Luño, A.E., op. cit., pp. 125-126.

(4) Como señala Frosini, V.: “Esto representa una nueva dimensión del “*right to privacy*”, que ya no debe ser entendido en un sentido puramente negativo, de rechazo de las intromisiones perpetradas por extraños en la vida privada, de interdicción de la difusión de informaciones sobre uno mismo, de renuncia a la participación en la vida social (“*to be let alone*”). Por el contrario, este derecho pasa a ser con-

tan sólo una esfera complementaria de libertad, del mismo modo que tampoco puede ser considerada como una *libertad-límite* —según la concepción tradicional de este concepto—. Se trata pues de un bien jurídico con proyección social y política, de ahí que en la actualidad las facultades inherentes al mismo puedan ser designadas como *libertades informáticas* (5). En cuanto tales facultades implican un derecho a *ejercer* un control sobre los datos personales informáticos, la “privacy” se erige en nuevo “*habeas*” del ciudadano, en “*habeas data*” o “*habeas scriptum*”, en definitiva en un derecho a la propia identidad informática o, como señala la más reciente literatura jurídica alemana, en un “*derecho a la autodeterminación informativa*” (6).

La tutela jurídica de la “privacy” en la sociedad in-

templado en un sentido positivo, de afirmación de la propia libertad y dignidad de la persona, de limitación impuesta por el individuo sobre el poder informático, de control activo del medio y del fin de este poder” (“Diritto alla riservatezza e calcolatori elettronici”, en *Banche dati, telematica e diritti della persona*, AA.VV. (Ed. a cargo de G. Alpa y M. Bessone), Padova, 1984, p. 33).

Sobre la evolución de la idea de “privacy” en los EE.UU. vid. Rigaux, F., “L’elaboration d’un “right of privacy” par la jurisprudence américaine”, en *Revue Internationale de Droit Comparé*, vol. XXXIII, 1980, pp. 701-730.

(5) Sobre tal concepto vid. entre otros: Frosini, V., “La protezione della riservatezza nella società informatica”, en *Privacy e banche dei dati*, op. cit., pp. 41 ss.; Id., “Die Menschenrechte in der technologischen Gesellschaft”, en *Rechtstheorie*, 1982, pp. 407 ss.; Ferri, G.B., “Privacy e libertà informatica”, en *Banche dati, telematica e diritti della persona*, op. cit., pp. 45 ss. En la doctrina española vid.: Pérez Luño, A.E., “La intimidad en la sociedad informatizada”, en *Derechos humanos, Estado de Derecho y Constitución*, Madrid, 1984, pp. 345 ss.; Morales Prats, F., *La tutela...*, op. cit., pp. 45 ss.

(6) Al respecto vid. Simitis, S., *Die informationelle Selbstbestimmung-Grundbedingung einer verfassungskonformen Informationsordnung*, NJW, 1984, pp. 398 ss.

formatizada, para quedar revestida de la necesaria racionalidad y efectividad, exige como premisa fundamental el planteamiento y tratamiento omnicomprensivo del tráfico de información en los sectores tecnológicos y de las consecuencias sociales y políticas que el mismo comporta (7). Asimismo debe establecerse una última reflexión introductoria: la dimensión informática de la "privacy" (*libertades informáticas*) trastoca de forma esencial la tradicional contraposición de los bienes de la personalidad (intimidad, honor, propia imagen...) con las libertades informativas. Si secularmente estas últimas han sido contempladas como libertades que podían entrar en tensión o conflicto con el honor o la intimidad del individuo, en el plano informático el reconocimiento del derecho de acceso al ordenador para controlar la calidad, cantidad y veracidad de los datos personales, se sitúa en la misma dirección que otros anhelos democráticos como el reconocimiento del derecho a la información en su faceta informática, esto es, el derecho de acceso colectivo a las fuentes de información tecnológicas por parte de los ciudadanos o de los grupos representativos (asociaciones ciudadanas, sindicatos, etc...) con relación a datos de interés social, económico, científico... (8).

(7) Sobre las repercusiones socio-políticas del uso de la informática vid. Vitalis, A., *Informatique, pouvoir et libertés*, París, 1981, *passim*; Simitis, S., "Auf dem Weg zu einem neuen Datenschutzrecht", en *Informatica e Diritto*, 1984, pp. 97 ss.; Morales Prats, F., *La tutela...*, *op. cit.*, pp. 33 ss. y 42 ss.

(8) Cfr. Rodota, S., "Tecnologie dell'informazione e frontiere del sistema socio-politico", en *Banche dati, telematica e diritti della persona*, *op. cit.*, pp. 89 ss.; Laudon, K.C., *Communication Technologie and Democratic Participation*, New York, 1977, *passim*; Laver, M., *Computers and Social Change*, Cambridge, 1980, *passim*; Morales Prats, F., *La tutela...*, *op. cit.*, pp. 60 ss.

Debe anticiparse ya que en nuestro país el problema relativo a la adquisición de datos personales informatizables, se afronta bien con el absoluto desconocimiento del titular de los datos —lo que ocurre la mayoría de las veces— bien bajo la lógica de la “*mitificación del consentimiento*” del titular de la información. Según esta filosofía del problema, la adquisición de datos personales por parte de centros informáticos públicos y privados constituiría una cuestión “*inter partes*”, en la que no debe interferir el Estado a través de la reglamentación jurídica. Ya a comienzos de la década de los años setenta fue ampliamente denunciado este planteamiento de la informatización de datos personales (9). La privatización del problema analizado deja traslucir las contradicciones o los oscuros designios de la *ratio* intervencionista del Estado, pues mientras para legitimar la acumulación informática de datos personales de los ciudadanos los poderes públicos apelan a la necesidad de mejorar las prestaciones de servicios públicos e incluso de fortalecer la “seguridad pública”, el propio Estado postula la renuncia a la hora de instaurar otras medidas intervencionistas encaminadas a la salvaguardia y garantía de los derechos y libertades de los ciudadanos frente al uso descontrolado del ordenador. En suma, los intereses económicos que subyacen en tal entendimiento de la cuestión y las graves consecuencias políticas y sociales que podía comportar, llevaron a la práctica totalidad de los Estados de la Europa occidental a desarrollar una política intervencionista sobre la circulación de datos personales informatizables o informati-

(9) Vid. Rodota, S., *Elaboratori elettronici e controllo sociale*, Bologna, 1973, pp. 45 ss.

zados. Sintéticamente pueden reseñarse los siguientes patrones intervencionistas (10):

1º) Establecimiento de un marco legal, regulador de la recogida y tratamiento informático de los datos personales.

2º) Creación de organismos o comisiones públicas independientes (por ejemplo en Suecia) o bien consultivas del Parlamento (por ejemplo en la República Federal Alemana) con el fin canalizar las tareas inspectoras sobre los bancos de datos, de presentar informes y memorias a las asambleas parlamentarias y a los Gobiernos, etc... (11).

(10) Para un planteamiento en extenso sobre los distintos modelos de tutela vid. Alpa, G., "Privacy e Statuto dell'informazione", en *Banche dati, telematica...*, op. cit., pp. 193 ss., donde se aborda un estudio comparado del sistema norteamericano (introducido por la "Privacy Act" de 1974) con los sistemas continentales. En particular sobre el sistema norteamericano vid. *Legislative History of the Privacy Act of 1974*, S. 3418 (Public Law 93-579), Source book on Privacy, Committee on Government Operations, House of Representatives (Subcommittee on Government Information and Individual Rights), Washington, septiembre, 1976 (esta obra incluye la del proceso de génesis legislativa, la literatura jurídica más relevante sobre la "Privacy Act" y un extenso apéndice bibliográfico). En general sobre los patrones intervencionistas en este ámbito, a la vista de la experiencia de la legislación comparada en la última década vid. Morales Prats, F., *La tutela...*, op. cit., pp. 45 ss.

(11) Sobre este punto vid. Bing, J., "The Ombudsman and Computerized Administration", en *Informatica e Diritto*, 1984 (núm. 3), pp. 83 ss. En particular sobre la figura del Comisario Federal de datos en la Bundesdatenschutzgesetz (BDSG) de 1977 en la RFA vid.: Dammann, U., en Simitis, S.-Dammann, U.-Mallann, O.-Reh, H.J., *Kommentar zum BDSG*, § 17 (pp. 563-578), § 18 (pp. 579-586), § 19 (pp. 587-606), § 20 (pp. 607-613), y § 21 (pp. 615-623), 3. Aufl., Baden-Baden, 1981 (en los citados parágrafos se regula la situación jurídica del *Bundesbeauftragter für Datenschutz*, sus funciones y el sistema de reclamaciones y recursos). En la literatura alemana al respecto vid. también: Dammann, U., *Datenschutzkontrolle, Bericht aus der Praxis*

3º) Regulación de los sistemas de seguridad en los bancos de datos y de los códigos de deontología profesional en el ámbito informático.

Por lo que respecta al primer punto, el establecimiento de un marco legal, deben concretarse algunos aspectos. Una adecuada regulación del tratamiento informático de datos personales, debe afrontar los siguientes puntos (12):

a) Reconocimiento y delimitación del principio de interdicción para la informatización de determinados datos personales sensibles, que integran el denominado “*núcleo duro de la privacy*”.

b) Establecimiento de un sistema de autorización para la creación de bancos de datos personales, que puede consistir en la necesidad de licencia previa y/o inscripción en un registro público al efecto. De este modo, se pueden asentar medidas preventivas más allá de las meras respuestas jurídicas (administrativas, civiles o penales) “*a posteriori*” para las violaciones de la legislación protectora de datos personales.

c) Reconocimiento de las libertades informáticas, que se concretan en un derecho al control sobre los datos personales informatizados (facultades de acceso individual a los bancos de datos, que implican a su

eines Landesbeauftragten für den Datenschutz, IBM-Nachrichten, núm. 236, 1977, pp. 188 ss.; Schimmel, W., “Die institutionelle Kontrolle des Datenschutzes nach den Datenschutzgesetzen der Länder”, en *Datenschutz und Datensicherung (DuD)*, 1979, pp. 25 ss. Sobre el sistema establecido en Francia vid. Holleaux, A., “La loi du 6 janvier 1978 sur l’informatique et les libertés”, en *Revue Administrative*, 1978, p. 33.

(12) Sobre tal esquema en extenso vid. Morales Prats, *La tutela...*, op. cit., pp. 48 ss. y 65 ss.

vez la posibilidad de cancelar, rectificar o agregar datos, y en facultades de control sobre el destino de la información personal). Estas medidas deben verse complementadas con un sistema de notificación de los datos personales automatizados.

II. Los poderes públicos en España todavía no han definido una política en torno al uso de la informática y la protección de datos personales. En consecuencia, no ha sido adoptada medida alguna de las anteriormente reseñadas y que, como hace algunos años indiqué debían significar el "*pacto entre tecnología y libertad*" (13).

Tras una década de vigencia de la Constitución de 1978 resta por desarrollar el art. 18.4 CE, que contiene una importante previsión de política legislativa en materia de derechos fundamentales (14). La interpretación del referido precepto no es pacífica. Para algún comentarista de la Constitución se trata de un mero "corolario" del inciso primero del propio art. 18.1 CE (15) "a todas luces innecesario". Tal interpretación parece a todas luces insostenible, tan sólo el desconocimiento de las posibilidades de control sobre los ciudadanos que ofrece la informática puede llevar a postular la innecesariedad del precepto (16). Por

(13) Morales Prats, F., *Privacy y Reforma Penal...*, op. cit., p. 579.

(14) El art. 18.4 CE dice así: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

(15) Alzaga Villaamil, O., *Comentario sistemático a la Constitución Española de 1978*, Madrid, 1978, pp. 209-210.

(16) En este sentido vid. Basile, S., "Los valores superiores, los principios fundamentales, y los derechos y libertades", en *La Constitución de 1978 (estudio sistemático)*, ed. a cargo de Predieri, A.-García Enterría, E., Madrid, 1980, p. 290.

otro lado, como indica Basile, el art. 18.4 CE no puede constituir un mero corolario del reconocimiento de los derechos a que alude el inciso primero, pues cuanto menos el legislador constitucional establece la reserva de ley para regular el uso de la informática por un lado, y alude al pleno ejercicio de los derechos de los ciudadanos por otro (17). A lo anterior cabe añadir que estamos ante una “cláusula constitucional de advertencia” sobre los peligros que puede suscitar el uso descontrolado de la informática para las libertades y los derechos fundamentales.

No obstante, se debe reconocer la oscuridad del art. 18.4 CE por lo que respecta a la expresión “pleno ejercicio de sus derechos”. En este punto la técnica legislativa empleada es imprecisa. A mi juicio, es acertada la disyuntiva interpretativa que formula Garzón Clariana (18): o se entiende que la limitación del uso de la informática —en el contexto del art. 18 CE— se limita al pleno ejercicio de los derechos en el ámbito privado que definen los bienes de la personalidad, o bien la esfera de derechos garantizados se circunscribe a aquellos que explícitamente reconoce la Constitución, soslayando en esta última opción interpretativa el marco contextual del precepto (ámbito de los bienes de la personalidad). En mi opinión, el legislador constitucional ha querido reconocer y resaltar la proyección social y política de los bienes de la personalidad en su dimensión informática. En especial “*la privacy informática*” constituye un derecho que, a su vez, es *presupuesto*

(17) Basile, S., *op. cit.*, pp. 290-291.

(18) Garzón Clariana, G., “La protección jurídica de datos de carácter personal”, en *Rev., 1ª Instancia*, núm. 2 (marzo), 1982, p. 12.

para el ejercicio de otros derechos y libertades constitucionales. En este sentido, la “privacy” dibuja una nueva dimensión de la libertad personal en la sociedad tecnológica (19). De ahí que las facultades de control sobre los datos personales informáticos queden configuradas como “*libertades informáticas*”, cuyo significado desborda el contenido y ámbito del clásico derecho a la intimidad, definido secularmente como derecho o libertad *límite* del que derivan facultades de *exclusión* en el ámbito privado.

