Seguridad ciudadana y prevención del delito.

Retos de la protección de datos ante las necesidades de seguridad.

Prof. Dr. Alfredo Chirino Sánchez
Catedrático de Derecho Penal
Facultad de Derecho
Universidad de Costa Rica
Juez del Tribunal de Casación
II Circuito Judicial de San José

1. Introducción. La seguridad como problema global.

Se viven tiempos en que la seguridad es un elemento esencial de las políticas públicas y constituye un requerimiento elemental para la vida de convivencia. Sin embargo, es quizá el concepto de "sociedad de riesgos", acuñado por el sociólogo Ulrich Beck[1], el que mejor define la actual tendencia de las políticas estatales tanto en el Viejo como en el Nuevo Continente.

El temor al delito y a ser víctima de un acto criminal han llevado al ciudadano a exigir seguridad a cualquier costo, incluso de las garantías y libertades que por centurias han engalanado las constituciones liberales. La "epistomología del riesgo" exige ya del legislador penal la posibilidad de adelantarse a riesgos lejanos, a puestas en peligro de bienes jurídicos apenas contingentes y procurar a través de mecanismos normativos la reducción de tales riesgos a su mínima expresión.

[1] Beck, Ulrich. La sociedad del riesgo. Hacia una nueva modernidad. Traducido por: Navarro Jorge y otros. Ediciones Paidós Ibérica, S.A., 2006.

Lo que podríamos denominar una "política posmoderna" desarrollada en Europa, y reproducida, de alguna manera en América Latina y los Estados Unidos, sobre todo después, del atentado sufrido en dicho país el 11 de septiembre de 2001[2], ha revelado una poderosa tendencia en el derecho y en la praxis del sistema de justicia penal, que hace uso de cada vez más poderosos conceptos de carácter funcional, que tienen el objetivo de modificar las tradicionales limitaciones del derecho penal y permitir investigaciones de más amplio espectro para perseguir y controlar, sobre todo, el terrorismo y otras formas de criminalidad globalizada[3].

La amenaza del delito se ha convertido en la moneda común de los profetas de la inseguridad, quienes exigen de manera estentórea una reacción contundente e inmisericorde contra el delito y los delincuentes, dibujando escenarios de muerte, de violación, de angustia y sufrimiento, que guardan mucha semejanza con las estadísticas de impunidad que no se cansan de lanzar a los cuatro vientos. Las exigencias son tan estentóreas que una reacción racional, tranquila y acorde a las circunstancias no es posible. Los paisajes de inseguridad, de miedo y de pérdida de orientación parecen haberse apoderado de las clases políticas de los países, y las soluciones de "mano dura" y de "super mano dura" son las ocurrencias con las

---

[2] Un análisis crítico de las tendencias en el ámbito político y jurídico puede encontrarse en: Rill, Bernd (Editor), Terrorismus und Recht. Der wehrhafte Rechtsstaat, Argumente und Materialien zum Zeitgeschehen 40, München, Hans Seidel Stiftung e.V., 2003, disponible en internet en: http://www.hss.de/downloads/argu40.pdf

[3] En la República Federal de Alemania es particularmente plástico el proceso de cambio de la legislación con el objetivo de controlar normativamente el fenómeno del terrorismo. En 1976, luego de los ataques realizados por la tristemente famosa Rote Armee Fraction (RAF) se puso en vigencia una ley antiterrorista y una ley para proteger la paz social. La primera introducía un nuevo tipo penal, el parágrafo 129 a) del Código Penal Alemán (StGB), que penaba la constitución o el apoyo a una organización terrorista. Pero mucho más importante que este delito son las consecuencias recibidas en el proceso penal, donde ya solo era necesaria una mera sospecha de haber cometido tal acción para dictar en contra de ese sospechoso una orden de detención. Desde el punto de vista de la prisión preventiva ya no era importante, por ejemplo, encontrarse ante un caso de peligro de fuga o de entorpecimiento de las investigaciones para hacerse merecedor del dictado de una prisión preventiva, o para hacerse acreedor a una observación constante del intercambio epistolar entre el defensor y el acusado. Además, las mencionadas leyes introducían en aquél momento tipos penales que permitían interpretaciones muy flexibles de conductas que se encontraban cerca del ámbito de acciones típicas de los hechos cometidos por el grupo terrorista RAF, tales como el parágrafo 88 a) sobre la Apología contraria a la Constitución de hechos penales y el Parágrafo 130 a) que castigaba el dictar órdenes para la realización de un hecho criminal. Comportamientos legislativos parecidos pudieron observarse con la Junta Militar en Grecia en 1969 y con una ley de excepción en España en 1975. Sin duda, legislación de su tiempo, que está condenada a repetirse luego de los hechos particularmente violentos que han dado inicio al siglo XXI.

que se han aderazado los últimos cambios de la legislación, por lo menos en Centroamérica, en los últimos años.

Por supuesto, el problema de la criminalidad ha alcanzado niveles de profunda preocupación, como también los niveles de profunda inequidad en los que se han sumido las sociedades modernas, donde la separación entre ricos y pobres se hace cada vez más profunda y dolorosa, donde el acceso al alimento, al trabajo o a una vivienda digna resulta una lucha cotidiana para numerosas personas en las sociedades latinoamericanas de hoy en día. El paisaje de las víctimas del delito, de los refugios supervigilados y controlados en los que habitan los más pudientes de las clases emergentes de nuestro margen cultural, así como el crecimiento exponencial de las policías privadas, y de la hipervigilancia de los espacios públicos, son los elementos con los que es indispensable identificar nuestras modernas sociedades, y donde cada vez más las herramientas de intercambio de información constituyen el medio más "eficiente" para brindarnos la seguridad perdida. Ahí comienza la crisis de esta evaluación que estamos proponiendo.

El Estado se ha movido, con pasos decididos, del lado de la libertad hacia el lado de la seguridad. En su condición de "partner" se pone al servicio de las sociedades angustiadas y les ofrece instrumentos para recuperar la seguridad perdida, pero sin detenerse en sus siempre presentes necesidades de información para todos los fines imaginables[4]. Los métodos para el control de las conductas

[4] En un artículo reciente, la prestigiosa revista "The Economist", bajo el singular título de "Conviviendo con el Gran Hermano" se reporta, por ejemplo, que Gran Bretaña ha promovido tareas de espionaje de sus ciudadanos, recopilando ingentes cantidades de información personal. Dicha información no sólo es accesible al Gobierno sino también a individuos particulares y agencias. La base de datos de salud de Gran Bretaña, la más grande de su tipo en Europa, contiene los registros médicos de 53 millones de personas, habitantes de Inglaterra y Gales. El Registro de Identidad inglés contiene información de toda la población, distribuida en 49 criterios o asuntos de consideración. A partir de 2009 se exigirá a los ciudadanos la portación de un documento de identidad biométrico con el cual accederán a servicios públicos, tales como: cirugías, agencias de empleo, bibliotecas y otros. No hay que teorizar demasiado para tener la certeza que el rastro de información que sea dejado por los ciudadanos en todas estas áreas de su actividad cotidiana será fácilmente monitoriado, comparado y analizado por quien quiera hacerlo, tras la búsqueda de cualquier cosa, desde perfiles de consumo o de personalidad o para investigaciones sobre la comisión de potenciales hechos criminales. Según el artículo, Estados Unidos planea un sistema similar mediante la incorporación de una "licencia de conducción inteligente". La licencia de conducir en Estados Unidos es el documento de identidad por excelencia de los ciudadanos. Estos cambios demuestran que los Estados no han desistido de

desviadas y que generan inseguridad implican también lesiones a derechos fundamentales de los ciudadanos inocentes que quedan en las redes informativas de los mecanismos de control instaurados con el fin de obtener la ansiada y huidiza seguridad[5].

La ciencia del derecho penal parecía oponerse a estas tendencias, sobre todo en la última parte del siglo XX, pero este nuevo siglo parece recomponer las líneas de batalla, y si se quiere también absolutiza algunas de las consecuencias y las perpetúa en el análisis jurídico y en la respuesta legislativa[6].

El concepto de seguridad en voga es aquél que conecta, directamente, con la idea de alcanzar paz a cualquier costo, incluso de garantías fundamentales y no se escatiman esfuerzos en implementar todo aquello que sea técnicamente posible, casi sin atender a ninguna consideración de carácter constitucional.

La prevención del delito significa hoy "combate de la criminalidad a cualquier costo" y los acercamientos teóricos y jurídicos provenientes del populismo penal hacen natural y razonable que los ciudadanos entreguen sus derechos y libertad para alcanzar una seguridad que les es huidiza y mítica.

Las "víctimas" de este proceso de "repensamiento" del derecho penal liberal no son otras más que la dogmática de los derechos fundamentales y el mismo marco de referencia del concepto antropológico constitucional, en la búsqueda de un reposicionamiento de fines y objetivos de carácter colectivo, que ya no parece ser

---

sus afanes de recopilación de información, solo que ahora las tecnologías facilitan el proceso y, además, se venden como útiles para garantizar seguridad y eficiencia estatal. Cfr. The Economist, "Conviviendo con el Gran Hermano", extraído de su versión en español, publicada por la Revista Summa, Edición Centroamericana, No. 166, marzo de 2008, p. 122.