Ciertamente el legislador constitucional podría haber optado por una formulación más explícita en el reconocimiento de las libertades informáticas, según el modelo que ofrece la Constitución portuguesa de 1976, que en su art. 35 garantiza el derecho al control sobre los datos personales informáticos y prohíbe la atribución de un número nacional único a los ciudadanos. No obstante, la imprecisión técnica del art. 18.4 CE no debe impedir una interpretación progresiva en el sentido apuntado. A ello debe añadirse que la falta de una declaración constitucional explícita sobre la privacy informática, no ha sido obstáculo para que en la mayoría de los países de la Europa Occidental se haya desarrollado una política legislativa de tutela de las libertades informáticas, en muchos casos a partir de principios o declaraciones constitucionales genéricas sobre la dignidad humana o el derecho al libre desarrollo de la personalidad. Tal

(19) Como señala Frosini, V. (*L'uomo artificiale*, op. cit., p. 132): “La libertad informática representa una nueva forma de desarrollo de la libertad personal... Esta libertad consiste en la “libertad de informarse”, esto es, de ejercitar un control autónomo sobre los datos informáticos que pertenecen a uno mismo, sobre la propia “identidad informática”, al igual que existe el derecho a la tutela de la propia integridad física y moral”.

es el caso de la República Federal Alemana; la Ley Fundamental de Bonn no contiene el reconocimiento expreso y autónomo del derecho a la intimidad a diferencia de cuanto acontece en nuestra Constitución con el art. 18 CE. De este modo, la elaboración del derecho a la intimidad por parte de la doctrina y la jurisprudencia (en especial del Tribunal Constitucional alemán), ha partido del derecho a la dignidad humana (*"Würde des Menschen"*) reconocido en el art. 1.1 de la *"Grundgesetz"* y del derecho al libre desarrollo de la personalidad (*"freie Entfaltung der Persönlichkeit"*) reconocido asimismo en el art. 2.1 de la GG alemana (20); este ejemplo ilustra cómo una normativa constitucional, en principio explícitamente menos ambiciosa que la española con relación a la limitación del uso de la informática, ha posibilitado un amplio desarrollo jurisprudencial y legislativo cara a la tutela de los datos personales (*"Datenschutz"*). En este punto debe mencionarse la *Bundesdatenschutzgesetz* (BDSG) —Ley Federal de Protección de Datos de fecha 27-I-1977 (21)— y, por lo que res-

(20) Sobre tal construcción referida a la tutela de datos que contempla la BDSG vid. Reh, H.J., en Simitis-Dammann-Mallmann-Reh, *Kommentar zum BDSG*, op. cit., § 1, pp. 95-96; Bull, H.P., "Zur verfassungsrechtlichen Verankerung des Dateenschutz", en *Öffentliche Verwaltung und Datenverarbeitung (OVD)* 11/1979, pp. 3 ss.; Rüpke, G., *Der verfassungsrechtliche Schutz der Privatheit*, Köln, 1976, pp. 73 ss.; Auernhammer, *Bundesdatenschutzgesetz, Kommentar*, Köln usw. 1977, § 1 Rdnr. 2.

La doctrina relativiza la necesidad de un reconocimiento explícito y especial de la protección de datos como derecho fundamental en la Constitución (GG), al respecto vid. Reh, H.J., op. cit., § 1 Rdnr. 4g (p. 96); Simitis, S., "Datenschutz als Bürgerschutz", *OVD* 3/1979, pp. 3 ss.; Schweinoch, J., "Fortschritte im Datenschutz", en *Wirtschaft und Verwaltung (WiVerw)*, 1980, pp. 1 ss.; Klopfer, M., *Datenschutz als Grundrecht*, 1980, pp. 37 ss.

(21) Vid. traducción al castellano de la BDSG en *Informática (Le-*

pecta a la jurisprudencia, la Sentencia del Tribunal Constitucional Federal (*Bundesverfassungsgericht*) de la RFA de 14 de diciembre de 1983, por la que se declara parcialmente contraria a la GG la Ley del Censo de Población (*Volkzählungsgesetz*) de 4 de marzo de 1982 (22). En esta sentencia el *Bundesverfassungsgericht* señala que el desarrollo de perfiles informáticos de la personalidad del individuo, acaban por convertir al ciudadano en un “*hombre de cristal*” (23), por lo que el Tribunal señala la necesidad de tutelar la intimidad en su faceta informática como expresión de un derecho a la autodeterminación informativa (*Recht auf informationelle Selbstbestimmung*), fundamentado todo ello en el principio básico del ordenamiento jurídico asentado por la GG: la dignidad de la persona (24). Esta argumentación puede trasladarse a la normativa constitucional española que, amén de la existencia del

yes de protección de datos), Documentación Informática, núm. 2, Servicio Central de Informática, Presidencia del Gobierno-Secretaría General Técnica, Madrid, 1977, pp. 35 ss.

(22) Vid. la referida sentencia del *Bundesverfassungsgericht*, en *BVerfGE* (“*Entscheidungen des Bundesverwaltungsgerichts*”), vol. 65, pp. 1 ss. Existe traducción al castellano en *BJC*, 1984, núm. 33, pp. 126 ss. (Trad. de Daranas, M.).

(23) *BJC*, núm. 33, 1984, pp. 137-138.

(24) Vid. Sentencia sobre la *Volkzählungsgesetz*, *BJC*, cit., p. 152. Sobre tal interpretación vid. Simitis, S., “Die informationelle Selbstbestimmung-Grundbedingungen einer verfassungskonformen Informationsordnung”, *NJW*, 1984, pp. 398 ss.; Schneider, H., “Anmerkung zum Urteil”, en *DOV* (*Deutsche Öffentliche Verwaltung*), 1984, pp. 161 ss.

En la referida sentencia el “*Bundesverfassungsgericht*” no sólo tuvo en cuenta las alegaciones de los demandantes (el recurso fue entablado por el movimiento de los “*Grünen*”), sino también las valoraciones vertidas sobre la Ley del Censo por el Comisario Federal de datos (Dr. Baumann) y por los Comisarios de datos de los “*Länder*”. A la vista de todo ello el Tribunal Constitucional alemán decretó la inconstitucionalidad de la citada ley.

art. 18 CE, contempla la dignidad de la persona como fundamento del orden político y la paz social (art. 10.1 CE) (25).

Un último aspecto debe abordarse con relación al tratamiento que la Constitución otorga al control sobre los datos personales. El art. 105 b) CE establece otra previsión de política legislativa que afecta al acceso de los ciudadanos a determinadas fuentes de información (26). A mi juicio, el art. 105 b) CE contiene una concreción del derecho a recibir información, contemplado en el art. 20.1 d) de la CE, de forma que debe vincularse con las facultades de *acceso colectivo* a los archivos o registros administrativos que, en definitiva, constituyen fuentes de información de carácter público, entre las que cabe incluir las de carácter informático (27). El precepto constitucional analizado merece una doble crítica: en primer lugar por su ubicación dentro del Título IV de la CE, dedicado al Gobierno y la Administración; hubiera sido, a todas luces, más aconsejable su inclusión en el capítulo relativo a los derechos fundamentales y las libertades públicas y, en particular, en el art. 20 CE. En segundo lugar, por su limitación

(25) En torno al principio de dignidad humana como fundamento de los derechos y libertades constitucionales (art. 10.1 CE) y a una interpretación articulada de éstos con los principios constitucionales, Morales Prats, F., "Adecuación social y tutela del penal del honor: perspectivas despenalizadoras", *CPC* (en prensa).

(26) Al respecto vid. Sáinz Moreno, F., "El acceso de los ciudadanos a los archivos y registros administrativos", *REDA*, núm. 24, pp. 120 ss.; Parada Vázquez, "Comentario al art. 105", en *Comentarios a la Constitución*, t. VIII, Madrid, 1985, pp. 316 ss. Vid. asimismo STS de 16 de octubre de 1979 (*Ar. 3369*) y S. del Tribunal Constitucional de 8 de junio de 1981.

(27) Sobre la fundamentación de tal interpretación vid. en extenso, Morales Prats, F., *La tutela...*, *op. cit.*, p. 102.

objetiva; en efecto, la previsión legislativa se establece con relación a archivos y registros de carácter público, parece pues que de la futura normativa deben quedar excluidos los de carácter privado.

En resumen, pues, el ordenamiento español carece en la actualidad de una ley de protección de datos personales informáticos, al no haberse colmado las previsiones del art. 18.4 CE. En esta situación de vacío legislativo, el Gobierno español procedió, en marzo de 1984 (27 bis), a la ratificación del Convenio para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal, adoptado por el Comité de Ministros del Consejo de Europa el 22 de septiembre de 1980 y abierto a la adhesión de los Estados miembros a partir del 18 de enero de 1981.

El referido Convenio no está concebido como un tratado "*self-executing*" (28), pues en el art. 4º del mismo, precepto ubicado en el Capítulo destinado a los "Principios fundamentales para la protección de datos", se obliga a las partes firmantes a adoptar en su respectivo derecho interno las medidas legislativas y administrativas pertinentes para el efectivo cumplimiento de los principios garantizadores básicos para la protección de datos personales que enuncia el Convenio internacional (29). En particular,

(27 bis) B.O.E. 15 de noviembre de 1985.

(28) Al respecto, Garzón Clariana, G., "La protección de los datos personales y la función normativa del Consejo de Europa", separata de la *Revista de Instituciones Europeas*, Madrid, 1981 (núm. 1), pp. 14 ss.

(29) Son principios básicos del Convenio: 1) Lealtad y licitud en la recogida, elaboración y utilización de los datos conforme a los fines declarados (art. 5); 2) Delimitación de datos sensible, no informatizables ("nucleo duro de la privacy") (art. 6); 3) Necesidad de medidas

precisa el apartado segundo del analizado art. 4º que, como máximo, tales medidas deberán ser adoptadas en el momento de entrada en vigor de la Convención en el país firmante. Como fuere que el Parlamento español no ha procedido al desarrollo del art. 18.4 CE y de las medidas institucionales que el mismo comporta, el Convenio del Consejo de Europa carece de efectividad en nuestro derecho interno. Cabe precisar que el Ministerio de la Presidencia del Gobierno español presentó, en junio de 1984, un borrador de propuesta de anteproyecto legislativo en desarrollo del art. 18.4 CE a un congreso de expertos celebrado en Madrid. Las críticas que recibió el referido borrador (elaborado con absoluto sigilo gubernamental, pues nunca fue publicado) por sus deficiencias técnicas, pudiera constituir uno de los motivos de su posterior retirada (30). Desde 1984 y hasta la fe-

técnicas y administrativas de seguridad en los sistemas informáticos (art. 7); 4) Reconocimiento y tutela del "*habeas data*" (art. 8); 5) Limitaciones a la tutela de los datos personales en atención a otros valores de la sociedad democrática (art. 9).

(30) El borrador de Anteproyecto fue elaborando un grupo de trabajo compuesto por funcionarios, parlamentarios e informáticos. Posteriormente fue distribuido a los subsecretarios para informe previo al envío a Consejo de Ministros; el nuevo texto en el que se recogían las observaciones de los subsecretarios fue presentado al coloquio celebrado los días 13 y 14 de junio en Madrid bajo el patrocinio conjunto del Consejo de Europa y la Secretaría de Estado para la Administración Pública (cfr. para más amplia información al respecto, Heredero Higuera, M., "La informática y el uso de la información personal", en *Introducción a la Informática Jurídica*, AA.VV. (ed. a cargo de Rivero, A.M.-Santodomingo, A.), Madrid, 1986, pp. 42-43).

El Anteproyecto, recogiendo la desafortunada técnica del art. 18.4 CE) se denominaba la "Ley Orgánica de regulación del uso de la informática para proteger los datos personales". El Anteproyecto en la versión de junio de 1984 (se ignora en la actualidad el estado de la cuestión) se estructuraba en dos partes: en una se regulaban los prin-

cha se carece de noticias en torno a una futura legislación relativa a la protección de datos informatizados. No obstante en la década de los años ochenta ha acontecido en España un desarrollo vertiginoso e incontrolado de la informatización de datos tanto en el sector público como en el privado. El ciudadano desconoce en la actualidad qué datos sobre su persona han sido informatizados por las administraciones públicas y por los bancos de datos de carácter privado (31). No obstante, la ratificación del

cipios que debían regular la recogida y uso de los datos personales; en otra se establecía la regulación del derecho de acceso, rectificación y cancelación de datos. El texto acogía también la figura del responsable del fichero, persona que decide sobre el contenido y uso del fichero de datos personales, con lo que se pretende establecer un principio de distribución de responsabilidades entre quien ejerce la función decisoria y de dirección del banco de datos y aquellas otras personas que realizan la tarea de operador en las terminales. El Anteproyecto, a diferencia de lo que acontece con la mayoría de las leyes europeas, no contemplaba un régimen de autorizaciones o licencias para la explotación de ficheros informáticos, aspecto criticable; el texto se limitaba a exigir una notificación.

(31) Amén del amplio desarrollo de la informatización de datos personales en la Administración pública y en las empresas privadas españolas, debe señalarse especialmente el ambicioso plan, impulsado por el Ministerio de Economía y Hacienda, de un gran banco de datos fiscales de ámbito estatal sobre el que reina total incertidumbre sobre los datos que va a contener. Asimismo el uso descontrolado de la informática puede suscitar problemas con relación a los censos. Junto a ello, como señala Heredero (*op. cit.*, p. 46) en nuestro país se han verificado múltiples encuestas entre la población estudiantil y otros colectivos que en gran número de casos serían ilícitas a la vista del Convenio del Consejo de Europa sobre protección de datos personales informáticos. En el Ministerio del Interior también se ha producido una importante informatización de datos ante el desconocimiento total del ciudadano (al respecto vid. Morales Prats, F., "Informatización de datos en el Ministerio de Interior", *El País*, 7-4-1984, p. 15).

Después de la firma del referido Convenio de Europa, el Estado español ha incumplido los plazos fijados (arts. 4 y 22 del Convenio) para la adopción de medidas internas que posibiliten la vigencia del acuerdo

mencionado Convenio del Consejo de Europa sobre protección de datos personales reviste, pese a la falta de adopción de medidas internas que lo hagan directamente aplicable en nuestro país, una cierta trascendencia jurídica. Al amparo del art. 10.2 CE, el citado Convenio internacional debe informar la interpretación de los derechos y libertades que la Constitución de 1978 reconoce. Este parece un argumento decisivo que respalda la interpretación que con anterioridad efectué sobre el art. 18.4 CE. A la vista de los principios fundamentales para la protección de datos personales que expresa el Convenio internacional (32), puede afirmarse que la cláusula del art. 18.4 CE constituye el refrendo constitucional de las *libertades informáticas* (derecho a la “*privacy informática*”).

Con el fin de completar el panorama legislativo español en la materia, puede anticiparse ya que el Código Penal, en consonancia con la carencia de una ley de protección de datos personales informáticos, no contiene referencia alguna a los delitos informáticos contra la “*privacy*”. La protección de tales datos sólo es contemplada por la Ley Orgánica 1/1982 de 5 de mayo de Protección Civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, en el Capítulo de Disposiciones transitorias, cuestión que será abordada con detenimiento en ulteriores epígrafes.

internacional en nuestro país. Al desprestigio que supone el incumplimiento de tales obligaciones internacionales, deben sumarse los graves problemas que se pueden suscitar en el caso, por ejemplo, de que un ciudadano extranjero pretenda hacer uso en España de los derechos que le concede el Convenio (cfr. sobre este punto Heredero, *op. cit.*, p. 45).

(32) Vid. *supra* nota 29.

III. En los siguientes epígrafes se abordará la problemática jurídico-penal de las libertades informáticas en nuestro ordenamiento y en las perspectivas de reforma legislativa, que han suscitado el Proyecto de Código Penal de 1980 (PrCP) y la Propuesta de Anteproyecto de Nuevo Código Penal de 1983 (PANCP).

A mi juicio la problemática jurídico-penal que plantea en los últimos tiempos la criminalidad informática, debe ser abordada a partir del esclarecimiento y delimitación de lo que se desea tutelar, esto es los datos informáticos. Esta reflexión debe presidir el análisis de las respuestas que frente a estas nuevas formas de criminalidad, ofrece el CP vigente y los proyectos legislativos antecitados, tanto por lo que respecta a informaciones relevantes en la esfera de los bienes de la personalidad como a datos con trascendencia económico-patrimonial. Este planteamiento permite, a mi entender, poner al descubierto en su justa medida las carencias que presentan en esta materia los tipos penales vigentes, bien por lo que respecta a la tutela de la libertad personal bien en lo atinente a la protección del patrimonio. Lo anterior supone que el criterio para detectar posibles lagunas en nuestro ordenamiento penal, no se centre exclusivamente en los nuevos medios comisivos que ha introducido la informática (33); efectivamente la distinción entre fases de manipulación "input" y "output", entre manipulación en sentido estricto y otros medios comisivos como el sabotaje, el espionaje o el denominado "hurto de tiempo" es fundamental

(33) Sobre tal planteamiento con relación a los delitos patrimoniales vid. Corcoy, M.-Joshi, U., "Delitos contra el patrimonio cometidos por medios informáticos", *Revista Jurídica de Catalunya*, núm. 3, 1988, pp. 681 ss.

para comprender los nuevos problemas jurídico-penales que suscita el uso del ordenador, pero todo ello requiere la previa reflexión sobre los bienes jurídicos que se pretende proteger en la esfera penal.

IV. La tutela penal de las libertades informáticas del individuo ha sido contemplada en el PrCP de 1980, que no llegó a ser presentado al debate parlamentario, y por la PANCP presentada por el Ministerio de Justicia en 1983, cuyo proceso de génesis legislativa se halla en la actualidad paralizado. El PrCP de 1980 preveía el art. 199 la represión penal del uso ilícito de la informática en el capítulo de delitos relativos al descubrimiento y revelación de secretos y a los atentados a la intimidad personal y familiar (34). Posteriormente la PANCP de 1983 reprodujo en su art. 189 la redacción que acogía el PrCP de 1980, con una única modificación, la sustitución del verbo “faltar” por el de “infringir” con relación a las prescripciones legales sobre el uso de la informática. Por otro lado en la PANCP de 1983 el referido delito informático pasaba a ubicarse en un capítulo destinado a los delitos contra la intimidad personal y familiar; esta última novedad con respecto al PrCP de 1980 reviste, a mi juicio, cierta trascendencia como después se expone.

(34) El art. 199 PrCP 1980 dice así: “El que, faltando a las prescripciones legales sobre el uso de la informática, grabare datos relativos al honor o a la intimidad personal o familiar de terceros, o en perjuicio de los mismos manipulare la información legítima o ilegítimamente procesada, será castigado con la pena de arresto de doce a veinticuatro fines de semana y multa de seis a doce meses, siempre que el hecho no constituya delito más grave.

Se impondrán las penas superiores en grado si se divulgare la información obtenida”.

Si bien el PrCP 1980 y la PANCP 1983 merecen una primera valoración positiva por haber advertido las graves lagunas imperantes en nuestro ordenamiento con relación a la "*privacy informática*", el análisis pormenorizado de ambos textos por lo que atañe al referido delito informático, no está exento de reflexiones críticas. Efectuaré el análisis de forma conjunta, pues como se ha indicado el art. 199 PrCP 1980 y el art. 189 PANCP 1983 adoptan una configuración prácticamente idéntica.

1º) Por lo que afecta al planteamiento *sistemático* con que se afronta la tutela de datos personales, debe destacarse que se ha optado por la inclusión de un *único* artículo dedicado al uso ilícito de la informática en menoscabo de las libertades informáticas ("*habeas data*"). El precepto se ubica en el Título II del Libro II, relativo a los delitos contra la libertad y seguridad en las relaciones entre particulares, concretamente en el Capítulo VI dedicado al descubrimiento y revelación de secretos y a los atentados contra la intimidad personal y familiar, por lo que afecta al PrCP 1980. Idéntico planteamiento sistemático está presente en la PANCP 1983, si bien en ésta los delitos contra la intimidad adquieren rango de Título independiente (Título VII) en el Libro II. En ambos casos se despreció un planteamiento más ambicioso, y a mi entender más correcto, en el plano técnico y político criminal. En este sentido, más pertinente parece un planteamiento sistemático tridimensional de estos delitos: se hace precisa pues la diferenciación de tres ámbitos de relación en los que las libertades informáticas y el uso ilícito de la informática asumen distinto significado político y jurídico. Jun-

to a las infracciones informáticas contra la privacy perpetradas por particulares, debe instituirse la tutela de este bien jurídico en cuanto garantía jurídico-política en el plano de las relaciones individuo-Estado, terreno en el que privacy informática se configura como "*habeas data*" en sentido estricto del ciudadano. De este modo, debe postularse la creación de delitos, perpetrados por funcionarios públicos, contra el "*habeas data*" del ciudadano dentro del capítulo relativo a los delitos atinentes al ejercicio de derechos fundamentales y libertades públicas (35). Asimismo, en un tercer plano, el de las relaciones de servicios públicos entre las administraciones públicas y el ciudadano, debe procederse a la inserción de modalidades típicas relativas a atentados contra las libertades informáticas. La ubicación adecuada de estas últimas figuras, de acuerdo a la sistemática del Libro II que presentan el PrCP 1980 y la PANCP de 1983, la ofrecería el Título relativo a los delitos contra la Administración pública.

Si el vigente CP otorga un triple tratamiento a aspectos de la intimidad de las personas plasmados documentalmente (tutela de secretos documentales y de correspondencia) en los arts. 497, 192 y 368, respectivamente (planteamiento sistemático que se reitera en el PrCP 1980 y la PANCP 1983 (36)), atendiendo a las distintas esferas de relación en que se produce la infracción penal, no se encuentran razones que permitan postular un tratamiento sistemá-

(35) Sobre esta propuesta sistemática en tres ámbitos de relación vid. Morales Prats, F., *Privacy y Reforma penal*, op. cit., p. 627.

(36) Vid. arts. 196, 469, 613 PrCP 1980; arts. 187, 395, 396 y 547 PANCP.

tico diverso en la tutela penal de los datos personales informáticos.

Obviamente esta propuesta no debe albergar un significado meramente sistemático. La protección penal de las libertades informáticas, en cada uno de los tres planos de relaciones reseñados, debería diversificarse por lo que respecta a las modalidades típicas en función de los peligros que ofrece el tratamiento automatizado de datos en cada uno de los mismos. Asimismo, por imperativo del principio de proporcionalidad (37), las penas imponibles en cada ámbito de relación deberán ajustarse a la entidad del injusto penal, que podrá adquirir una significación y trascendencia diversas según se trate de relaciones entre particulares, relaciones políticas individuo-Estado, o de relaciones de servicio ciudadano-Administración pública.

2º) Como antes quedó apuntado, la PrCP 1980 ubicaba el delito informático contra la "privacy" en el Capítulo VI del Título II ("Delitos contra la libertad y seguridad") del Libro II, que adoptaba la rúbrica "Del descubrimiento y revelación de secretos y de los atentados a la intimidad personal y familiar". Parece por tanto que en el Proyecto se retomaba la fórmula del CP vigente (Cap. VII, Tít. XII CP), a

(37) Sobre el principio de proporcionalidad en sentido estricto vid. Cobo del Rosal, M.-Vives Antón, T.S., *Derecho Penal. Parte General*, 2ª ed., Valencia, 1987, que sobre el particular señalan: "Es evidente que la proporcionalidad así entendida, dada la función de tutela del orden jurídico que a la pena corresponde, ha de atender, en primer término, a la gravedad del delito cometido, esto es, al contenido de injusto, al mal causado y a la mayor o menor reprochabilidad del autor. La pena proporcionada a la gravedad del delito será también, en abstracto, la adecuada a la finalidad de tutela" (p. 65).

la que se añadía la referencia a los atentados a la intimidad personal y familiar, probablemente por influencia de la declaración constitucional del art. 18 CE. En cambio en la PANCP el referido delito pasa a ubicarse en el Título VII (“Delitos contra la intimidad”) del Libro II, concretamente en el Cap. I del mismo (“Delitos contra la intimidad personal y familiar”). En mi opinión, la desaparición en la rúbrica de la referencia a los “*secretos*” me parece positiva, pues tal alusión tan sólo alude a un concepto instrumental (38), que en último término no hace más que enturbiar la elucidación del verdadero objeto jurídico de protección. En este sentido, si lo que se tutelan son exclusivamente “*secretos*”, puede abrirse el camino para interpretar que lo protegido penalmente son facultades de exclusión *de carácter formal* (39), tras las cuales puede cobijarse tanto la tutela de aspectos relativos a la intimidad como al patrimonio. Es por ello que la nueva rúbrica de la

(38) Los secretos vienen caracterizados por su instrumentalidad en el ordenamiento jurídico; en este sentido el interés protegido no es la ocultación “*per se*” sino bienes jurídicos de diversa naturaleza (intimidad, propiedad industrial, intereses estatales, etc...). Al respecto vid. Moreno Catena, V.M., *El secreto en la prueba de testigos del proceso penal*, Madrid, 1980, pp. 93-94; Crespi, A., *La tutela penale del segreto*, Palermo, 1952, p. 42.

(39) Este entendimiento formal del bien jurídico protegido (el secreto) está muy arraigada en la legislación y la literatura de la RFA; así en la Sección 15 del StGB se titula *Verletzung des persönlichen Lebensund Geheimbereichs*; el § 202 contempla la *Verletzung des Briefgeheimnisses* (quebrantamiento del secreto epistolar o documental), el § 203 la *Verletzung von Privatgeheimnissen* (quebrantamiento de secretos de particulares perpetrado por profesionales) etc... Ello ha motivado un desarrollo doctrinal del bien jurídico en estos delitos desde una vertiente formal instrumental (el concepto de secreto), vid. por todos Lenckner, T. en: Schönke-Schröder, *Strafgesetzbuch Kommentar*, 23 Aufl. München, 1988, § 202 Rdnr. 2; § 203 Rdnr. 3.

PANCP, al aludir explícita y exclusivamente a la intimidad, esclarece el bien jurídico protegido; se alude así tan sólo a la vertiente "*material*" del bien jurídico de protección, introduciéndose así un importante factor cara a la adecuada delimitación de los tipos penales, que permite excluir de los mismos todas aquellas conductas que no atenten contra la intimidad de las personas. En definitiva, la nueva sistemática y rúbrica acogidas en la PANCP, suponen un claro avance con respecto al CP vigente y a la PrCP 1980.

3º) Las perspectivas de reforma penal por lo que respecta a la "privacy informática" (*libertades informáticas*), parece que se centran, en lo concerniente a la técnica legislativa, en la inserción de nuevos delitos en el Código Penal (así PrCP 1980 y la PANCP 1983). Si bien, como más adelante se expondrá, la opción en cuanto al instrumento legislativo a auspiciar no es tan nítida como pudiera parecer a primera vista, lo cierto es que, de forma explícita, no ha sido planteada en España la creación de una ley especial en materia de uso ilícito de la informática contra las libertades informáticas o, cuanto menos, la inclusión de tales delitos en una futura ley general de tutela de datos personales informáticos. Esta última es la opción político-legislativa adoptada por la mayoría de los países europeos; así, a título de ejemplo, la "*Datategen*" de Suecia de 1973 (reformada en 1979; arts. 20 y siguientes), la *BDSG* de la RFA de 1977 (art. 41) o la ley francesa de 1978 sobre *Informática, Archivos y Libertad* (arts. 41 y siguientes) (40).

(40) Una cuidada recopilación de textos nacionales e internacionales puede verse en *Banche dati e tutela della persona*, Camera dei deputati, Servizio per la documentazione automatica, Roma, 1981.