5 Cfr. al respecto, con más detalles, Hassemer, Winfried, Erscheinungsformen des Modernen Rechts, Frankfurt am Main, Vittorio Klostermann, 2007, p. 241.

6 Cfr. Chirino, Alfredo, El Retorno a los delitos de peligro. ¿Un camino posible hacia el derecho penal del enemigo?, en: Llobet, Javier (Editor), Libro Homenaje al Profesor Francisco Castillo González, San José, Costa Rica, Editorial Jurídica Continental, 2007.

posible limitar o incluso matizar en su enfrentamiento con libertades y derechos individuales.

Estos cambios ya es posible observarlos en la jurisprudencia y en la legislación comparadas, donde el afán consiste en darle "funcionalidad" a la administración de justicia penal[7] a través, principalmente, de una desformalización del proceso penal y de un equilibrio contradictorio con los derechos fundamentales del acusado. Los elementos de este proceso discursivo toman elementos de la discusión sobre el "derecho fundamental a la seguridad"[8], que ya apunta, por sí mismo, a una absolutización de los fines de la sociedad.

En la presente investigación, sin embargo, no haremos una valoración exhaustiva de este "espíritu de los tiempos" que se vive en la legislación comparada, ni tampoco escudriñaremos con detalle las consecuencias sociopolíticas de estas tendencias, aspectos que deberán quedar para un estudio posterior[9]. Lo que sí haremos es un balance de las garantías clásicas del proceso penal liberal frente a los retos del combate de la criminalidad globalizada, principalmente la criminalidad organizada, el terrorismo y la criminalidad por medios electrónicos. Igualmente, haremos algunas observaciones sobre el destino de nuestra jurisprudencia y legislación ante los embates de las urgencias político criminales populistas derivadas de los fenómenos sociales recientes. Para hacer esta ponderación tomaremos algunos datos de la doctrina y la jurisprudencia alemanas, que son

---

7 Sobre el punto puede ser consultado Hassemer, Winfried, Die Funktionstüchtigkeit der Strafrechtspflege - ein neuer Rechtsbegriff?, StV (Strafverteidiger, Revista de los Defensores Penales, Rep. Fed. de Alemania) 6/1982, pp. 275 y ss. Sobre este concepto y su influencia en el debate sobre el uso de las TIC`s en el proceso penal cfr. Chirino Sánchez, Alfredo, Das Recht auf Informationelle Selbstbestimmung und seine Geltung im Strafverfahren, am Beispiel der neuen Ermittlungsmethoden in der Strafprozessordnung, Frankfurt am Main, Berlin, Bern, New York, Paris, Wien, Peter Lang Verlag, 1999, pp. 163 y ss.

8 Cfr. Isensee, Josef, Das Grundrecht auf Sicherheit. Zu den Schutzpflichten des freiheitlichen Verfassungsstaates, Berlin, New York, Walter de Gruyter, 1983. Cfr. Con críticas a esta perspectiva: Hassemer, Erscheinungsformen op. cit., pp. 234-235.

9 Hemos adelantado algunas consideraciones de este problema en nuestro trabajo: "La seguridad como un topos discursivo en la política criminal centroamericana. Perspectivas de una desesperanza", en: Revista Hermeneútica, Revista Jurídica Estudiantil, San José, Costa Rica, Facultad de Derecho, Universidad de Costa Rica, No. 14, junio de 2005, pp. 35-53.

muy plásticos de las preguntas, y de los riesgos de algunas respuestas que se han venido dando.

El objetivo general del estudio, podría enmarcarse, entonces, tanto como una advertencia de una crisis ya presente[10], como también de los peligros de la asunción de los himnos de batalla que se empiezan a escuchar por doquier, especialmente, de las trincheras del populismo jurídico penal.

En concreto, este trabajo pretende dar algunas líneas interpretativas, sobre todo desde la perspectiva del derecho a la autodeterminación informativa, que puedan ser útiles para comprender los graves riesgos que afronta el Estado de Derecho, con algunos usos, demasiado generosos, de las nuevas políticas de investigación penal.

Con el fin de acotar los espacios de desarrollo de la presente investigación, haremos en primera instancia, una evaluación de los desarrollos legislativos en materia de seguridad ciudadana y prevención del delito de las últimas fechas, evaluaremos sus problemas desde la perspectiva del derecho a la autodeterminación informativa, y, finalmente, a modo de conclusión, haremos un balance acerca de los éxitos y fracasos, en materia de garantías, que estos desarrollos permiten vislumbrar.

2. Desarrollos legislativos recientes en materia probatoria en el proceso penal

Uno de los más importantes desarrollos en la construcción de un mundo globalizado lo es, sin lugar a dudas, el aumento y diversidad de las posibilidades

[10] A la cual ya nos hemos referido con algún detalle en: Chirino Sánchez, Alfredo, "La "Criminalidad Organizada" como un nuevo topos de la política de seguridad y orden. Algunas Consideraciones sobre los cambios procesales surgidos del ímpetu de esta polìtica", en: Llobet Rodríguez, Javier y Chirino Sánchez, Alfredo, Principio de Oportunidad y persecución de la criminalidad organizada (Problemas prácticos e ideológicos de un proceso penal "eficiente"), San José, Costa Rica, Editorial Areté, 2000.

técnicas para realizar un más minucioso y detallado control policial a nivel internacional. Luego de los sucesos del 11 de septiembre de 2001 en los Estados Unidos, fue posible observar un recrudecimiento de las medidas de investigación, principalmente, se le dan más y mejores posibilidades observación y persecución a los órganos del control penal, mediante la vigilancia del intercambio epistolar a través de Internet y mediante la escucha de los telefonemas. Junto a ello se tomaron medidas para combatir el lavado de dinero y, por supuesto, la posibilidad de observar y escudriñar los intercambios monetarios entre diversos países y los Estados Unidos, también, y como era imaginable, se introdujeron limitaciones para la obtención de visados de viaje y para la entrada al país, también se abrió la puerta para perfilar genéticamente a terroristas y a otros criminales violentos y la posibilidad de revisar expedientes estudiantiles en todas las sedes educativas[11]. Esto último no sin pocas consecuencias para el derecho a la protección de datos y otras libertades civiles de los ciudadanos.

La anterior tendencia en la política legislativa demuestra un claro alejamiento de la doctrina clásica del Estado Democrático y Social de Derecho, lo que en última instancia se considera un efecto colateral de una orientación necesaria de la política criminal a una igualación de armas en la batalla frente a fenómenos criminales para los cuales no parece existir otra respuesta.

Los sistemas electrónicos de vigilancia y de control tienden a obtener un "sospechoso" a partir de la rápida y poderosa comparación de datos entre diversos bancos o acervos de informaciones, a veces sin una sospecha concreta o sin un delito que perseguir, o incluso en inmensas operaciones de rastreo que llevan a muchos ciudadanos "inocentes" a formar parte de un listado de posibles

[11] Estas medidas están contenidas en la denominada "Ley Patriótica" (US Patriot Act) del 26 de octubre de 2001. El texto completo de esta legislación puede consultarse en: http://news.findlaw.com/cnn/docs/terrorism/hr3162.pdf

sospechosos de haber cometido un hecho punible[12]. Esto, por sí mismo, podría significar el retorno de un verdadero derecho penal antidemocrático.

En palabras de Vassilaki, tal parece que la verdadera "naturaleza de las cosas" de este siglo que recién comienza está definida por el uso de las tecnologías de la información[13]. Y esta afirmación no es casual, si se toma en cuenta el papel esencial que cumple la información en la actual sociedad tecnológica, donde ocupa, junto a la energía y la materia, un importantísimo papel en la vida social. Por eso no debe sorprender que también ella constituya una fuente de peligro para la vida comunitaria, en el sentido de que puede ser procesada de manera ilícita, lesionando derechos y garantías individuales, o afectando directa o indirectamente bienes jurídicos penalmente tutelados[14].

La política criminal internacional, muy especialmente la europea, pero también la estadounidense, permiten determinar que se ha instrumentalizado la idea de la funcionalidad de la administración de justicia penal, concepto que ha conducido, inevitablemente a un deterioro intenso y marcado del nivel de protección del ciudadano frente a los poderes informativos del Estado. Poderes que han sido

---

12 La revisión y análisis de la información también la pueden ejecutar ciudadanos particulares, utilizando la poderosa capacidad instalada de equipos informáticos de nueva generación. La Revista "The Economist" reporta que Frank Asher, vendedor de fármacos y convertido a empresario tecnológico, decidió utilizar los datos acumulados de 450 millones de personas en su compañía privada, "Seisint", para ver si podía identificar a los terroristas involucrados en los ataques a Nueva York y Washington. Para hacerlo, filtró los datos disponibles utilizando criterios tales como nombre, religión, historial de viajes, preferencias de lectura y otras cosas y obtuvo una lista de 1200 personas "sospechosas". La lista fue entregada al FBI y sin saberlo incluía cinco de los individuos involucrados en los ataques terroristas. El programa que permitió tal perfil de "sospechosos" recibió el sugerente nombre de "MATRIX" (siglas en inglés para el intercambio interestatal de información antiterrorista) y pronto será utilizado para comparar y analizar 20 mil millones de trozos de información para identificar potenciales terroristas. Un programa denominado "STAR" (Sistema Evaluador de Riesgos), una nueva versión de "MATRIX", se vale de bases de datos públicas y privadas para realizar las comparaciones. El artículo se plantea, con razón, de que los eventuales "sospechosos" no sabrán de que han sido escogidos automáticamente por un sistema informatizado, tampoco podrán rebatir su "potencial" condición y, además, si esta información es compartida con otras agencias estatales, lo que sucederá inexorablemente, es probable que no puedan aspirar a conseguir un trabajo en el gobierno, una beca de estudios o incluso un contrato público o la ansiada visa de inmigración. Cfr. The Economist, "Conviviendo con el Gran Hermano", op. cit., p. 120.

13 Vassilaki, Irini, Materielles Strafrecht, Strafprozessrecht, Rechtsinformatik und Informationsgesellschaft, en: http://www.alfred-buellesbach.de/PDF/33_Vassilaki_Materielles.pdf

14 Así Vassilaki, op. cit., pp. 348-350.

aumentados exponencialmente por el uso indiscriminado de bancos de datos públicos y privados, así como de herramientas de intercambio, comparación y control de datos, principalmente en la "red de redes" Internet[15].

3. La actividad policiaca como actividad informativa. El caso de EUROPOL y del Sistema de Información de Schengen.

Uno de los modelos de actividad policiaca basada en la recopilación de datos personales lo constituye, sin duda, EUROPOL[16]. Su tarea primordial es la recopilación sistemática y la valoración de datos personales que pudieran estar en relación con criminalidad extrafronteras de carácter organizado. La central que se ubica en La Haya se comunica con los Estados miembros a través de las denominadas "oficinas nacionales". La idea es centralizar en un solo banco de datos las informaciones que provienen de estas oficinas nacionales, estas últimas, por supuesto, tienen la posibilidad de acceder a este banco de datos centralizado. Junto a las informaciones que proceden directamente de EUROPOL también se cuenta con información de terceros, como lo sería, por ejemplo, informaciones de INTERPOL, las cuales también son accesibles a los Estados miembros mediante sus oficinas nacionales.

El proceso de análisis de la información puede ser iniciado por una investigación penal en concreto, pero también podrían tener lugar dentro de una investigación penal pero cuyos datos son necesarios por razones puramente estratégicas. Si es

---

15 No en balde, y a raíz de esta circunstancia es que se ha hecho especial hincapié en la Conferencia de los Encargados de la Protección de Datos europeos celebrada en Cracovia, Polonia, en abril de 2005, sobre la necesidad que la lucha contra la criminalidad extrafrontera vaya acompañada de un alto nivel de regulaciones de protección de datos. Esto último no sólo por una exigencia de razón práctica sino porque el derecho a la protección de datos forma parte ya de la Carta de Derechos Fundamentales Europea del 7 de diciembre del año 2000, que en su artículo 8 establece la necesidad de que los datos personales solo podrán ser tratados si ha existido de previo un consentimiento de la persona afectada y solamente para el fin para el que fueron recopilados. La vigilancia y control de estos requerimientos ha de ser alcanzado mediante la intervención de autoridades de control de la protección de datos, que son parte esencial de la normativa en esta materia.

16 Convenio basado en el artículo K3 del Tratado de la Unión Europea por el que se crea una Oficina Europea de Policía, que puede ser consultado en: https://www.agpd.es/portalweb/canaldocumentacion/legislacion/union_europea/convenios/common/pdfs/B.24-cp--CONVENIO-EUROPOL.pdf

este el caso, las informaciones son compartidas con todos los Estados miembro. Si se trata de investigaciones en casos concretos, la información solo es compartida con el Estado miembro que hizo la solicitud.

Como puede observarse, las tareas de EUROPOL son principalmente de naturaleza informativa y por ello los problemas de protección de datos que ofrecen son de enorme importancia. En primer lugar, a pesar de que ya forman parte de la "cultura" de la protección de datos, los principios de ahorro y de evitación de datos, tenemos que EUROPOL puede valorar y recoger todas las informaciones personales a su disposición que provengan de criminalidad organizada de carácter internacional. Lo problemático es que estas informaciones no se concentran a los sospechosos sino sobre toda otra persona que pueda dar alguna información para la investigación de hechos penales de interés para EUROPOL[17]. A pesar de que existen mecanismos de control estos son puramente formales y tienen poco sentido en la práctica, como lo son, por ejemplo, los recursos legales, que no se sabe contra quien pueden dirigirse ya que EUROPOL concentra casi 5 gremios dentro de ella. Además, no existe ninguna norma que imponga un deber de informar a los afectados de estos procedimientos de recopilación y comparación y análisis de datos personales. Tampoco ha sido incluida en la Convención ninguna norma que prevea la posibilidad de una anonimización cuando esta sea posible.

Por su parte, el Acuerdo de Schengen de 14 de junio de 1985, entre los Estados de la Uníon Económica de BENELUX, de la República Federal de Alemania y de la República Francesa relativo a la supresión gradual de controles en las fronteras comunes, plantea también problemas de protección de datos[18]. Quizá la primera cuestión que resulte interesante mencionar que es un Acuerdo que no surge precisamente por las preocupaciones de derechos humanos en los países de la

[17] Entre estos hechos destacan: la prevención y la lucha contra el terrorismo; el tráfico de drogas; el tráfico de seres humanos; las redes de inmigración clandestina; el tráfico ilícito de materias radiactivas y nucleares; el tráfico de vehículos robados; la lucha contra la acuñación de monedas falsas y la falsificación de medios de pago; el blanqueo de dinero (excepto infracciones primarias).

[18] Acerca de este acuerdo v. http://europa.eu/scadplus/leg/es/lvb/l33020.htm

Unión Europea, o incluso sobre la protección de aquellos que son sujetos de controles fronterizos.

Schengen habilita una serie de usos informativos de ficheros policiales y por ello en diversas secciones de su normativa se encuentran reglas sobre protección de datos, en especial sobre derechos de los afectados. En una Europa sin fronteras resultaba esencial preservar el intercambio de información policial, que garantizara las labores de prevención y represión de delitos.

La estructura del sistema de información de Schengen (SIS) mantiene un estándar equivalente, tanto en estructura informática, contenidos, protocolos y procedimientos de consulta, los cuales abiertamente dejan los ficheros de carácter local únicamente para la consulta de las autoridades del Estado que las ha recopilado (artículo 92.2). Hay en Estrasburgo una oficina central de apoyo técnico a la que tienen acceso todas las policías nacionales..

Según el artículo 94.3 se incluyen en los ficheros datos personales tales como: nombre y apellidos, y los alias registrados de la persona, rasgos físicos particulares objetivos e inalterables, fecha y lugar de nacimiento, sexo, nacionalidad, indicación de si se trata de personas armadas o violentas, motivo dela inscripción en el registro policial, entre otros.

El Acuerdo de Schengen establece para las partes que lo suscriben diversos problemas para la transposición de las reglas en el derecho nacional. Se trata de reformas legales en las regulaciones del derecho policial, del derecho de extranjería, del derecho de asilo, de las regulaciones sobre armas y explosivos. Pero por sobre todo se trata de reglas sobre protección de datos, en especial sobre normas del tratamiento de datos personales, derechos de información y corrección.

Desde el punto de vista de las regulaciones policiales deben preverse también reglas sobre las condiciones en que se podrá tener acceso al sistema de información de Schengen[19], las disposiciones sobre conservación de los datos, la seguridad prevista para garantizar la integridad de la información, así como las condiciones en que se podrá pedir la colaboración de otras policías. Esto además implica establecer de previo una regulación sobre la entrega o no de datos a terceros interesados, los derechos específicos de los afectados, en especial sobre entrega de información contenida en los ficheros que pudiera causarles perjuicio, pero también sobre la cancelación y destrucción de datos una vez que pierdan sentido a partir del fin para el cual fueron registrados.