En favor de una u otra opción legislativa se formulan los argumentos que tradicionalmente ha acuñado la doctrina ante los procesos de incriminación de nuevas conductas que acontecen en esferas de actividad tecnológica. En favor de la inclusión de los referidos delitos informáticos en el Código penal se aduce la necesidad de preservar las *funciones preventivo-generales*, que en mejor medida desempeña el cuerpo punitivo básico (41). Desde otra perspectiva, se alega que la inserción de los delitos analizados en una ley

También se ofrece una buena información de la legislación y los proyectos internacionales en *Banche dati, telematica e diritti della persona*, op. cit. Para una completa información de previsiones penales en la legislación sobre datos informáticos, abarcando la legislación de todos los países con amplios apéndices bibliográficos, es fundamental la obra de Sieber, U., *The International Handbook on Computer Crime*, Chichester-New York-Brisbane-Toronto-Singapore, 1986.

En particular sobre la BDSG de la RFA vid., con carácter general Simitis-Dammann-Mallmann-Reh, *Kommentar zum BDSG*, op. cit., Auernhammer, H., "Das Bundesdatenschutzgesetz", *BB (Betriebsberater)*, 1977, pp. 205 ss., Id. "Aufgaben und Instrumente des Datenschutzes nach dem Bundesdatenschutzgesetz", *Zeitschrift für die gesamte Versicherungswissenschaft*, 1978, pp. 33 ss.; Dammann, U., "Erste Erfahrungen mit dem Bundesdatenschutzgesetz", *NJW*, 1978, pp. 1931 ss.; Erflog, W.-Schimmel, W., "Bundesdatenschutzgesetz-die 'Magna Carta' des Bürgers von heute?", *Demokratie und Recht* 5 (1977), pp. 124 ss.; Ehrich, H.-Kircherr, R., "Bundesdatenschutzgesetz und Landesdatenschutzgesetze", *DuD*, 1979, pp. 84 ss.; Simitis, S., "Bundesdatenschutzgesetz-Ende der Diskussion oder Neubeginn", *NJW*, 1977, pp. 729 ss.; Id., "datenschutz als Bürgerschutz", *OVD* 3/1979, pp. 3 ss.; Id., "Datenschutz: Erfahrungen und Perspektiven", *Versicherungsrecht*, 1981, pp. 197 ss.

(41) Con respecto a la situación legal en la RFA, después de la entrada en vigor de la BDSG, algunos autores postulan la opción codificadora; para ello se invocan las funciones preventivo-generales y el amplio ámbito de aplicación del § 41 BDSG (que contempla los tipos penales de la legislación especial); en este sentido ilustrativamente vid. Dammann, U., en Simitis-Dammann-Mallmann-Reh, *Kommentar zum BDSG*, op. cit., § 41 Rdnr. 1 (p. 1102).

protectora de los datos personales informáticos, que contemplara un capítulo destinado a los tipos penales en la materia, puede facilitar la *interpretación e integración de los tipos penales*, pues en este ámbito describen siempre conductas delictivas sofisticadas, referidas a una esfera de actividad tecnológica compleja (42). En este sentido, la cercanía sistemática de los preceptos penales a las cláusulas legales generales sobre la protección de datos personales informáticos (por ejemplo cláusulas que definen o esclarecen conceptos técnicos de carácter informático) redundaría en una mejor integración y delimitación de los tipos penales (43). Sin embargo, como ya se apuntó, esta opción legislativa corre el riesgo de afectar a la eficacia preventiva general de las normas penales.

(42) Así, por ejemplo en la *BDSG* la integración de los tipos previstos en el art. 41 requiere adoptar como criterio rector el bien jurídico protegido que define el § 1 *BDSG*, y el preciso contenido de la acción típica requiere acudir a los conceptos normativos que determina el § 2 (Cfr. Dammann, U., *op. cit.*, § 41 Rdnr. 2 (pp. 1102-1103). Vid. arts. 1 y 2 (este último define conceptos como “almacenar”, “comunicar”, “cancelar” datos personales etc.), en *Informática (Leyes de Protección de datos)*, *op. cit.*, pp. 35-37. En particular el § 41 *BDSG* dice:

“Acciones punibles

El que, sin la debida autorización,

1. comunicare o modificare, o

2. recuperare o se procurare a partir de archivos encerrados en depósitos adecuados,

datos referidos a personas y protegidos por la presente ley que no fueren de dominio público, será castigado con pena de privación de libertad de un año como máximo o con pena de multa.

Si el autor obrare por precio o con el propósito de procurarse a sí mismo o a otro un lucro o de causar perjuicio a otro, la pena será privativa de libertad de dos años como máximo o de multa.

El hecho sólo será perseguido a instancia de parte”.

(43) Morales Prats, F., *La tutela...*, *op. cit.*, p. 336.

4^o) Por lo que respecta el bien jurídico protegido en el art. 199 PrCP 1980 y en el art. 189 PANCP 1983, parece no ser otro que las *libertades informáticas* (“*privacy informática*”). Esta argumentación viene ratificada por la propia sistemática seguida en ambos textos. Por lo que respecta al PrCP 1980 la referencia en la rúbrica del Capítulo al descubrimiento y revelación de secretos junto a la intimidad, podría llevar a la interpretación de que no se protegen tan sólo aspectos concernientes a la esfera de los bienes de la personalidad sino también a *otros* ámbitos como el del patrimonio o la propiedad (44). Tal argu-

(44) Con referencia al ordenamiento de la RFA, junto al citado § 41 de la *BDSG*, la “Segunda Ley para la lucha contra la criminalidad económica” (2.WiKG) introdujo el delito de espionaje de datos (*Ausspähen von Daten*, § 202 a) *StGB*), que reza así: “1. El que indebidamente consiguiese para sí o para otro datos no previstos para él y especialmente protegidos contra cualquier acceso no autorizado, será castigado con pena privativa de libertad de hasta tres años o con multa.

2. Son datos, a tenor de lo dispuesto en apartado 1 sólo aquellos que están almacenados o son transmitidos de manera electrónica o magnética o de cualquier otro modo no directamente perceptible”.

Mientras que con relación al § 41 *BDSG* la doctrina vincula lógicamente la tutela de datos informáticos con los bienes de la personalidad (al respecto vid. Höft, H., *Straf- und Ordnungswidrigkeitenrecht im Bundesdatenschutzgesetz*, Köln, 1986, pp. 3 ss., quien reproduce en este ámbito la ya clásica “*Sphärentheorie*”, a través de los conceptos de “esfera privada” y “esfera de confidencialidad” —“*Vertrauensphäre*”—), el § 202 a) no incorpora referencias sobre el contenido de los datos, o los intereses que se protegen a través de los mismos (vid. Lenckner, T., en Schönke-Schröder, *op. cit.*, § 202 a) Rdnr. 1, p. 1350; Lenckner, T.-Winkelbauer, W., “Computerkriminalität-Möglichkeiten und Grenzen des 2.WiKG” (I), *Computer und Recht*, 8/1986, p. 485; Lackner, K., *Strafgesetzbuch*, 17 Aufl., 1987, § 202 a) Rdnr. 1, pp. 846-847; Schlüchter, E., *Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität*, Heidelberg, 1987, pp. 61 ss.). En este sentido el § 202 a) contendría una tutela de datos mucho más amplia que la prevista en el § 41 *BDSG* (limitada a los datos personales; para Lenckner (*op. cit.*) pese a que el derecho de disposición de da-

mentación no me parece sustentable, ya indiqué que el objeto jurídico de protección no podía quedar delimitado a través de la apelación a conceptos *formales e instrumentales* como el de secreto. Desde una perspectiva *material* el bien jurídico protegido se ubica en la esfera de los bienes de la personalidad y, más concretamente, queda constituido por las *libertades informáticas* (“*privacy informática*”). Esta interpretación se apoya además en la sistemática que adopta el PrCP 1980: el delito informático (art. 199), así como los restantes tipos penales que abarca el Cap. VI, se

tos frecuentemente se halla asociado a intereses económicos (vinculación que no es estrictamente necesaria), el § 202 a) no constituye propiamente un delito contra el patrimonio, bien jurídico este último sobre el que más se constataría un “reflejo de protección” (“*Schutzreflex*”); en cambio, Haft (“Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (Computerdelikte)”, *NSiZ*, 1987, p. 9) indica que los datos deben revestir un valor económico, por lo que se tutelaría la propiedad, argumentación que encontraría apoyo en la connotación patrimonial de la acción típica (“conseguir”). La doctrina mayoritaria intenta acercar el análisis del bien jurídico protegido en § 202 a) a las construcciones teóricas formalistas e instrumentales propuestas para el § 202 (delito de descubrimiento y revelación de secretos). Así se indica que el bien jurídico es la atribución o competencia “formal” de disposición de los datos que a modo de “señorío sobre los datos” permite determinar a quien pueden ser facilitados; pero la referida atribución formal se proyectaría sobre el contenido de los datos, de forma independiente de las relaciones de propiedad sobre el soporte de los datos (en este sentido vid. Möhrenschrager, M., “Das neue Computerstrafrecht”, *WISTR*, 1986, pp. 139-140; Lenckner, T.-Winkelbauer, *op. cit.*; Leicht, “Computerspionage-Die besondere Sicherung gegen unberechtigten Zugang (202 a) *StGB*”, *Informatik und Recht*, 1987, p. 45; en otro sentido cfr. Tiedemann, K., “Die Bekämpfung der Wirtschaftskriminalität durch Gesetzgeber”, *JZ*, 1987, p. 871).

La incorporación del § 202 a) al *StGB* vino motivada por la necesidad de cubrir las lagunas originadas por la aparición de informaciones con soporte y transmisión informática (sobre estos aspectos político criminales vid. por todos Sieber, U., *Informationstechnologie und Strafrechtsreform*, Köln-Berlin-Bonn-München, 1985, pp. 51 ss.).

incluyen en el Título II del Libro II, cuya rúbrica alude a la “libertad y seguridad”, conceptos que deben quedar referidos al ámbito de lo *personal*, lo que implica la exclusión de la tutela de intereses patrimoniales.

La tesis aquí sostenida en torno al bien jurídico protegido queda confirmada con nitidez en la PANCP 1983. En efecto, el art. 189 de la misma se halla enclavado en el Título VII del Libro II, cuya rúbrica es la de “Delitos contra la intimidad”, desterrando de forma positiva la alusión a los *secretos*; se enuncia así con carácter exclusivo la *materialidad* del bien jurídico protegido, lo que cierra el camino para incluir en el referido Título otros intereses o bienes jurídicos. Ciertamente que con respecto al delito informático (art. 189 PANCP), el concepto de intimidad no abarca —como ya apuntó la nueva dimensión de la libertad personal que constituyen las libertades informáticas (“privacy informática”), pero la rúbrica adoptada en la PANCP es aceptable. Se alude a la intimidad “*lato sensu*”, esto es, de forma que se incluyan los aspectos informáticos de la misma. A buen seguro, en la redacción de la rúbrica ha influido el contenido del art. 18 de la CE.

Ahora bien, llegados a este punto se hace precisa una importante reflexión que afecta tanto al art. 199 PrCP como al art. 189 PANCP. Ambos preceptos aluden a dos *modalidades típicas*, la grabación y manipulación de datos relativos al honor y a la intimidad personal o familiar. Más correcto hubiera sido el empleo de la expresión “*datos personales*”, pues sobre ello se proyectan las facultades que derivan del “*habeas data*” en el ciclo operativo del ordenador. Además,

no se comprende por qué en ambos casos el “pre-legislador” limita el ámbito de tutela a los datos relativos al honor o a la intimidad. Ante todo debe precisarse que es extremadamente difícil y aleatoria la delimitación de los datos que pertenecen a la esfera del honor o de la intimidad. Pero, junto a este escollo interpretativo, concurre otra deficiencia técnica más grave: en el terreno informático son datos personales sensibles no sólo aquellos que “*a priori*” puedan dar lugar a discriminaciones y, en definitiva, a atentados contra la “*privacy*”, entendida como libertad informática del individuo; otros datos personales, que en principio fuera del ciclo informático *pudieran parecer* inocuos, una vez automatizados y por combinación informática de unos con otros, pueden dar lugar a la obtención de información “*sensible*” por inferencia, o bien pueden posibilitar la creación de “*perfiles informáticos sensibles*” de un individuo (45). Por ello, la limitación objetiva de los preceptos analizados sugieren —por lo que respecta al objeto material del delito— parece injustificada y poco coherente con las posibilidades de obtención de información que ofrece la informatización de datos. En síntesis, pues, una correcta tutela penal de los datos personales automatizados no debe quedar circunscrita a los datos relativos al honor o a la intimidad; debe abarcar, por contra, todo tipo de datos personales, pues la acción típica

(45) Conviene advertir pues que la sensibilidad de las informaciones no depende sólo de su inmediata conexión con aspectos que afecten a la intimidad como de su potencial utilización en procesos que afecten finalmente a las libertades informáticas u otros derechos fundamentales (en sentido vid. sentencia del “*Bundesverfassungsgericht*” de 15-12-1983 sobre la Ley del Censo de Población, BJC, 1984, *op. cit.*, p. 154.

(grabar, manipular) debe producirse en infracción de las prescripciones legales sobre el uso de la informática. Parece que el “prelegislador”, al configurar este delito, ha confundido lo que debe ser el *objeto material del delito* (los datos personales informatizables) con el *objeto jurídico de protección* (“la privacy informática”), en el buen entendido que no son conceptos que puedan superponerse.

La referencia a los datos relativos al *honor* suscita ulteriores incertidumbres interpretativas en torno al bien jurídico protegido. Parece que el “prelegislador” ha operado con un cierto mimetismo respecto de la declaración del art. 18.4 CE. Efectivamente, en este precepto constitucional se señala que la ley limitará el uso de la informática para garantizar, en especial, el honor y la intimidad. Parece extraña la referencia al honor, pues el derecho que constituye un presupuesto de ejercicio de otros derechos (a los que también alude genéricamente el art. 18.4 CE) frente al uso del ordenador no puede ser otro que la “*privacy informática*” o “*habeas data*”. Ante la carencia en nuestro léxico oficial de una expresión equivalente a la de “*privacy*” (en el futuro pudiera ser “*privacidad*”) hubiera bastado con que el legislador constitucional se hubiera referido a la garantización de “*intimidad informática*” o, mejor aún, a las “*libertades informáticas*” de forma específica, expresión esta última que más se acerca en la actualidad a la de “*privacy informática*”. La referencia específica al honor en el art. 18.4 CE, parece así perturbadora y, en cualquier caso, la garantía de este derecho ya hubiera quedado incluida implícitamente en la referencia genérica al pleno ejercicio de los derechos de

los ciudadanos, respecto de los que —frente al uso de la informática—, sólo la “privacy” o “libertad informática” es presupuesto de su ejercicio (46).