El poder de este sistema de información es enorme. Se trata de la compilación de millones de registros de personas. Cuando la policía tiene acceso a la descripción de personas y cosas que es común a todas las policías europeas estaría ampliando su ámbito de investigación a todo el territorio Schengen y a una población potencial de más de 450 millones de habitantes[20]. No en vano, desde la suscripción de los Acuerdos de Schengen y de Dublin, aumentaron las preocupaciones de los Comisionados de la protección de datos de Europa acerca de los potenciales peligros de una observación policial extrafronteras de enormes proporciones. Es por ello que estos encargados plantean, en especial, el aumento de las capacidades de control del funcionamiento de este Sistema de Información, para lo que es necesario crear competencias e instrumentos que hagan posible un control eficiente. Al respecto, los controles deben satisfacer los diversos pilares dentro de los cuales se ha organizado la protección de datos personales en Europa. En primer lugar, la Directiva 95/46/EG del Parlamento Europeo y del Consejo del 24 de octubre de 1995 sobre la protección de las personas naturales en el procesamiento de sus datos personales y sobre el tráfico de sus datos, para

---

19 Una descripción del procedimiento de acceso y de los derechos de corrección que tienen los afectados en el marco de Schengen puede ser consultada (en inglés) en la página del Garante de la Privacy italiano, disponible en: http://www.garanteprivacy.it/garante/doc.jsp?ID=23229

20 Cfr. las observaciones del Comisionado de la Protección de Datos de Suiza del 28 de octubre de 2005, en: http://www.datenschutz.ch/themen/2005_abkommen_schengen_dublin.pdf, p. 5.

alcanzar el primer pilar de los niveles de protección: control en fronteras, visa, control de armas y en parte para el control de drogas. Así como, al menos, las regulaciones del Convenio del 28 de enero de 1981 sobre la protección de la persona en el procesamiento automatizado de sus datos personales para el ámbito del tercer pilar de la Unión Europea, en especial, sobre la cooperación policiaca y judicial en materia penal. Estas dos fuentes dan claridad sobre el tipo de instrumentos y normas que han de ser construidas, principalmente, sobre la independencia del control, las tareas a cumplir, así como los instrumentos a disposición de los encargados de la supervisión del sistema.

Las cuestiones fundamentales de estas tendencias en el marco internacional serían entonces: ¿Hasta qué punto y de qué manera pueden estos aspectos de la "internacionalización de la política criminal"conducir a un deterioro de los niveles de protección constitucional de los ciudadanos y a un recrudecimiento del derecho penal a nivel nacional e internacional? ¿En qué medida y hasta qué punto se transformará la idea de un proceso penal democrático con la ayuda de estos cambios en los medios de investigación con el fin de combatir una criminalidad tan compleja y con tales contornos tan poco definidos? ¿Qué posibilidades reales tiene el derecho a la protección de datos de mantenerse como un ámbito de obligado cumplimiento en la investigación penal ante las urgencias investigativas y de prevención general que se buscan con el uso de un derecho penal contundente en estas áreas?

Es indudable que estas preguntas han de contestarse teniendo como base la idea de que el derecho a la protección de datos y el derecho a la autodeterminación informativa no tendrá el papel que merece en el diseño y construcción de las autorizaciones legales para la intromisión de los órganos del control penal en la esfera de derechos de los ciudadanos. Esto desecha, por imposible, la oportunidad de analizar estas garantías de la sociedad de la información como un complemento práctico que bien podría ser tomado en cuenta frente a valores y principios que hoy tienen, y probablemente tendrán en el futuro, la condición de

correquisitos de validez general para la construcción de instrumentos de persecución mediante la utilización de herramientas de las tecnologías de la información y la comunicación (TIC`s).

4. Policía y prevención del delito. Los problemas de la actividad policiaca desde los principios de la protección de datos.

El uso de las tecnologías de la información para actividades policiales es hoy un hecho ineludible. Ya lo observamos en el entorno de la Unión Europea, pero también sucede en el entorno individual de las policías nacionales, las cuales, a pesar de orientar su trabajo hacia la obtención de fines generales de indudable valor, pueden poner en peligro derechos fundamentales del ciudadano, por extralimitaciones en las que pudieran incurrir, como lo recordó claramente el Tribunal Constitucional españól en una sentencia de 1990[21].

Para lograr una mejor prevención del delito qué mejor que contar con perfiles de personalidad cada vez más completos, no sólo con indicaciones sobre los perfiles de consumo y empleo del ocio, sino también sobre las apetencias, gustos y singularidades éticas, religiosas o políticas, o incluso mediante la observación directa del ejercicio de ciertos derechos como el de huelga y a manifestarse públicamente, de la libertad de expresión, imagen, honor o de la intimidad. Todos estas informaciones personales pueden ser recopiladas fácilmente, integrando datos disponibles en bancos de datos públicos y privados[22] o de las

[21] Sentencia del Tribunal Constitucional Español, 55/1990, (FJ 5)

[22] Las policías nacionales en Centroamérica suelen utilizar, por ejemplo, bancos de datos privados de protección de crédito para identificar personas y para obtener direcciones y contactos telefónicos, entre otras informaciones útiles para la investigación penal. Hacen uso de estos datos como lo haría cualquier otro ciudadano que compra los servicios de estas empresas. La pregunta que se plantea aquí es la siguiente: estos bancos de datos no responden, generalmente, a los estándares de protección de datos, no hay mucha certeza sobre la calidad de la información incluida, así como la posibilidad de ubicar homónimos y personas sobre las que no pesa ninguna sospecha son altamente probables. Además, los afectados por estos usos de información personal no suelen estar informados de que forman parte de estos acervos y de que eventualmente sus nombres y datos personales pueden formar parte de investigaciones policiales de carácter preventivo o

videovigilancias, sempiterna compañera en los espacios públicos de nuestras sociedades, produciendo fichas electrónicas multimediales. El producto final puede ser de enorme utilidad para dar seguimiento a la actividad criminal, pero también para crear condiciones para poner en peligro las libertades[23].

De lo anterior se desprende que el trabajo policial mediante el tratamiento de datos personales augura muchas posibles incidencias en el área de derechos fundamentales de los ciudadanos. Algunas pruebas podrían ser obtenidas con vulneración de tales derechos, sobre todo cuando no existe una base legal para las intromisiones informativas. No obstante, la consideración de la licitud de estos métodos y de los productos informativos que generan debería ser un elemento central del debate sobre estas actividades policiacas. Como lo postuló con razón el Tribunal Constitucional Español en una sentencia de 1984: "*Esta garantía* (se refiere a la de los derechos fundamentales en su doble dimensión de derechos subjetivos y de elemento esencial de una comunidad orientada a la convivencia humana, justa y pacífica) *deriva, pues, de la nulidad radical de todo acto – público o, en su caso, privado –violatorio de las situaciones jurídicas reconocidas en la sección primera del capítulo segundo del Titulo I de la Constitución y de la necesidad institucional por no confirmar, reconicéndolas efectivas, las contravenciones de los mismos derechos fundamentales (el deterrent effect propunado por la jurisprudencia de la Corte Suprema de los Estados Unidos). Estamos, así, ante una garantía objetiva del orden de libertad, articulado en los derechos fundamentales*,…"[24]

Las pruebas obtenidas mediante mecanismos del tratamiento de la información deben tener no sólo un fundamento legal, que separe datos preventivos de los represivos, con claras delimitaciones del destino y fin para el que fueron

represivo. Tampoco el uso que se hace de estas informaciones en el marco de la investigación penal sigue ninguna consideración de protección de datos que permita garantizar su validez y utilidad probatoria.

[23] Cfr. al respecto, con más referencias, Martínez Martínez, Ricard, Tecnologías de la Información, Policía y Constitución, Valencia, Tirant Lo Blanch, 2001, pp. 34 y ss.

[24] Sentencia del Tribunal Constitucional Español, 114/84, (FJ 4)

recopilados, sino también contar con una autorización judicial. Igualmente el marco regulatorio debe contener cláusulas de olvido y de destrucción de los datos cuando ya no sean necesarios. No debe perderse de vista, tampoco, que las intromisiones informativas de la policía han de contar con las autorizaciones judiciales requeridas, debidamente fundamentadas[25] en el principio de legalidad y proporcionalidad, en especial del principio de proporcionalidad aplicable al derecho de protección de datos personales.

Los ficheros policiales, tanto los que se construyan con fines preventivos o represivos, además, deben de cumplir los principios del derecho de protección de datos. En primer lugar, deben atender al principio de calidad de los datos. Los datos personales que se recopilen deben ser adecuados, pertinentes y no excesivos con respeto a fin legal que se pretende llenar con ellos. En cuanto a esto último, el principio de finalidad exige que los datos no sean desviados del fin original para el que fueron recopilados. Junto a ello los datos deben contar con "veracidad" es decir, han de ser precisos y deben hacer referencia a la persona o personas que están bajo vigilancia a partir de una sospecha policial. No sólo han de ser verdaderos, sino que también deben ser comprobados y puestos al día. Este principio conlleva la eliminación, cancelación, rectificación de aquellos datos que no cuenten con precisión y calidad. Contracara de este derecho es la facultad que habrá de reservarse legalmente para que los interesados puedan comprobar el tipo de informaciones policiales que se conservan en ficheros de uso cotidiano para efectos de exigir la eliminación o corrección de aquellos datos que le afecten y que no tengan razón para conservarse o mantenerse activos.