Probablemente, la redacción del art. 18.4 CE ha pesado en la configuración de los arts. 199 PrCP y 189 PANCP respectivamente. Sin embargo, debe remarcarse que en ambos preceptos el único bien jurídico protegido es la “privacy” o “libertad informática”, pues los abusos informáticos constituyen actos de intromisión tecnológica en menoscabo de este bien jurídico. La tutela del honor “*stricto sensu*” se debe configurar frente a otro tipo de conductas atentatorias. La grabación ilícita o la manipulación informática de datos personales en todo caso puede llegar a constituir un delito precedente contra la “privacy” o “libertad informática”, que puede facilitar un *ulterior* delito contra el honor (injuria o calumnia), pero fuera ya del ámbito de actividad informática (47).

5º) En los arts. 199 PrCP y 189 PANCP se prevén dos modalidades típicas (la grabación de datos relativos al honor o a la intimidad, y la manipulación de la información legítima o ilegítimamente obtenida en perjuicio de los titulares de los datos), que se estructuran a través de una *ley penal en blanco*, pues deben producirse con infracción de las prescripciones legales sobre el uso de la informática. Por tanto, la conducta típica se completa con una remisión al ordenamiento

(46) Sobre este carácter de la “privacy informática”, vid. Morales, F., *La tutela...*, *op. cit.*, pp. 42 ss.

(47) Ni tan siquiera la amplia definición legal de injuria (art. 457 que alude no sólo a expresiones sino también a acciones, permite afirmar que “per se” el uso ilícito de la informática puede constituir un delito contra el honor.

extrapenal en materia de protección de datos personales. Lógicamente en la actualidad, caso de ser derecho vigente, las citadas previsiones no encontrarían el contexto normativo que reclaman para la determinación y complementación del tipo penal; tan sólo el Convenio del Consejo de Europa sobre protección de datos personales automatizados constituiría un asidero *interpretativo* a tal efecto y a tenor de lo que dispone el art. 10.2 CE (48).

La expresión utilizada para establecer la normativa complementaria del tipo penal en blanco (“prescripciones legales sobre el uso de la informática”) es susceptible de crítica. A mi juicio, debe interpretarse que el art. 18-4 CE prevé la *reserva de ley orgánica* (49), pues alude a una futura ley sobre el uso de la informática que afecta al ejercicio de derechos fundamentales; en este sentido, la ley penal en blanco analizada debería haber remitido al referido instrumento legislativo y no a otros, como efectivamente se constata en el PrCP y la PANCP, a través de cláusulas de remisión indeterminadas que completan el tipo penal con toda clase de “prescripciones legales sobre el uso de la informática” (50). Tal precisión es rele-

(48) Vid. *supra* nota 29.

(49) En este mismo sentido vid. Pérez Luño, A.E., *Nuevas tecnologías...*, *op. cit.*, p. 86; Heredero Higuera, M., “La informática y el uso de la información personal”, *op. cit.*, pp. 37 ss.; asimismo la Propuesta de Anteproyecto sobre la materia preveía como instrumento legislativo la ley orgánica (vid. *supra* nota 30).

(50) Sobre el sistema seguido en la *BDSG* (§ 41) vid. Dammann, U., en Simitis-Dammann-Mallmann-Reh, *BDSG*, *op. cit.*, § 41 Rdnr. 2, pp. 1102-1103. En la *BDSG* el preciso contenido de la acción típica del § 41, se debe integrar con los conceptos definidos en el § 2 de la *BDSG*, no obstante la norma penal en blanco también requiere que se acuda a otras normas complementarias diversas de la propia *BDSG* (señalando la inseguridad jurídica que ello produce vid. Zielinski,

vante en orden a la preservación de las garantías del principio de legalidad. En sentido contrario podría opinarse que el art. 18.4 CE no establece una reserva de ley orgánica; el art. 81.1 CE establece un *sistema cerrado* de ley orgánica, y podría interpretarse que, de las esferas objeto de la misma, ninguna afecta a la cláusula del art. 18.4 CE. En particular se podría argumentar que las libertades y derechos del art. 18 CE *no requieren* un “desarrollo” legislativo; en otros términos que la previsión legislativa del art. 18.4 CE no supondría un desarrollo legislativo de derechos fundamentales y libertades públicas, supuesto contemplado en el art. 81.1. CE como materia objeto de reserva de ley orgánica. Ahondando en esta línea interpretativa, sería sustentable incluso que el art. 18.4 CE ni siquiera contemplaría una reserva de ley *ordinaria*, recogida en el art. 53.1 CE; a tal conclusión llevaría la consideración de que el derecho a la intimidad *no es susceptible de ejercicio*, y como tal la regulación legal que prevé el art. 18.4 CE no podría encuadrarse en la reserva ordinaria de ley que contempla el art. 53.1 CE, puesto que en este precepto la reserva de ley ordinaria se establece para regular el “*ejercicio*” de los derechos y libertades del Cap. Segundo Título I de la CE. Finalmente, frente a la tesis aquí sustentada sobre el art. 18.4 CE, podría esgri-

D., “Das legislatorische Problem “Datenschutz” aus strafrechtlicher Sicht”, en Kilian-Lenk-Steinmüller, *Datenschutz*, Frankfurt, 1973, p. 147; Artz, G., “Die Ahndung von Verstößen gegen den Datenschutz”, en *Aktuelle Beiträge über den Datenschutz*, Schriftenreihe Schmelpfeng Band 9 (1977), pp. 133 ss.; Tiedemann-Sasse, *Delinquenzprophylaxe, Kreditsicherung und Datenschutz in der Wirtschaft*, Köln usw., 1973, pp. 121 ss. y p. 148. Vid. también en favor de una interpretación restrictiva Tiedemann, K., “Datenübermittlung als Straftatbestand”, *NJW*, 1981, pp. 946-948.

mirse un último argumento: el art. 18.4 podría encuadrarse entre aquellas cláusulas concretas de reserva de ley de la CE que, según un sector de la doctrina (51), cuya intensidad de desarrollo por ley es *menor* que la reconocida en el art. 53.1 CE; de este modo la reserva de ley concreta, expresada en el art. 18.4 CE sólo alcanzaría a las “*líneas maestras*” de la regulación sobre las libertades informáticas y el uso del ordenador, cabiendo incluso remisiones genéricas al reglamento e, incluso, la deslegalización (52).

A mi entender, las interpretaciones expuestas no son postulables por las razones que a continuación se exponen. En primer lugar estimo que *todos* los derechos fundamentales y libertades públicas recogidos en la CE son *ejercitables*, de acuerdo con una comprensión articulada de los mismos con el fundamento y los principios generales de tutela que expresa el art. 10.1 CE según he expuesto en otro lugar (53). Y especialmente las libertades informáticas (“*privacy informática*”), en cuanto *nueva dimensión de la libertad personal*, son ejercitables, pues su contenido material viene constituido por facultades de acceso al ordenador con el fin de “*ejercitar*” un derecho al *control sobre los datos informáticos* (sobre la licitud de su informatización, sobre su veracidad, sobre su circulación y destino en los circuitos telemáticos

(51) Sobre esta corriente de opinión vid. Tornos Mas, J., “La relación entre la ley y el reglamento: reserva legal y remisión normativa. Algunos aspectos conflictivos a la luz de la jurisprudencia constitucional”, *Rev. Administración Pública* (núm. 100-102), 1983, pp. 483 ss.; Villar Palasi-Villar Ezcurra, *Principios de Derecho Administrativo*, t. I, Madrid, 1982, p. 108.

(52) Tornos Mas, *op. cit.*; Villar Palasi-Villar Ezcurra, *op. cit.*

(53) Morales, F., “Adecuación social y tutela penal del honor: perspectiva despenalizadora”, *CPC* en prensa.

etc...). Es por ello que se desvanece la tesis según la cual el art. 18.4 CE no estaría afectado por la reserva de ley establecida en el art. 53.1 CE. Pero, como ya indiqué, el art. 18.4 CE contempla la reserva de ley orgánica, esto es la reserva de ley *reforzada o cualificada* (54) y no la general de ley ordinaria (art. 53.1 CE). Efectivamente la previsión del art. 18.4 CE debe conectarse con el art. 81.1 CE, pues afecta a una materia que implica el *desarrollo* de derechos fundamentales y libertades públicas. En este sentido puede indicarse que el “desarrollo” legislativo (la actuación del legislador) alcanza no sólo a derechos fundamentales de contenido prestacional sino también a los “*derechos de libertad*”; como señala García Macho: “La intervención del legislador, que en la época liberal se consideraba una injerencia en la libertad, en la actualidad ha llegado a ser un medio de garantizar esa misma libertad” (55). Ahora bien, incluso puede plantearse que las libertades informáticas del art. 18.4 CE *participan* de un cierto *contenido prestacional*, por constituir derechos fundamentales de “*tercera generación*”, en los que se constata la crisis de la vieja dicotomía entre derechos individuales y derechos sociales; en la medida que la efectiva garantía de las libertades informáticas requiere la creación de un entramado institucional por parte del Estado (creación de un registro para bancos de datos; dotación de cuerpos inspectores; sistemas de comunicación de los datos informatizados, etc...) junto a la estricta existencia de una legislación protectora al respecto, nos hallamos ante derechos que im-

(54) Al respecto vid. García Macho, R., *Reserva de ley y potestad reglamentaria*, Madrid, 1988, pp. 118 ss.

(55) García Macho, R., *op. cit.*, p. 146.

plican *también* prestaciones públicas. Valga este excurso para justificar la subsunción de la previsión legislativa del art. 18.4 CE en la reserva de *ley orgánica* del art. 81.1 CE, por lo que respecta al supuesto de “desarrollo de derechos fundamentales y libertades públicas”. No obstante, el Tribunal Constitucional ha señalado que la expresión “desarrollo” debe entenderse de forma *restringida* (56), esto es, como “desarrollo legislativo directo” o bien como *complemento legislativo indispensable* (57). Pues bien, a mi juicio, la ley prevista en el art. 18.4 CE constituye el *complemento o desarrollo indispensable* para dotar de efectividad al art. 18 CE en el ámbito informático. En otros términos, si el desarrollo legislativo de aspectos preinformáticos de los bienes de la personalidad reconocidos en el art. 18 CE (honor, intimidad, propia imagen) quedó afectado en su día por la reserva de ley orgánica (L.O. 1/1982 de 5 de mayo sobre Protección Civil de los referidos derechos), *no existen razones materiales ni formales* que determinen que otra deba ser la conclusión para el

(56) En la sentencia 6/1982 de 22 de febrero el Tribunal Constitucional señala: “el art. 81 CE se refiere al desarrollo “directo” de los derechos fundamentales, pues este artículo y las otras muchas alusiones de la Constitución al instrumento de la ley orgánica en materias concretas, que, como se ha dicho, convierte a las Cortes en constituyente permanente, no puede extremarse, con los importantes problemas de consenso interno que conlleva, al punto de convertir el ordenamiento jurídico entero en una mayoría de leyes orgánicas, ya que es difícil concebir una norma que no tenga conexión, al menos remota, con un derecho fundamental”. En la posterior sentencia 77/1985 de 27 de junio, el Tribunal Constitucional equipara “desarrollo” con el objeto mismo reservado, esto es, con el núcleo del derecho fundamental que necesariamente tiene que ser desarrollado por ley orgánica.

(57) Vid. Sentencia 76/1983 de 5 de agosto (Tribunal Constitucional).

desarrollo legislativo de las libertades informáticas, debiéndose tener en cuenta además que para este último supuesto existe una explícita previsión constitucional de desarrollo legal (art. 18.4 CE) (58).

6º) Por otro lado, debe significarse que toda opción legislativa centrada en la inclusión de los delitos informáticos contra la “privacy” en el Código Penal, aboca al empleo de *tipos penales en blanco*. De lo contrario, los tipos penales pueden quedar obsoletos en corto lapso de tiempo, o bien pueden hallar múltiples dificultades interpretativas (59). Por consiguiente, parece coherente la técnica legislativa adoptada en el PrCP 1980 y en la PANCP 1983. Sin embargo, se debería haber precisado mejor el contexto de la remisión normativa, pues no se adecúa a las exigencias del principio de legalidad y de la taxatividad típica la remisión genérica a las “prescripciones legales” sobre el uso de la informática. La técnica empleada en el PrCP y en la PANCP puede dar lugar a la incriminación de meras infracciones formales, que en todo caso deben ser sancionadas en el ámbito del derecho administrativo. De no concretarse la remisión al ámbito normativo extrapenal, pueden suscitarse también problemas de superposición normativa entre las esferas tutela penal y de administrativa. La preservación del carácter de “*ultima ratio*” del Derecho Penal debe traducirse en un adecuado “escalonamiento” de los distintos instrumentos legislativos preventivos y sancionadores (el administrativo y el penal,

(58) Sobre este tipo de cláusulas explícitas entendidas como auténticas reservas de ley a todos los efectos vid. García Macho, R., *Reserva de ley...*, op. cit., pp. 116 ss.

(59) Vid. Morales, F., *La tutela...*, op. cit., p. 336.

sin despreciar tampoco una hipotética tutela civil de los datos personales) (60) en función del grado y calidad de los peligros que se ciernen sobre las libertades informáticas en las distintas fases en que se vertebra el uso del ordenador. Como he indicado en otro lugar (61): “el escalonamiento de las facultades del *habeas data* durante el “*iter*” del ciclo operativo de los bancos de datos facilita la valoración de la entidad del peligro, o bien la constatación del peligro efectivo. Transportando las ideas de peligro y de lesión o perjuicio para el bien jurídico protegido a las distintas fases del ciclo informático, puede establecerse como criterio general que, a partir de la fase de efectiva recogida de los datos personales, son posibles violaciones o restricciones del ejercicio del “*habeas data*”, por lo que desde ese momento la intimidad puede ser puesta en peligro de manera relevante para las normas penales. Con anterioridad a las actividades de recolecta de datos, deberán actuarse las sanciones administrativas pertinentes (por ejemplo por falta de autorización o licencia), pues la anticipación de la protección penal más allá del momento indicado puede conducir a la incriminación de meras infracciones administrativas” (62).

(60) Sobre la tutela administrativa de los datos personales en la BDSG (§ 42) de la RFA, vid. Höft, H., *Straf- und Ordnungswidrigkeitenrecht*..., *op. cit.*, pp. 77 ss.

Cabe pensar en la tutela administrativa para todas aquellas cuestiones en el uso de los circuitos informáticos que requieren la intervención de la Administración para garantizar los sistemas de comunicación al afectado de los datos personales informatizados o la designación del responsable o comisario de los bancos de datos etc...

(61) Morales, F., *La tutela*..., *op. cit.*, p. 345.

(62) Es de destacar que la OCDE ha elaborado una lista de actos que podrían constituir (a modo de común denominador entre los diversos Estados) los delitos informáticos. De la citada lista (vid. OCDE-ICCP,

7º) Procederemos a continuación al estudio de las dos modalidades típicas que contienen el art. 199 PrCP 1980 y el art. 189 PANCP 1983.

a) Grabación de datos relativos al honor o a la intimidad con infracción de las prescripciones legales sobre el uso de la informática.

En primer lugar, en cuanto al tipo objetivo, debe destacarse que es difícil la delimitación típica de la conducta de grabación de datos pues reina la incertidumbre en torno al alcance de la remisión extrapenal complementadora de la norma penal. Una futura ley de datos permitiría delimitar la trascendencia de la previsión típica en el ciclo operativo de los bancos de datos (63). En todo caso, parece que quedan fuera del tipo de conductas de mera apertura de bancos de datos sin licencia o autorización (aspectos en la actualidad carentes de regulación en nuestro ordenamiento) (64), así como el funcionamiento de bancos de datos personales sin previa inscripción en el Registro (materia también

Information, Computer and Communication Policy-Series no. 10, -Computer-related crime: Analysis of legal policy, Paris, 1986, pp. 69-70), sólo alguna de las recomendaciones es referible a los datos personales, pues la citada lista parece pensada en mayor medida para la protección de datos con trascendencia económica, o para la tutela de programas informáticos comercializables.

(63) Sobre la acción típica del § 41 de la *BDSG* (comunicación, modificación, recuperación o consecución de datos personales sin la debida autorización) vid. Höft, H., *op. cit.*, pp. 20 ss.

(64) Estas conductas serían atípicas a los efectos del § 41 *BDSG* de la RFA. En cambio el ámbito de intervención penal es más amplio en la "Datalegen" de Suecia de 1973, que en su art. 20, entre otras conductas punibles, contempla la creación o explotación de archivos de personas sin la autorización debida, así como el incumplimiento de instrucciones dictadas por la Inspección de datos (vid. *Informática (Leyes de protección de datos)*, *op. cit.*, p. 31).

necesitada de reglamentación) (65), siempre claro está que todas estas *medidas preventivas* fueran en su día recogidas por la ley de protección de datos personales. También quedan fuera del tipo penal la recolecta ilícita de datos sin posterior grabación de los mismos, lo que es criticable pues a partir de ese momento en la fase operativa de los bancos de datos, a mi juicio, ya es oportuna la intervención del Derecho penal (66).

Por otra parte el tipo analizado adopta una estructura de peligro. Al respecto debe reseñarse que, con relación a la tutela de los bienes de la personalidad, la doctrina mayoritaria tradicionalmente ha venido reseñando que todo lo más puede hablarse de "*impropios delitos de peligro*" en función de la textura del bien jurídico protegido (67). Sin ser este el lugar apropiado para profundizar en la cuestión, baste con reseñar que la informática supone una esfera de actividad técnica en la que el concepto penal de riesgo

(65) Sobre los distintos sistemas de licencia previa y registro vid. Morales, F., *La tutela...*, *op. cit.*, pp. 58 ss.

(66) Tales conductas podrían quedar subsumidas en el art. 187.1 PANCP (equivalente por lo que se refiere al apoderamiento de secretos documentales o cartas para descubrirlos al vigente art. 497 CP) pero esta vía de tutela es excesivamente estrecha y no está pensada para las recogidas ilícitas de datos con fines informáticos; ello es así por dos razones: 1º) porque en todo caso los datos han de tener una plasmación en papeles o cartas; 2º) porque en todo caso el apoderamiento de los papeles o cartas ha de ser subrepticio y en las técnicas de recolección de datos personales con fines informáticos se constatan otro tipo de actuaciones ilícitas más sofisticadas. Por tanto la recogida ilícita de datos personales con fines informáticos requiere una incriminación específica, para lo que es necesario definir en el ámbito legal extrapenal la esfera de licitud en la recolecta de tales datos.

(67) Sobre ello vid. Herrmann, *Zum Begriff der Gefahr, insbesondere der Gemeingefahr im deutschen Strafrecht*, Tübingen, 1939, pp. 19 ss.

o peligro sobre la “privacy informática” es coherente con las necesidades de protección penal del bien jurídico. En consonancia con la afirmación precedente, debe tenerse en cuenta que la proyección informática de la “privacy” ha trastocado —como ya se indicó— el contenido tradicional de este bien jurídico; las libertades informáticas suponen un elenco de facultades de control sobre los datos personales de carácter preventivo con respecto a otros aspectos tradicionales de la intimidad. Ahora bien, la calificación del tipo analizado como estructura de peligro concreto o abstracto dependerá del *carácter y contenido* que, en cada caso, adopte la legislación protectora de datos personales, así como de la *calidad y sensibilidad informática de los datos* sobre los que se opere ilícitamente (68).

Por lo que respecta al tipo subjetivo cabe indicar que sólo admite la *modalidad dolosa*, pues tanto el PrCP 1980 (art. 18) como la PANCP 1983 (art. 15) adoptan el sistema de incriminación específica de las conductas culposas y en ambos textos, por lo que respecta a los delitos contra la intimidad, no se contempla cláusula alguna que preste cobertura a la incriminación de tales conductas. Sin embargo podría plantearse la incriminación de conductas culposas en este ámbito delictivo; si bien con respecto a los delitos tradicionales contra la intimidad o el honor, se ha señalado la necesidad de limitar la intervención penal a las conductas dolosas, la esfera de actividad técnica que supone el uso de la informática podría aconsejar

(68) Debe recordarse al respecto lo afirmado sobre los peligros que ofrece la informatización de datos, en principio, inocuos para las libertades informáticas, pero cuyo procesamiento y combinación informática puede constituir un peligro para el bien jurídico protegido.

la creación de tipos culposos, pues se trata de un ámbito de actuación en el que deben ser exigibles normas de cuidado y diligencia a los profesionales de la informática. No obstante, estimo que la prevención y represión de las referidas conductas debe establecerse a través de instrumentos alternativos de tutela (de carácter administrativo y civil) (69) como forma de preservar el principio de intervención mínima. La apelación a técnicas de tutela alternativas al Derecho Penal no obsta que sea postulable la regulación de las normas de cuidado en el ámbito informático a través de códigos de deontología profesional (70).

b) La segunda modalidad típica consiste en la manipulación de datos relativos al honor o a la intimidad en perjuicio de los titulares de los datos, infringiendo las prescripciones legales sobre el uso de la informática.

Los mayores problemas interpretativos surgen a la hora de interpretar la expresión “en perjuicio” que debe ubicarse en el tipo subjetivo. En un *sentido causal* la expresión analizada equivaldría a “manipular causando un perjuicio”. En cambio, en un sentido final de la misma debe ser equivalente a “manipular

(69) Sobre tales instrumentos alternativos de tutela en el § 42 de la *BDSG* vid. Höft, H., *Straf- und Ordnungswidrigkeitenrecht...*, *op. cit.*, pp. 77 ss.; Auernhammer, H., *Das Bundesdatenschutzgesetz. Kommentar*, Köln usw 1977, § 42 Rdnr. 1; Ordemann § 42 Anm. 1, en Ordemann-Schomerus, *Bundesdatenschutzgesetz*, 3 Aufl., München, 1982; Simitis, § 42 Rdnr. 1-6, en Simitis-Dammann-Mallmann-Reh, *BDSG*, *op. cit.*

En la legislación comparada, no obstante, se encuentran ejemplos de incriminación de conductas imprudentes, así en el art. 20 de la “Datalegen” sueca de 1973.

(70) Al respecto en extenso vid. Morales, F., *La tutela...*, *op. cit.*, pp. 346 ss.

para perjudicar” o “con el fin de perjudicar”. A nuestro juicio, la expresión “en perjuicio” debe ser interpretada en un *sentido final*. No puede interpretarse tampoco que dicha expresión aluda a un modalidad de la acción de manipular. Debe interpretarse pues que el referido sentido final de la expresión configura un *elemento subjetivo del tipo*, distinto del dolo, que excede de este último, y no tiene correspondencia con el tipo objetivo, en aras a fundamentar la ilicitud penal del acto. Por lo tanto, estamos en presencia de un tipo penal incongruente por exceso subjetivo (71). La adopción de esta estructura típica debe ser criticada, pues introduce una “*coloración patrimonialista*” en la conducta típica, de todo punto ajena al bien jurídico tutelado de carácter estrictamente *personal* según se expuso más arriba; en suma la tutela de las libertades informáticas queda sometida a la comprobación de un elemento subjetivo del tipo *extraño a los intereses* que se pretende proteger, lo que no hace más que crear incertidumbre interpretativa. La cuestión podría solventarse, atribuyendo un significado dogmático diverso a la expresión “en perjuicio”, que, entendida en *sentido final*, revestiría un alcance diverso en función del bien jurídico que pretende tutelar el tipo penal; se trataría de otorgar a la expresión analizada la función de concretar la exigencia de *dolo directo*, con exclusión del eventual, lo que llevaría a concluir que no se está en presencia de un elemento subjetivo del tipo distinto del dolo. Esta argumentación atendería a la sensibilidad de los datos informáticos, cuya manipu-

(71) Sobre tales estructuras típicas vid. por todos Mir Puig, S., *Derecho Penal. Parte General*, Barcelona, 2ª ed., 1985, pp. 167-168.

lación posibilita la materialización de la “puesta en peligro” de las libertades informáticas (*con potencial perjuicio para las mismas*), aspecto abarcable por el dolo. Sin embargo esta solución interpretativa parece forzada y puede poner en cuestión el sentido final que se pretende atribuir a la expresión analizada.

La reflexión precedente no exime de un análisis más amplio de este tipo penal. Cabe interrogarse por las razones que han llevado al prelegislador a *limitar* la acción típica a la manipulación de datos personales, pues puede dejar *fuera* del ámbito típico de incriminación graves conductas verificables en el ciclo operativo del banco de datos con posterioridad a la grabación de datos personales (conducta contemplada en el tipo analizado anteriormente). Por ejemplo podrían quedar fuera del tipo penal la infracción de normas por la Administración o el poder legislativo en atención a la sensibilidad y cantidad de datos a incluir en el ordenador (72), pues no necesariamente se da en tal caso una conducta de manipulación. Estimo más correcto que, en el futuro, la ley penal diferencie un primer grupo de modalidades típicas que impliquen la alteración de datos personales. Junto a este grupo deben crearse otros tipos penales que contemplen, por ejemplo, la transmisión ilícita de datos de un sistema informático a otro, instalado en el propio país o en el extranjero que no contemple las debidas garantías para la prevención de violaciones de las libertades informáticas; con ello se daría respuesta penal a los denominados “*paraísos informáticos*”, que posibilitan

(72) Cfr. al respecto la mejor técnica empleada en los § 41 BDSG y § 20 de la *Datalegen* de Suecia.

graves violaciones del derecho a controlar la circulación de datos personales informáticos (73). Asimismo debería incriminarse la facilitación de informaciones falsas en infracción de la obligación de notificación de los datos procesados, obligación que debería recaer sobre los responsables de los bancos de datos frente a los titulares de la información personal automatizada y los órganos de inspección de datos informáticos (74).

8º) a) Las penas previstas en el PrCP 1980 y la PANCP son las siguientes: arresto de doce a veinticuatro fines de semana y multa de seis a doce meses. La penalidad se sitúa en consonancia con los nuevos principios reguladores que inspiran las penas privativas de libertad y las penas pecuniarias en los textos citados (75). Cabe matizar, no obstante, que la PANCP 1983 ha equiparado las penalidades, por lo que afecta a los delitos contra la intimidad —salvo en el delito de allanamiento de morada— (arts. 187 a 191 PANCP). Ello no empece, sin embargo, para que se postule un mejor entendimiento del principio de *proporcionalidad*; en este sentido, estimo conveniente que los ataques contra la “privacy”, a través de medios técnicos (control auditivo clandestino y abusos informáticos), tengan asignada una penali-

(73) Sobre tal problemática vid. Frosini, V., *Banche dei dati...*, *op. cit.*, pp. 16 ss.

(74) En este sentido la redacción del art. 20 de la *Datalegen* de Suecia constituye un ejemplo a seguir.