Un tema pendiente en materia de archivos y ficheros policiales es el del derecho al olvido, esto es, a la cancelación de aquellas entradas que ya no sean necesarias para los fines de una investigación. La renuencia a eliminar información ya es muy conocida, sobre todo cuando el inventario de datos en manos de la policía,

[25] Sobre la fundamentación y su esencialidad para justificar las intromisiones en el área de derechos fundamentales cfr. Sentencia del Tribunal Constitucional Español, 54/1996 (FJ)

potencialmente, pudiera servir para evitar la incidencia de delitos a futuro, como un marco más de realización de los fines de la epistemología de riesgos a la que hacíamos referencia al inicio de este estudio. Lo cierto es que los datos procedentes de la investigación policial deben tener un plazo de conservación, cumplido tal deben desecharse cuando ya no sean necesarios para las averiguaciones que motivaron su tratamiento.

Las investigaciones policiales por medios informativos deben realizarse por cauces legales y no fraudulentos. Por más que las herramientas de las tecnologías de la información y la comunicación permitan cada vez más y mejores instrumentos de observación y seguimiento de las actividades de las personas, su uso debe quedar preservado de actuaciones dolosas y fraudulentas que de manera desleal vulneren derechos y garantías, justificando tal actuación en el eventual descubrimiento de un hecho delictivo.

Ciertos derechos derivados de la protección de datos, como el de información previa al afectado del tratamiento de datos personales, tienen, en el marco de la actividad policial, algunas consideraciones especiales. No es difícil imaginar la dificultad de cumplir con este principio cuando se investiga una organización criminal, que podría ser alertada de la actividad policiaca si se les informa que sus datos personales, así como sus actividades están siendo sujetas a la averiguación electrónica. Excepciones al principio del consentimiento podrían aceptarse para los fines de la investigación penal, como la hace la legislación de protección de datos personales de España (artículos 6.2 y 22.3 LOPD). Los datos que correrían esa suerte son aquellos que son indispensables para las actividades para prevenir riesgos y peligros a la seguridad pública o para atender a la represión de actividades criminales.

La protección institucional a través de un órgano de control, como la Agencia de Protección de Datos de España o los Comisionados de la Protección de Datos de Alemania (Datenschutzbeauftragten) es una garantía adicional para el correcto

funcionamiento de las actividades informativas en manos de la policía. La misma Recomendación número R (87) 15, de 17 de septiembre de 1987, emanada del Comité de Ministros del Consejo de Europa a los Estados Miembros y que tenía como objetivo la regulación del uso de datos de carácter personal en manos de la policía, indicaba en sus anexos, Principio 1, como una función de las autoridades de control la de recibir información sobre la creación de nuevos medios técnicos y de sistemas de procesamiento de datos, y de recibir notificación de que se están creando registros permanentes de datos personales para un caso concreto. Con esta actividad, la autoridad de control podría interesarse en los cambios que sufra la actividad investigativa de la policía, así como en la sensibilidad de los datos que están siendo recopilados y de la calidad del tratamiento que se les está aplicando. A pesar de la relativa antigüedad de esta Recomendación, no puede dejarse de apuntar la razonabilidad de esta medida, la cual puede todavía seguirse sosteniendo en el estado actual de la técnica.

La observación del intercambio epistolar en Internet, así como la visita de páginas públicas, como las que ofrecen redes sociales ("*Facebook*", por ejemplo) podrían ser objeto de observaciones policiales. Esto último, no sólo por constituir páginas de acceso público, sino también porque allí se producen interacciones que eventualmente podrían conducir a datos de interés para una investigación penal. Por supuesto, las observaciones que haga la policía de sitios públicos en Internet deben también someterse a los principios generales de la protección de datos, máxime que esta vigilancia y observación se hace sin el consentimiento de los afectados, y porque la información obtenida debe recopilarse atendiendo a su grado de fiabilidad y a partir del cumplimiento de los fines legales de la investigación penal. En cuanto a esto último, no puede perderse de vista que una eventual observación policial de estos sitios públicos en Internet podría entenderse como una injerencia de amplio espectro en la vida y actividades de gran cantidad de personas, que se convertirían en sospechosas por la sola circunstancia de compartir en este tipo de espacios virtuales. Tal injerencia, si no cuenta con una justificación legítima y con la observancia de los principios de la protección de

datos personales, podría generar una ilicitud general de toda la actividad policiaca emprendida.

En concreto, y sobre el acceso a Internet, no debe perderse de vista tampoco que ciertos datos pueden obtenerse sólo mediante la colaboración de los prestadores del servicio de acceso. Entre ellos destacan, por ejemplo, los datos que se dan derivados del protocolo TCP/IP del ordenador que se conecta y de la línea telefónica o sistema de conexión a Internet de que se trate, así como los datos de transacción, los cuales permiten seguir los pasos del navegante en los sitios de Internet visitados. Estos últimos datos darían pie a reconstruir perfiles de uso y consumo de servicios en Internet, datos que ya se ha dicho tienen una enorme sensibilidad.

El manejo y aprovechamiento de estos datos de transacción resultan muy importantes para la actividad investigativa en cierto tipo de delitos, como los de difusión de pornografía en Internet, actividades terroristas o estafas o fraudes electrónicos. Por esta razón no puede simplemente negarse el acceso a los datos transaccionales por su sensibilidad. Los operadores de servicios de telecomunicaciones y los proveedores de servicios deben mantener los datos de tráfico y facturación por un determinado tiempo, pero han de borrarse o tornarse anónimos en cuanto la comunicación termine. Si debe autorizarse una interceptación de las comunicaciones por vías virtuales, entonces los prestadores de estos servicios deben garantizar que las autoridades policiales puedan tener acceso a estos datos transaccionales aun cuando no a la comunicación misma[26].

[26] La doctrina del Tribunal Europeo de Derechos Humanos en los Casos Malone, de 2 de agosto de 1984 (sobre artificios técnicos que permiten registrar números telefónicos sobre un determinado aparato) y Valenzuela Contreras de 30 de julio de 1998 (sobre escuchas telefónicas en el marco de una investigación judicial en España, cuestionando el marco legal para habilitar tales intromisiones con la legislación vigente en ese país en el año 1995), ha dejado de manifiesto la inviolabilidad del mensaje y de los datos relativos a la comunicación que permitan identificar a los interlocutores o receptores de la comunicación, o los datos sobre duración, lugar o tiempo en que tuvo lugar la comunicación o cualesquiera otra característica que permita determinar el tipo de comunicación producida. Además el mismo Tribunal Europeo de Derechos Humanos hizo patente que era necesario el fundamento legal para tales intromisiones, de tal forma que no fueran ejecutadas de manera sorpresiva y que los ciudadanos estuvieran preparados frente a la posibilidad de que tales intervenciones podrían tener lugar dentro de ciertas circunstancias (tipo de delitos, personas que podrían

Además, debería de haber una prohibición general de las vigilancias exploratorias o a beneficio de inventario, ya que esto implica una sensible merma del valor de derechos fundamentales de enorme importancia para la vida de convivencia.

5. Las TIC´s y las garantías de un derecho penal liberal

El vertiginoso desarrollo de las TIC`s ha permitido que haya cambios también muy profundos en las expectativas de investigación en el proceso penal, lo que ha llevado, en parte, a que los órganos del control penal se apertrechen informáticamente para enfrentar diversos retos de la criminalidad moderna[27]. Este apertrechamiento ha conducido a que aumenten sus poderes informativos, lo que junto al fenómeno de la "funcionalización del derecho penal" ha permitido cambios muy profundos en la óptica del derecho a la protección de datos, que en algunos sectores ha venido siendo criticado como una especie de derecho protector de los delincuentes[28].

---

ser objeto de intervención, precauciones a la hora de obtener las grabaciones y procedimientos para su escucha y resguardo y procedimientos para la destrucción o borrado de las grabaciones luego de que hayan servido para un proceso judicial). Las sentencias mencionadas pueden ser consultadas en el sitio WEB del Tribunal Europeo de Derechos Humanos en los dos idiomas de trabajo de esa instancia judicial (inglés y fránces), http://www.echr.coe.int/echr/

[27] No solo los órganos del control penal, sino también los Poderes Judiciales, empiezan a ofrecer cada vez más servicios de acceso a la información. Desde los libros de entrada y salida de asuntos de juzgados y tribunales, hasta la información misma de expedientes, los que en un futuro se visualiza serán accesibles por Internet, y las mismas sentencias, como información jurídica, están siendo ofrecidas de diversas formas. Aun no existe una consideración adecuada del tipo de regulaciones que deben introducirse para proteger la intimidad y la privacidad de las personas, y mucho menos, del uso lícito e ilícito que se puede hacer de estos datos, como podrían ser, también en procesos electrónicos de elaboración de perfiles, para lo cual hay un verdadero estado de indefensión para los ciudadanos. Cfr. al respecto: Gregorio, Carlos, Gestión Judicial y Administración de la Justicia en América Latina, Washington, Banco Interamericano de Desarrollo, pp. 13-17, disponible en: http://www.iadb.org/sds/doc/sgc-Doc13-S.pdf