(75) Sobre este aspecto vid. Mir Puig, S., “El sistema de sanciones en la Propuesta de Anteproyecto de Nuevo Código Penal de 1983”, en *Documentación Jurídica* (Monográfico dedicado a la PANCP de 1983) núm. 37/40, Madrid, 1983 (vol. 1), pp. 183 ss.; Quintero Olivares, G., “La Reforma penal en España”, *Documentación Jurídica*, *op. cit.*, pp. 14 ss.

dad mayor que la correspondiente a los atentados tradicionales contra la intimidad, como el apoderamiento de secretos documentales o la violación del secreto profesional (por cierto, todavía ausente en un sentido amplio de nuestro CP vigente, pese a constituir ya un atentado “clásico” contra la intimidad en la mayor parte de los ordenamientos europeos).

b) El art. 199 PrCP y el 189 PANCP incluyen respectivamente una referencia típica que puede revestir gran trascendencia. Las modalidades típicas antes analizadas (tipos básicos), así como las penas que tienen asignadas, ven condicionada su aplicación por la expresión “siempre que el hecho no constituya delito más grave”. Parece pues que el prelegislador ha querido establecer una norma de *subsidiariedad expresa* para los tipos básicos del delito informático objeto de estudio (76). Desde luego no está claro cuál pueda ser el fundamento de la cláusula comentada. Si se ha querido expresar la subsidiariedad de los tipos analizados con respecto a otros que tutelan la intimidad con los que pueda establecerse una relación de concurso aparente de normas, el prelegislador ha obrado con precipitación: en primer lugar, porque en la PANCP 1983 no hallamos delito alguno contra la intimidad que contemple una penalidad más grave que la asignada para el delito informático (salvo por lo que respecta a los delitos contra la intimidad domiciliaria —arts. 190 y 191 PANCP— cuya “*ratio essendi*” y dinámica comisiva poca relación guardan con los ataques informáticos contra la “privacy” (77).

(76) Morales, F., *Privacy y Reforma penal...*, op. cit., pp. 626-627.

(77) Sobre el delito de allanamiento de morada en particular vid.

Con la cláusula de subsidiariedad analizada tampoco el prelegislador ha querido referirse a *otros* delitos más graves contra las libertades informáticas en ámbito de los delitos de funcionarios públicos, pues, como ya se indicó, aquellos no están previstos en el PrCP 1980 ni en la PANCP 1983.

Otra solución interpretativa al respecto llevaría a considerar el delito informático como un "*tipo de recogida*" con respecto a otros delitos más graves, que no necesariamente deberían atentar contra la intimidad. Esta solución no parece admisible. El delito contra las libertades informáticas no puede constituir un *tipo genérico de recogida*, puesto que, si aceptáramos esta interpretación, deberíamos sustraerlo "*tout court*" de las reglas generales reguladoras del concurso de delitos, lo que parece inaceptable en la medida que en los concursos de delitos subyace una diversidad de bienes jurídicos menoscabados o puestos en peligro. Con tal proceder las libertades informáticas quedarían configuradas como un bien jurídico de *rango inferior*, cuya tutela penal perdería entidad propia en la medida que se suscitara un concurso de delitos que, "*ex lege*", quedaría excluido a la vista de la cláusula de subsidiariedad objeto de estudio. Por otro lado, la configuración típica del mencionado delito informático no *permite* considerarlo como un tipo genérico "de recogida" con respecto al resto de delitos contemplados en el PrCP y la PANCP.

Jorge Barreiro, A., *El allanamiento de morada*, Madrid, 1986, *passim*.

A la vista de la redacción del art. 189 PANCP podría especularse en torno a la construcción de un concurso ideal de delitos si el abuso informático ha tenido como medio de la obtención de datos el allanamiento de morada (art. 190 PANCP). Según la redacción del art. 189 PANCP, el delito informático debería quedar excluido en favor del allanamiento de morada (art. 189 PANCP), lo que parece absurdo.

Una última vía interpretativa puede ser sustentada y parece la más postulable. Según esta tercera perspectiva interpretativa la cláusula de subsidiariedad analizada estaría configurando un “*tipo de recogida*”, pero referido a *otros posibles delitos informáticos* que en el futuro pudiera prever la *legislación protectora de datos personales informáticos*. De este modo, la inclusión del delito informático en el PrCP 1980 y la PANCP 1983 no prejuzgaría la inclusión o no de otros tipos penales de carácter “más grave” contra las libertades informáticas en la *legislación especial*. No obstante, si ello fuera así, la amplia remisión que prevé la ley penal en blanco de los artículos analizados suscitaría múltiples problemas de superposición de normas en la medida que la mentada legislación especial contuviera también tipos penales con igual o menor penalidad que la expresada en los arts. 199 PrCP y 189 PANCP.

c) Con respecto a la penalidad prevista para los tipos básicos analizados que respectivamente contienen los arts. 199 PrCP y 189 PANCP, debe efectuarse una última consideración crítica. La pena es idéntica para las modalidades de grabación de datos o manipulación de los mismos (supuesto este último en el que es indiferente que la información fuera legítima o ilegítimamente procesada) en infracción de las prescripciones legales sobre el uso de la informática. Desde una perspectiva técnica y político criminal parece adecuado equiparar la penalidad del supuesto típico de grabación ilícita con el de manipulación de datos legítimamente procesados; no obstante, tal equiparación parece incorrecta si la manipulación ha venido precedida de una grabación ilícita o ilegítima. En este

último supuesto, a la vista de la regulación contenida en el PrCP y la PANCP, la conducta de grabación ilícita quedaría absorbida por el posterior acto de manipulación de la información, lo que parece lógico siempre y cuando para esta hipótesis se contemplara una mayor penalidad.

9º) Finalmente, los arts. 199 PrCP y 189 PANCP prevén un tipo agravado para el supuesto en que, con posterioridad a la perfección del tipo básico, se llevare a cabo la divulgación de la información obtenida. Se respeta así la estructura que, en cuanto a los tipos básicos y agravados, adoptan otros delitos contra la intimidad (78). Para los tipos agravados se establecen las penas superiores en grado a las previstas para los tipos básicos.

V. Como antes quedó indicado, el Código penal vigente no obtiene previsiones legales que permitan una adecuada tutela de las libertades informáticas frente al uso ilícito del ordenador.

a) Por lo que respecta a los sujetos autorizados para acceder y operar en un sistema informático algunos autores (79) traen a colación los arts. 498 (revelación

(78) Sobre la estructura doble en torno a los conceptos de actos de intromisión y de revelación vid. Morales, F., *La tutela...*, op. cit., pp. 296 ss.

(79) En este sentido, refiriendo la cuestión al ámbito de los delitos patrimoniales vid. Corcoy, M.-Joshi, U., *Delitos contra el patrimonio por medios informáticos*, op. cit., p. 144: "En los supuestos que el sujeto activo del delito es una persona autorizada para acceder al sistema informático, estamos frente a un comportamiento, en principio, descrito en el art. 498 CP, con la particularidad de que los secretos que se revelan son datos automatizados o programas. Cuando el autor es un funcionario público destinado a trabajar con aquellos medios

de secretos por parte de sujetos en régimen de dependencia), 367 y 368 (revelación de secretos por parte de funcionarios públicos en el ejercicio de sus cargos) para intentar dar respuesta penal a las conductas de revelación de datos personales informáticos.

A mi juicio, tan sólo el art. 368 CP puede cubrir esas necesidades de intervención penal; intentaremos razonar esta afirmación. En primer lugar, el art. 498 CP *no puede* ser invocado en los mencionados supuestos (80), porque ni los potenciales sujetos activos del delito, ni el objeto material del delito están pensados para reprimir conductas de revelación de datos por parte del personal informático. El art. 498 CP menciona como autores del delito a administradores, dependientes y criados. Estimo que *no puede* establecerse una asimilación de tales categorías de sujetos con el personal autorizado para acceder al sistema informático (81); podría especularse al respecto con el concepto de administrador, entendiendo que podría abarcar al personal informático que desempeña sus tareas por cuenta de otro (en régimen laboral de dependencia), pero al conectar el sujeto activo del delito con el objeto material y el sujeto pasivo del mis-

informáticos, el precepto aplicable es el art. 367 o el 368. Para la aplicación del art. 498 CP, en los supuestos de revelación de secretos contenidos en ficheros informáticos, no existe especial dificultad para su punición". En la misma línea interpretativa vid. también González Rus, "Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos", *Revista Facultad de Derecho de la Universidad Complutense de Madrid* (Monográfico 12), p. 149.

(80) Sobre las limitaciones típicas del art. 498 CP vid. Morales, F., *Privacy y Reforma penal...*, *op. cit.*, pp. 592-595.

(81) De otra opinión Corcoy, M.-Joshi, U., *Delitos contra el patrimonio...*, *op. cit.*, p. 146.

mo se comprueba que el art. 498 no puede abarcar típicamente las conductas mencionadas. En efecto, el tipo objetivo del art. 498 se limita a proteger los *secretos del principal* (sujeto pasivo del delito) a los que ha accedido lícitamente la persona dependiente de él. Por tanto, el art. 498 CP establece una esfera de tutela muy restringida, y en ningún caso puede interpretarse que se incrimina *toda* revelación de secretos por parte de personas *en régimen de dependencia* autorizadas para acceder a los secretos de otro. El anacronismo del precepto y su desfase político criminal no permiten extender el alcance del mismo con las pretensiones antes enunciadas (82). En suma, la revelación de secretos referibles a persona que no sea estrictamente "*el principal*" por parte de los referidos sujetos es atípica, lo que en nada satisface las exigencias político criminales orientadas a la tutela penal de las libertades informáticas.

En segundo lugar, el art. 367 CP tampoco puede ser referido a la tutela de datos personales informáticos; en este precepto se incriminan conductas de revelación por parte de funcionarios públicos en el ejercicio de sus cargos (83). Las modalidades típicas que acoge el art. 367 tienen como objeto material de delito, respectivamente, "secretos" y "papeles" o "copia de papeles". Efectivamente nada impide referir los secretos aludidos en el precepto a aquellos contenidos

(82) Sobre ello vid. Morales, F., *Privacy...*, *op. cit.*, pp. 593 ss.; Bustos Ramírez, J., *Manual de Derecho Penal. Parte Especial*, Barcelona, 1986, p. 108.

(83) La invocación del art. 367 CP podría plantearse con relación a un bien jurídico diverso de la privacy informática, con lo que en este punto podría sustentarse el planteamiento de Corcoy-Joshi, *op. cit.*, pp. 144 y 146.

en ficheros informáticos, pero con una limitación: por exclusión de lo dispuesto en el art. 368 —precepto en el que se alude expresamente a los secretos de particulares— debe entenderse que el art. 367 CP sólo debe referirse a *secretos oficiales, estatales o administrativos* (84). Por tanto el art. 367 CP *no puede* ser invocado para la tutela de datos personales informáticos. Tan sólo el art. 368 sirve a tales fines, en el buen entendido que el CP vigente carece de todo planteamiento sistemático y político criminal global sobre la tutela de las libertades informáticas en el ámbito de los delitos de funcionarios públicos en el ejercicio de sus cargos (85).

b) El art. 497 CP contempla el delito de descubrimiento y revelación de secretos documentales, precepto también ajeno al problema que suscita el uso ilícito de la informática en detrimento de las libertades informáticas. Las conductas que se inculpan en el mismo estimo que no pueden encuadrarse en los actos ilegítimos que puedan suscitarse en el estricto ciclo operativo de los circuitos informáticos. Cuando los datos se hallan “*fuera del sistema*”, el art. 497 puede ser aplicado cuando se constata un *apoderamiento (acción del tipo básico)* (86) de datos perso-

(84) Así vid.: Quintano Ripollés, A., *Curso de Derecho Penal*, t. II, Madrid, 1962, p. 560; Muñoz Conde, F., *Derecho Penal. Parte Especial*, 7ª ed., Valencia, 1988, pp. 713-714.

(85) Vid. Morales F., *La tutela...*, *op. cit.*, p. 268.

(86) El momento consumativo del tipo básico se sitúa en la acción de apoderamiento “para descubrir”, de forma que el efectivo conocimiento del contenido de los papeles o cartas tan sólo constituye un ligamen entre el tipo básico y la acción de revelación del tipo agravado (en este sentido vid. Cobo del Rosal, M., “Sobre el apoderamiento documental para descubrir los secretos de otro”, *ADP*, 1971, p. 683; siguiendo esta interpretación Morales, F., *La tutela...* *op. cit.*, pp. 180-181.

nales *plasmados* en “papeles o cartas” (*objeto material del delito*); ello significa que el precepto serviría para incriminar aquellas recogidas ilícitas de informaciones personales que supusieran un apoderamiento subrepticio de documentos. No obstante, las técnicas de colecta de datos personales se verifican mediante actos más sofisticados que los previstos en el art. 497 CP. No obstante, pese a que la estructura del tipo básico parece que responde al modelo de los delitos de apoderamiento subrepticio contra el patrimonio (87) (de forma que se exigiría un apoderamiento físico de los papeles o cartas), la captación mental del contenido de los documentos (sin desplazamiento de éstos) *puede ser equiparada* a la acción típica de “apoderamiento” (88), criterio adoptado en la STS 3-4-1957; de este modo el precepto podría hallar un ámbito más amplio de aplicación con respecto a las recogidas ilegítimas de datos personales con fines informáticos (89).

Sin embargo, cuando los datos personales se encuentran ya *dentro del sistema* informático (una vez han sido informatizados), el art. 497 CP *no ofrece* respuestas frente a las conductas que menoscaban la “privacy” informática; ni siquiera el precepto es aplicable en las hipótesis de extracción u obtención ilícita

(87) Así, Quintano Ripollés, A., *Tratado de Derecho Penal. Parte Especial*, t. I, vol. 2, Madrid, 1972, p. 1011.

(88) En este sentido: González Rus, *Aproximación...*, *op. cit.*, p. 145; Morales, F., *La tutela...*, *op. cit.*, p. 177. La aceptación de la equiparación de la captación intelectual del contenido de los papeles con el apoderamiento material o físico de los mismos, no obstante, no puede significar que el “descubrimiento” constituya el momento consumativo del tipo básico (vid. *supra*, nota 86).