[28] Recientemente en junio de este año 2008, según lo informa la página del Comisionado Federal para la Protección de Datos, el Bundestag (Parlamento Federal Alemán) ha decidido iniciar los trabajos para producir una reforma integral de la Ley de la Policía Federal Alemana con el fin de habilitarla de mejor manera para la defensa frente a riesgos provenientes del terrorismo. Esta reforma le proveería a la Policía Federal (Bundeskriminalamt) una gran cantidad de posibilidades de intervención, muy superiores a las que se les ha otorgado a las policías estaduales de los Länder, a pesar de que el ámbito de competencia de la BKA es muy restringida en los casos que pretenden provocar esta reforma. Con razón, el Comisionado Federal para la Protección de Datos, Peter Shaar indicó el interés de su oficina por dar seguimiento al proceso de reforma, principalmente por las posibles violaciones al principio de proporcionalidad que podrían generarse con esta ley, por más que contiene una supuesta normativa para proteger el núcleo central de protección del ámbito

La utilización de nuevos medios de investigación obliga a los juristas a observar lo que podemos denominar una perspectiva del Estado Democrático y Social de Derecho, perspectiva que ha sido altamente criticada y sometida a un proceso de desvaloración por parte de críticos que pretenden alcanzar una política criminal contundente, sobre todo en el ámbito de la criminalidad organizada, pero ahora también en la criminalidad cotidiana y en el terrorismo.

La búsqueda de una verdad procesal ahora también a través de medios sutiles e incruentos como los derivados de las TIC´s, significa un reto mayúsculo para el discurso de garantías. Esto último, no sólo por el alejamiento vertiginoso que ha experimentado la legislación del centro de garantías tradicional al que estábamos acostumbrados bajo el lema del "derecho procesal como derecho constitucional aplicado", sino también porque el uso de este nuevo arsenal informativo en manos de los órganos del control penal significa, en última instancia, un riesgo más de hacer la personalidad y asuntos íntimos del ciudadano aun más transparentes. En efecto, la vigilancia electrónica y la comparación de datos de la más diversa índole y calidad, es útil, tanto para fines de control de los delitos, pero también para otros objetivos, que pueden ir desde la evitación de la disidencia como la investigación de costumbres y apetencias. Las TIC`s se convierten –entonces- en la base fundamental de una nueva sociedad panóptica, donde ya casi no hay espacio para esconderse, ni para desarrollar un ámbito privado, libre de intromisiones indecorosas del Estado y de los ciudadanos.

íntimo de configuración de la vida cuando se producen medidas de ataque. Esta reforma contiene, por ejemplo, más allá de las medidas estándar policiales, como lo son los servicios de identificación, los interrogatorios, o las referencias de lugar, también regulaciones sobre observaciones acústicas y ópticas de lugares habitados, vigilancia de las telecomunicaciones, y el acceso secreto a sistemas técnicos de información (búsqueda "on line"). Cfr. Página del Comisionado Federal para la Protección de datos y el Acceso a la Información, en: http://www.bfdi.bund.de/cln_027/nn_533554/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2008/PM-19-08-NachbesserungenBeimBKA-Gesetz.html, consultada en, agosto de 2008. La entrevista en el prestigioso periódico "Die Zeit" de Alemania al Profesor de la Universidad de Frankfurt Spiros Simitis, antiguo Comisionado de la Protección de Datos del Land Hesse, en el año 2001 deja en claro que la protección de datos no fue pensada para proteger delincuentes sino para dar un verdadero sentido a la realización del Estado de Derecho y sus principios en el uso de tecnologías de información dentro del proceso penal, esto, en especial, después del 11 de septiembre de 2001 y los atentados terroristas. Esta entrevista puede ser consultada en: http://www.zeit.de/2001/41/200141_datenschutz.xml?page=2

Por supuesto que estos cambios no han sucedido por el influjo exclusivo de las TIC´s, pero estas han marcado, sin duda, un ritmo especial. En todo caso, ya era posible discernir muchas consecuencias desde que que se empezó a discutir en círculos policiales y de la judicatura, acerca de la necesidad de valorar los aspectos probatorios derivados de largos procesos de vigilancia de las conversaciones y actividades cotidianas de los ciudadanos, con la ayuda de mecanismos audiovisuales, método muy útil en la investigación de las actividades de las mafias del narcotráfico, por ejemplo. Sin embargo, estos instrumentos se suman a las posibilidades extraordinarias que el tratamiento de estas informaciones de audio y video puede generar, lo que aumenta, sin duda, el poder informativo de la investigación penal, y provoca, sin duda, nuevas preguntas que aun permanecen sin respuesta en nuestra doctrina y en nuestra jurisprudencia.

En algunos países, quizá más plásticamente en Alemania, se ha podido observar el aumento contínuo de nuevas autorizaciones legales para el uso de estas herramientas de investigación, con el objetivo de autorizarles la recogida y posterior procesamiento de una enorme cantidad de datos, algunos de ellos de alta sensibilidad, otros conservados en inmensos acervos de información en manos de empresas y compañías privadas, donde las autoridades del control penal solo deben intervenir para obtener las informaciones que requieren para sus investigaciones de gran espectro, que ahora realizan en el marco del terrorismo y el lavado de dinero, principalmente.

Estas formas de criminalidad son presentadas a la opinión pública en la forma de espantosos escenarios de riesgo y peligro, que solo pueden ser conjurados con autorizaciones, cada vez más generosas, para reducir el ámbito de libertades civiles, especialmente de los derechos de defensa y de intervención del acusado, pero también de los derechos de personas inocentes que quedan atrapadas en las complejas y detalladas redes de investigación electrónicas, hoy disponibles también en nuestros países.

El listado de solicitudes para la política criminal es cada vez mayor, y casi todas constan de reducciones para derechos de los ciudadanos y de sus correlativas y generosas autorizaciones para las autoridades de la investigación penal para que causen una más profunda consolidación de un proceso penal contundente.

Hace algunos años, en Costa Rica, se solicitaba a través de una ley, denominada de “Kattia y Osvaldo”, en honor a dos niños que fueron víctimas de diversos tipos de abuso y de agresiones a su vida, que se establecieran listados de todos los agresores sexuales del país, que sus informaciones fueran publicadas en Internet y en otros medios, que se hicieran públicas ahí donde residían, con el objetivo de alertar a la colectividad de que, entre ellos, habitaban sujetos condenados por hechos de abuso sexual contra menores y otros tipos de violencia sexual. La ley fue dichosamente archivada, debido a sus evidentes lesiones a derechos constitucionales, y especialmente a los derechos de autodeterminación informativa de estos ciudadanos, sin embargo, la posibilidad de su aprobación era muy alta, sobre todo por el manejo político que se hizo de estos casos de violencia, y de la oportunidad que encontraron los grupos populistas que impulsan estas reformas para causar en el legislador la necesidad de dictar este tipo de normativas que, en definitiva, solo tienen un tinte de efecto simbólico y de muy escaso impacto en la criminalidad.

Pero es una realidad que ya casi no se discute racionalmente la “necesidad” de estos cambios en la legislación. La política populista solo muestra direcciones hacia el diálogo de batalla con la criminalidad, sin prestar ninguna atención a las garantías indisponibles que se van eliminando inspirados en el canto de sirena de los corifeos del menetekel político criminal.

El caso de Alemania es especialmente interesante, ya que a partir de los cambios generados con la Ley de Combate de la Criminalidad Organizada (OrgKG) y la Ley de Combate del delito (Verbrechensbekämpfungsgesetz), se notó una fuerte

tendencia hacia la conversiòn de la Ordenanza Procesal Penal Alemana en una herramienta del combate del delito. Donde se le entrega a la policía y al Ministerio Pùblico, nuevos y más poderosos instrumentos de observación e investigación, asì como autorizaciones para que aumente sus fuentes de informaciòn[29].

La muestra más clara de estos cambios de orientación se denota en las autorizaciones para la policía para que acceda a bancos de datos privados, así, como para recoger libremente, tratar y transmitir estos datos personales, los cuales pudieron haber sido obtenidos en diversas actividades policiales de carácter preventivo o represivo.

Es posible que el primer problema que se trató, en terminos de eficiencia para el proceso penal alemán haya sido, el del uso del detector de mentiras en el proceso penal, a principios de la década de los años cincuenta del siglo veinte. La tendencia continúa hoy con la utilización del perfil por ADN (o "huella genética"[30]) como instrumento de investigación en delitos sexuales, a pesar de los graves problemas de sensibilidad informativa que este procedimiento implica. Junto a él, sin embargo, se unen otros temas complejos como el uso de grabaciones como prueba, el uso de agentes encubiertos y de personas de confianza en organizaciones criminales, asi como el uso de todo tipo de sustancias extraídas del cuerpo del acusado.

---

[29] Jacob, Joachim, Strafvefahren und Datenschutz -aktuelle Forderungen, Vortrag anläßlich des 5. Wiesbadener Forums Datenschutz im Hessischen Landtag, November 1996, Manuskript, 1996, p. 2.

[30] El perfil por medio de ADN es un poderoso medio de investigación criminal. Inglaterra posee una base de datos nacional con las muestras genéticas de más de cuatro millones de personas, es decir, el 7% de su población. Esta enorme cantidad de información ha sido obtenida a través de la entrega de rutina de muestras corporales de los detenidos por "delitos serios" o sujetos a "penas aflictivas". El almacenamiento de estas muestras es de por vida. En los Estados Unidos el banco de muestras conserva registros de 4.6 millones de personas, 1.5% de la población, y provienen de delincuentes convictos. A partir de enero de 2006, el FBI puede tomar muestras de los sospechosos al momento del arresto, pero éstas pueden ser destruidas a solicitud del interesado si el caso no llega a instancias judiciales. Las pruebas de perfil por ADN tienen un gran prestigio por su precisión, sin embargo, muchos problemas podría afectar su credibilidad, sobre todo la posibilidad que tiene de generar "falsos positivos", además de los muchos cuestionamientos que pueden hacerse a los escasos reparos de protección de datos con los que se suelen construir los bancos genéticos. Esta información ha sido extraída de "The Economist", Conviviendo con el Gran Hermano, op. cit., p. 122.

6. Tendencias derivadas de los ataques terroristas

Un aspecto esencial de estas circunstancias es el hecho de que este tipo de criminalidad vuelve a cada ser humano en sospechoso[31], y las herramientas utilizadas para la investigación han permitido que esta ampliación de la sospecha sea alcanzada generosamente. En este sentido se orienta la introducción de datos sobre la identificación de las personas y otras informaciones en los pasaportes, así como el posible uso futuro de controles biométricos en aeropuertos y otros sitios públicos, colectando datos e informaciones de grandes cantidades de personas para fines aun no establecidos.

Se anuncia también la creación de archivos de datos sobre específicas cuentas de banco, no sólo para evitar delitos fiscales y el lavado de dinero, sino también para el combate del terrorismo, que desarrolla ampliamente la capacidad de las autoridades del control penal para analizar transacciones financieras. Esta capacidad también se extiende para los servicios secretos de diversos países, donde el intercambio de información entre estos servicios y la policía y la fiscalía, ya no parece causar a nadie ningún tipo de preocupación[32].

Quizá lo peor es que estas herramientas arrojan muy poca luz sobre futuros atentados, o permiten, con muy poca probabilidad, detener y enjuiciar a sus posibles causantes y perpetradores, dejando en el balance únicamente un sentimiento de seguridad irreal, a costa de muy valiosas garantías del Estado de Derecho, especialmente del principio de inocencia[33].

---

31 Weichert, Thilo, Datenschutz zwischen Terror und Informationsgesellschaft, Einführungsreferat von Thilo Weichert bei der Tagung RechtsLinks am 10. November 2001 in der Humboldt-Universität Berlin, que puede ser consultado en: http://www.datenschutzverein.de/Themen/Datenschutz_zwischen_Terror_und_Informationsgesellschaft.pdf

32 Weichert, op. cit. La separación constitucional entre servicios secretos y autoridades civiles del control penal había sido, por lo menos hasta la década de los años noventa, un fundamento esencial del Estado de Derecho en la República Federal de Alemania. Hoy, sin duda, las tendencias permitirán un intercambio de datos que sin duda eliminará esa frontera, con consecuencias inciertas para el equilibrio constitucional diseñado luego de los terribles acontecimientos de la Segunda Guerra Mundial.

33 Cfr. Weichert, op. cit.

Lo que era posible en los años setenta podría parecer un juego de niños hoy. Instrumentos de observación desde el espacio, aparatos de escucha y grabación de la imagen cada vez más sensibles y desarrollados, técnicas de comparación de datos a velocidades gigantescas y con capacidad para comparar datos de toda naturaleza, han llegado para quedarse y forman parte del arsenal disponible, y es quizá ahora que la intimidad, la esfera privada y la libertad se han convertido en los derechos fundamentales más valiosos, y los que directamente tienden a desaparecer con esta hambre de información manifestada en la lucha contra el terrorismo globalizado.

7. El derecho a la autodeterminación informativa en el proceso penal

El proceso penal se ha convertido en un instrumento sutil para la recogida, procesamiento, almacenamiento y transmisión de datos personales. Esto es especialmente cierto ante las últimas evoluciones del fenómeno criminal, a tal punto que las intervenciones del proceso, antes caracterizadas por su violencia y claridad, hoy se han convertido en muy discretas observaciones y comparaciones de datos.

Los órganos del control penal, los servicios de seguridad del Estado, y otros órganos, se han venido apertrechando tecnológicamente, de tal manera que el acceso que tienen a las informaciones de los ciudadanos, les permiten ángulos y perspectivas de observación antes desconocidos. Adicionalmente, la transmisión de los datos puede realizarse desde cualquier parte, y los datos obtenidos pueden compararse y analizarse en cuestión de segundos con otras informaciones a fin de lograr perfiles de los ciudadanos, de una claridad y especificidad extraordinarias.

La utilización de informaciones en el proceso penal, sin embargo, sigue desarrollándose, sin tener una regulación jurídica específica, y la ausencia de ese sustento legal sigue debilitándola.

Como lo indica Hassemer, no sólo la seguridad, sino también el concepto de "prevención" ha adquirido una especial relevancia en la perspectiva informativa[34]. La prevención abarca conceptualmente cualquier intento de adelantarse a la producción de un peligro. Los medios para alcanzar esta tarea no tienen límites, y hoy se espera que podamos enfrentarnos a los peligros también mediante mecanismos informativos[35]. Una sentencia del Tribunal Supremo Alemán (Bundesgerichthof) del año 2001 considera que forman parte de la información de la comunicación telefónica también los datos sobre la ubicación de quien telefonea mediante un aparato celular, aun cuando no esté hablando en ese momento, con lo que se abre la puerta para la fabricación de perfiles de movimiento de las personas[36].

A pesar de lo esencial de lo discusión, los aspectos básicos de una regulación de protección de datos no se han planteado siquiera en la reforma penal de América Latina, y sigue haciéndose necesario establecer los pormenores de este problema[37].

---

[34] Cfr. Hassemer, Escheingunsformen, op. Cit., p. 237.

[35] Hassemer reporta como la prensa alemana pone en titulares noticias que tienen que ver con problemas de acceso irrestricto a información de los ciudadanos. Uno de los titulares a que hace referencia es del Tagesspiegel, de comienzos de marzo de 2001, donde se pone en grandes letras: "Alemania es el campeón mundial de la escucha telefónica" y donde se informa que en los grandes países industrializados cada adulto en promedio aparece registrado por lo menos en 200 bancos de datos y de que entre 1988 a 1999 el número de órdenes judiciales para hacer escuchas telefónicas aumentó de 9800 a 12600 o de que el Servicio de Inteligencia Federal (Bundesnachrichtendienst) utilizaba su software de "aspiradora" para investigar palabras clave sospechosas en por lo menos 100 000 telecomunicaciones. Cfr. Hassemer, Erscheinungsformen, p. 238.

[36] Az. 2 BGs 42/2001

[37] Máxime que se escuchan en América Latina las voces de aquellos que quieren poner en Internet la fotografía y la ficha del caso de aquellos sospechosos de haber cometido delitos sexuales o delitos violentos contra la propiedad o estafas, entre otros delitos comunes, con el fin de que la ciudadanía esté informada si entre ellos habita alguien acusado de estos hechos, como ya sucede en casos de pedofilia en Gran Bretaña, Bélgica e Italia. También se ha tenido noticia de esfuerzos por incluir bases de datos sobre la información de perfiles genéticos de todas las personas de una comunidad con el objetivo de investigar hechos delictivos o para determinar algún sospechoso. Es curiosa la frecuencia con que se plantean estos "proyectos de reformas

No hay duda que el proceso penal, mucho más que antes, se ha convertido en un proceso de tratamiento y valoración de informaciones de carácter personal. No sólo la criminalidad organizada y el terrorismo, pero también la delincuencia común (robo de vehículos, extorsiones, estafas y fraudes, entre otros hechos criminales) se desarrollan hoy con diversos niveles de transmisión de datos e informaciones. El éxito de una investigación penal dependerá, entonces, de la calidad de las intervenciones y de la capacidad de los órganos del control penal para valorar los datos obtenidos.

La prueba que está siendo producida, en muchos casos, tiene que ver con diversos grados de complejidad tecnológica y esa complejidad está causando diversos problemas e incertidumbres en el trabajo actual de la justicia.