(89) Vid. Corcoy-Joshi, *op. cit.*, pp. 144-145.

de datos, pues éstos deben tener como *soporte material* “papeles o cartas” y debe constatarse una acción de apoderamiento (requisito que no sería problemático desde una interpretación amplia que incluyese la captación intelectual de la información en la referida acción típica) (90). Pero el objeto material del tipo básico contempla una *limitación objetiva* para incriminar estas conductas en la medida que el objeto material del delito sobre el que debe proyectarse la acción típica son papeles o cartas (*soporte físico de la información*).

c) Por lo que respecta a la *transmisión* de datos en los sistemas informáticos entiendo que el CP *no ofrece* respuestas adecuadas. La Ley Orgánica 7/1984 introdujo en el CP vigente el delito de control clandestino por medio de la interceptación de comunicaciones telefónicas o de la utilización de instrumentos de escucha, transmisión, grabación o reproducción del sonido, con un doble planteamiento legal según el delito fuere perpetrado por particulares (art. 497 bis) o por funcionarios públicos (art. 192 bis) (91). A mi

(90) Debe repararse, no obstante, en que el precepto incluye el posesivo “sus” para referirse al objeto material de la acción de apoderamiento, razón por la cual *debe coincidir la titularidad* sobre los papeles o cartas con la titularidad de los secretos contenidos en los mismos. Por ello cuando los datos se hallen dentro del sistema informático, con independencia de que la asimilación de los papeles o cartas al soporte informático constituiría *analogía contraria el reo*, debería constatarse además la *coincidencia del titular de los secretos con el titular del soporte informático*. En suma el precepto no es aplicable en las hipótesis analizadas.

(91) Con carácter exhaustivo sobre estos nuevos delitos vid. por todos González Guitián, L., “Protección de la intimidad y escuchas clandestinas” (pp. 49 ss.), “Escuchas clandestinas realizadas por funcionarios públicos” (pp. 85 ss.) y “Escuchas clandestinas realizadas por particulares” (pp. 157 ss.), en *Comentarios a la legislación penal*

juicio los problemas, cara a la incriminación de actos ilegítimos verificados en los sistemas informáticos, son similares a los que se plantean con relación al art. 497 CP. Como se indicó este último precepto puede ofrecer una vía de incriminación de conductas que sólo *mediatamente* pueden referirse al ciclo operativo de los sistemas informáticos, y tan cuanto se trate de datos que se hallen "*fuera del sistema*" (descubrimiento y revelación de datos plasmados en papeles o cartas). Con relación a los arts. 497 bis y 192 bis debe indicarse que uno y otro precepto *no pueden* abarcar típicamente las interceptaciones ilegítimas que se verifiquen por *impulsos magnéticos*, del mismo modo que no alcanzan a incriminar las interceptaciones de comunicaciones por *télex*. Por tanto la protección penal introducida por los referidos artículos debe entenderse, como señala Muñoz Conde, que se limita a las *comunicaciones orales*, ya fueren verificadas mediante teléfono o sin él (92). Otras comunicaciones quedan *fuera* del contenido típicos de los preceptos enunciados, pues estos aluden estrictamente a la interceptación de comunicaciones telefónicas o a la utilización de instrumentos técnicos (de escucha, transmisión, grabación o reproducción) que tenga por objeto sonidos. En definitiva, los arts. 192 bis y 497 bis CP son ajenos a la problemática suscitada por la interceptación de transmisiones que tengan por objeto datos informáticos. Más claramente queda fuera del contenido típico de los enunciados preceptos la pro-

(dirigidos por M. Cobo del Rosal y coordinados por M. Bajo Fernández), tomo VII, Madrid, 1986.

(92) Muñoz Conde, F., *Derecho Penal. P.E., op. cit.*, p. 149.

pia transmisión ilícita de informaciones personales automatizadas (93).

d) Cuestión diversa a la hasta aquí analizada es si los tipos penales del CP hasta ahora analizados permiten establecer una tutela penal *mediata* (esto es *residual* y respecto de datos que se hallan *fuera del sistema* en los términos y límites más arriba expresados) con relación a informaciones de trascendencia *económica*. Especialmente el interrogante se proyectaría sobre los arts. 497 y 497 bis CP. A mi juicio en ambos preceptos el *único* bien jurídico tutelado de forma inmediata es la intimidad (94); por tanto se trata de un bien jurídico de carácter personalísimo, lo que no obsta para que, ocasionalmente, la tutela en ese ámbito pueda suponer una protección *indirecta* de otros intereses, en cuanto que la "privacy" se erige con frecuencia en presupuestos de ejercicio de otros derechos y libertades (95). Pudiera pensarse que en los referidos delitos el bien jurídico protegido es el secreto "*per se*", pero ya indiqué que ese es un concepto *formal e instrumental* y no el bien jurídico protegido desde una perspectiva *material*. Otra podría ser la argumentación en otros ordenamientos en los que la regulación legal constantemente alude a la tutela de secretos (por ejemplo el StGB de la RFA) (96). En el CP español la ubicación de los arts. 497 y 497 bis

(93) Corcoy-Joshi, *op. cit.*, p. 147, señalan con respecto a los arts. 192 bis 497 bis: "Una redacción más afortunada del tipo habría permitido incluir las comunicaciones por telex, impulsos magnéticos..."

(94) En sentido contrario, Corcoy-Joshi, *op. cit.*, p. 148 señalan que en el art. 497 es posible que se tutele tanto la intimidad como la propiedad.

(95) La tutela del patrimonio en todo caso vendría determinada por un reflejo de protección ("*Schutzreflex*").

(96) Vid. *supra* nota 44.

CP en el Título destinado a la regulación de bienes de impronta *personal* como la libertad y seguridad, así como la apelación explícita a la “intimidad” en el art. 497 bis, aconsejan concluir que estamos frente a tipos penales que tutelan *bienes de la personalidad*. Que la estructura típica del art. 497 CP se asemeje a la de los delitos patrimoniales de apoderamiento por el contexto histórico en el que se conforma este precepto (97), no puede llevarnos a concluir que el bien jurídico protegido sea la propiedad (98).

e) Por lo que respecta a los delitos contra el honor (calumnia e injuria), amén de las razones relativas al bien jurídico antes expuestas, la *dinámica comisiva* de estos ilícitos penales obliga a considerarlos inaptos frente a los ataques informáticos contra la “privacy”.

f) En otro ámbito delictivo, el de las coacciones (tipo penal “de recogida” por excelencia en el terreno de los delitos contra la libertad) (99), tampoco parece posible la incriminación de los atentados informáticos analizados. Ni tan siquiera a costa de ampliar el concepto de violencia para dar entrada por vía interpretativa a la “*vis in rebus*” (100), es posi-

(97) Vid. Morales, *La tutela...*, *op. cit.*, p. 191.

(98) Ni siquiera es argumento para tal conclusión que se sostenga que el momento consumativo se da con el apoderamiento intencional, siendo irrelevante en el tipo básico del art. 497 CP el efectivo descubrimiento del secreto.

(99) Vid., García Pablos, A., “Derecho Penal y protección de la libertad de obrar de la persona. El delito de coacciones”, en García Pablos, *Estudios penales*, Madrid, 1984, p. 252; Torío López, A., *La estructura típica del delito de coacciones*, ADP, 1977, p. 19.

(100) En sentido crítico sobre la desnaturalización por exceso del término “violencia” en el art. 496, acertadamente vid. García Pablos, *op. cit.*, pp. 274-275.

ble que el delito de coacciones cumpla, a los efectos aquí analizados, la reseñada función de recogida típica de conductas. Se trata de un delito contra la “actuación de la voluntad” (libertad de obrar) (101), por tanto las conductas típicas deben ser *percibidas* por el sujeto pasivo del delito. Los atentados informáticos contra la “privacy”, por su carácter *insidioso*, suelen pasar *inadvertidos* para la víctima. Además la configuración del delito de coacciones (art. 496 CP) es ajena a toda la complejidad técnica que subyace en los atentados informáticos. Finalmente, debe indicarse que la “privacy”, en su dimensión tecnológica, delimita una nueva esfera de libertad del individuo (la libertad informática), necesita de la creación de delitos específicos para su adecuada y eficaz tutela penal.

g) En el catálogo de delitos perpetrados por funcionarios públicos contra derechos de la persona, el único resquicio legal para incriminar los atentados informáticos contra el “*habeas data*” del ciudadano viene dado por el art. 194 CP. En la medida que el precepto *no concreta* la modalidad de la acción típica, ni el objeto jurídico de tutela, con notable desprecio de las garantías del principio de legalidad penal, lógicamente permite la subsunción de abusos informáticos contra el “*habeas data*” del ciudadano. La interpretación del art. 194 CP suscita múltiples interrogantes (102). En primer lugar, reina la incertidumbre en cuanto al *objeto jurídico de tutela*; la expresión “derechos cívicos” no tiene una clara definición normativa en nuestro ordenamiento. En cual-

(101) Así, García Pablos, A., *op. cit.*, pp. 257 ss.

(102) Vid. Morales, F., *Privacy...*, *op. cit.*, pp. 599-600.

quier caso parece que abarca los derechos y libertades constitucionales. Por consiguiente, y a la vista del art. 18.4 CE posibilita la protección de las libertades informáticas. *Tampoco* concreta el legislador las *modalidades de la acción típica*, la ley sólo alude a la acción de “impedir”, que parece referible a los abusos informáticos. Por último, el CP prevé para el delito analizado una penalidad a todas luces benigna e insuficiente. Y respecto del supuesto abordado, no sirve de paliativo el oscuro art. 204 bis a), que posibilita la aplicación de los arts. 178 a 204 CP, sin perjuicio de lo ordenado en otros preceptos del CP que señalen mayor pena a cualquiera de los delitos comprendidos en los mencionados preceptos. Dado que la libertad informática, fuera del contexto de las relaciones políticas individuo-Estado (contexto en el que se ubica el art. 194 CP), no encuentra protección en otros preceptos del CP —como ya se ha indicado anteriormente—, la única penalidad a aplicar sería la prevista en el art. 194 CP. En cualquier caso es evidente que la libertad informática, en cuanto garantía jurídico-política, precisa de una explícita y más adecuada tutela penal.

VI. Al comienzo de la presente intervención se constató que la única referencia explícita en nuestro ordenamiento al desarrollo del art. 18.4 de la Constitución está contenida en la Ley Orgánica 1/1982 de 5 de mayo relativa a la “Protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen”; la Disposición transitoria Primera de la misma establece: “En tanto no se promulgue la normativa prevista en el art. 18, apartado 4 de la Constitución, la protección civil del honor y la intimidad

personal y familiar frente a las intromisiones ilegítimas derivadas del uso de la informática se regulará por la presente ley”.

El legislador anticipa así que en la futura Ley reguladora de la protección de datos personales automatizados se procederá a la creación de ilícitos y sanciones civiles. Nada hay que objetar a esta previsión, pues como han destacado recientemente Bricola y Roxin entre otros (103), el derecho civil puede desempeñar *funciones represivas y preventivas*, junto a las tradicionales de carácter reparatorio, en el ámbito de tutela de los bienes de la personalidad. Pero no parece que éstas vayan a ser las únicas normas sancionadoras que establezca la futura ley sobre el uso de la informática. Ya efectué una reflexión sobre la posible inclusión, en el futuro instrumento legislativo, de tipos penales; pero más segura parece la inserción de ilícitos y sanciones administrativas en una esfera de actividad sobre la que se deberá producir el intervencionismo del Estado, según demuestra la legislación comparada.

La Disposición transitoria Primera antes transcrita alude a las intromisiones ilegítimas en el uso de la informática. De tal forma, por vía interpretativa, el uso ilícito de la informática deberá quedar encuadrado en el art. 7º de la Ley de protección civil de 1982, que establece el catálogo de intromisiones ilegítimas en el ámbito de los bienes de la personalidad. Es evidente que la redacción del art. 7º no está pensada

(103) Bricola, F., “La riscoperta delle “pene private” nell’ottica del penalista”, *Politica del Diritto*, 1985, núm. 1, pp. 72 ss.; Roxin, C., “Risarcimento del danno e fini della pena” (trad. L. Eusebi), *Rivista Italiana di Diritto e Procedura Penale*, 1987, pp. 12 y 21.

para los abusos informáticos. No obstante, el apartado 2º del art. 7º posibilita su subsunción pues alude a la utilización de medios técnicos para conocer la vida íntima de las personas, por medio de una cláusula de "*numerus apertus*"; el precepto se refiere a la utilización de "cualquier otro medio", entre los que cabe incluir a la informática. A los efectos de *desarrollo interpretativo* deberá ser tenido en cuanto el Convenio internacional del Consejo de Europa sobre protección de datos personales automatizados, antes citado, en especial los artículos 4 y siguientes del mismo que contemplan los principios fundamentales de la protección de datos personales. Las conductas de revelación de datos relativos a la vida privada, que arranquen de un acceso legítimo o ilegítimo a los datos personales automatizados también pueden quedar tipificadas como ilícitos civiles a la vista de lo que prescribe el apartado 3º del art. 7º de la Ley de 1982.

Es de destacar que las respuestas jurídicas previstas en la Ley de 1982 van más allá de las meramente reparatorias o indemnizatorias. El contenido del art. 9º permite colegir que la ley cumple *también* funciones represivas y preventivas (así, por ejemplo, la previsión de medidas cautelares encaminadas al cese inmediato de la intromisión ilegítima, la referencia a las medidas tendentes a prevenir o impedir intromisiones ulteriores etc., ...).

Finalmente, debe reseñarse que la Ley de 1982 parece más pensada para la tutela de la intimidad que del honor, dadas las continuas referencias en el cuerpo legal a las intromisiones ilegítimas en la vida privada o íntima. Pero, paradójicamente, en la práctica,

como ha destacado Muñoz Machado, la ley se ha revelado mayormente como un instrumento de tutela del honor (104). Puede señalarse que la vía penal en materia de tutela del honor ha sufrido una notable atrofia. Este dato parece abrir la vía para una futura política penal *despenalizadora* en materia de delitos contra el honor, de los que —a mi juicio— solo la calumnia y la modalidad de injuria relativa a la imputación de delitos perseguibles a instancia de parte (art. 458.1 CP) deberían subsistir en el Código Penal, para dar paso en el resto de los casos a una *exclusiva* (y no concurrente como en la actualidad) protección civil del honor (105).

(104) Muñoz Machado, S., "Mitos, insuficiencias y excesos en la construcción jurídica de las acciones por difamación", *Poder Judicial* (2ª Época), 1986, pp. 13-14.

(105) Sobre tal propuesta vid. Morales, F., "Adecuación social y tutela penal del honor: perspectiva despenalizadora", *CPC* en prensa.