Recientemente se planteó en Costa Rica, por ejemplo, la licitud o no de una prueba recibida a distancia, mediante videoconferencia, que unió dos países y dos tribunales diversos, donde se estaba recibiendo la declaración de un coimputado en una causa por homicidio de un periodista, que dio información de gran valor para la persecución y castigo de los imputados detenidos en Costa Rica. El Tribunal de Juicio consideró que la prueba había quebrantado garantías[38] pensadas para la presencialidad y la gestión tradicional de la información, no la que ahora puede ser lograda mediante mecanismos tecnológicos, que preservan esa condición de interacción y de virtualidad, en un equilibrio técnico impecable. Sin embargo, la observación de estos medios probatorios con los ojos tradicionales podría estar empañando la utilidad de estas nuevas herramientas de la investigación y de la gestión de los procesos penales.

urgentes" y la facilidad con que son admitidos como instrumentos "eficientes" para la investigación de hechos penales sin plantear siquiera los problemas de proporcionalidad que acarrean consigo.

[38] Tribunal De Juicio del Segundo Circuito Judicial de San José, Sentencia 584-06, a las dieciséis horas del veinte de noviembre del dos mil seis, Expediente Número 03-25233-0042-PE.

Buena parte de estos problemas podría ser resuelto mediante la inclusión de normativa que contemple las reglas de ese equilibrio entre técnica y derechos fundamentales y provea a las autoridades judiciales con elementos de juicio basados en la dogmática de la protección de datos para ponderar la licitud y proporcionalidad de las intervenciones realizadas en las esferas de derechos de los ciudadanos.

Un tal acercamiento es el que resulta consecuente con los dictados constitucionales y con el actual estado de la jurisprudencia costarricense[39]. Sin embargo, el signo de los tiempos indica que manifestarse en el presente estado espiritual del debate político criminal en dirección hacia el respeto de la privacidad y la intimidad o por más limitaciones a la observación sin límites de la comunicación, ubicación o relaciones de una persona resulta, en el mejor de los casos, en hacerse acreedor del calificativo de "abolicionista" y, en el peor de los casos, de "protector de los delincuentes", lo que no sólo lo deja con las "peores cartas"[40] sino que probablemente lo deslegitimaría de acercarse a las cámaras legislativas a dar su opinión acerca de estas evidentes violaciones a la visión tradicional de los derechos fundamentales como derechos de defensa frente al poder omnímodo del Estado y de las autoridades del control penal.

Sin una normativa especial en materia procedimental, como la que ha sido ensayada en Alemania, por ejemplo, se hace muy difícil que nuevos progresos como la informatización de las historias clínicas de los ciudadanos, el desarrollo de sistemas de análisis, grabación y lectura de huellas genéticas, la utilización de medios informáticos para el control de los movimientos de los ciudadanos en vehículos y a pie, puedan ser utilizados sin inquietudes sobre su licitud.

---

39 La jurisprudencia constitucional costarricense ha ido incorporando, entre tanto, los principios de la protección de datos personales como sucedió en el fallo de la Sala Constitucional de Costa Rica, Voto No. 5802-99 de las 15:36 hrs. del 27 de julio de 1999, comentado ampliamente en Chirino, Alfredo y Carvajal, Marvin, El Camino hacia la Regulación Normativa del Tratamiento de Datos Personales en Costa Rica, en: Piñar Mañas, José Luis (Director), Protección de Datos de Carácter Personal en Iberoamérica (II Encuentro Iberoamericano de Protección de Datos, La Antigua, Guatemala, 2-6 de junio de 2003, Valencia, Tirant Lo Blanch, 2005, pp. 232 a 238.

40 Cfr. Hassemer, Erscheinungsformen, p. 239.

La autodeterminación informativa como bien jurídico exige, entonces, y ante el actual desarrollo tecnológico, un replanteamiento, que permita conciliar las evidentes promesas de progreso y avance material que este camino muestra, con los intereses de los ciudadanos de que los ámbitos en que solía concretar sus decisiones, sus sueños y aspiraciones, en una palabra: su autodeterminación, sigan libres del control estatal o de los particulares.

El proceso penal debe tomar conciencia que la protección de la vida privada ciudadano en el actual momento del desarrollo tecnológico, tal y como lo postula con razón Schmitt Glaeser[41], es realmente una "protección de la información". Así las cosas, la justificación para otorgar este "status positivus" del ciudadano se vincula directamente con la tutela de la dignidad de la persona humana, con la necesidad de proteger el libre desarrollo de la personalidad, y con el afianzamiento de la libertad en la sociedad democrática, ya que el control de las informaciones "...aparece como una condición para una convivencia política democrática" .

No se trata de limitar el tratamiento electrónico de los datos que es, en esencia, y esto como una verificación de los posibles desarrollos futuros, una condición para el progreso de los Estados, sino más bien de luchar porque dicho tratamiento se realice de una manera respetuosa de los derechos y garantías del ciudadano, y promocionando la participación social de todos los seres humanos.

Salta a la vista que un acceso a las informaciones públicas permitirá no sólo una mayor transparencia en el funcionamiento de las instituciones, sino también una más eficiente investigación de los delitos, que hoy tienen lugar en todas las diversas formas de comunicación e interacción humanas. No obstante, mejorar las condiciones de investigación de estos hechos, requiere que los ciudadanos no pierdan la posibilidad de preservar su personalidad del acceso extralimitado y

41 Schmitt Glaeser, Walter, Schutz der Privatssphäre, en: Isensee /Kirchhof (Hrsg.), Handbuch des Staatsrechts, Heidelberg, Bd. VI, 1989, pp. 41 y ss.

objetivizante del Estado o de los particulares. Este dilema enfrenta a las sociedades modernas ante una complicadísima y difícil ponderación de intereses, donde entran en juego no sólo las necesidades de información de la sociedad, y la nueva configuración de las relaciones económicas entre los países, sino que habrá de considerarse igualmente el interés del ser humano no sólo a gozar de mayor información en todos los ámbitos del conocimiento y de la cultura ("freedom of information"), como también la necesidad de tutelar a la persona frente al uso desmedido de sus datos personales[42].

El nuevo papel de la intimidad, así planteado, rompe los viejos compartimentos estancos en que se desarrollaba la artificial escisión entre lo público y lo privado, entre lo personal y lo colectivo, entre lo íntimo y lo general, para abrir la puerta a la discusión sobre los espacios sociales donde se produce la interacción entre los ciudadanos para el alcance de objetivos comunes, haciendo ejercicio de nuevos matices de la libertad, potenciados por nuevas formas de comunicación .

Esta nueva dimensión de la intimidad se manifiesta prontamente en el desarrollo jurídico de la década de los setenta y los ochenta, bajo la estructura jurídica del derecho a la autodeterminación informativa, con un profundo arraigo en principios tales como la dignidad humana, la libertad individual, la autodeterminación y la democracia, que antes de ser utilizados como puntos de sustentación vacíos y sin contenido, adquieren una nueva perspectiva en el Estado de Derecho de la sociedad tecnológica.

Es así como resultan, en un principio, como tareas primordiales de este derecho del ciudadano en la "sociedad informatizada", la conservación de un ideal de ser humano, capaz de autodeterminarse y de incidir proactivamente en su entorno, sin

---

42 En la Administración de Justicia, como también en otros campos, como en el uso de datos de prevención del delito para la represión de los mismos, o para intercambiar datos bancarios y financieros para la persecución del terrorismo, existe la necesidad de considerar principios de la protección de datos, que vayan más allá de un mero acceso a los datos, tal y como se postula en el debate sobre la privacidad en la información judicial, cfr. sobre la posible aplicación de los principios de la protección de datos en este campo, Gregorio, op. Cit., p. 15.

temor a que su participación social sea observada ilimitadamente por cualquiera que quisiera a acceder a sus datos personales y a las huellas dejadas por este en su paso por los diversos ambientes en que se desarrolla su existencia. Como lo afirma oportunamente el Comisionado para la Protección de los Datos Personales de Baja Sajonia Gerhard Dronsch[43], a propósito de su disputa con Nitsch sobre el papel de la protección de datos en la actualidad, y como crítica al acercamiento "cuasi-populista" al tema que hoy nos ocupa, "…*la protección de los datos es un presupuesto funcional de la sociedad de la información organizada bajo los supuestos de una sociedad de mercado que desea satisfacer las exigencias democráticas y de derechos civiles. El ser humano "no automático" debe ser protegido en un mundo que se automatiza*".

8. Consecuencias que se derivan para el legislador

El derecho a la autodeterminación informativa, es decir, la posibilidad que tiene el individuo de decidir, fundamentalmente, sobre la entrega y la utilización de sus datos personales[44], no es un derecho sin límites, sino que está sometido a una serie de requisitos que le dan sentido a su razón jurídica.

Casualmente los acontecimientos de terrorismo han llevado a pensar específicamente sobre el ámbito de protección de este derecho, sobre todo frente al potencial uso del “Rasterfahndung”, o investigación por rastros, que consiste en una verdadera ampliación de las redes policiales mediante la comparación electrónica de diversas bases de datos, siguiendo una serie de pistas de carácter criminalístico.

En relación al tema de la amenaza terrorista, y en circunstancias que causaron grave preocupación por este tema en la República Federal de Alemania,

---

[43] Dronsch, Gerhard, Nochmals: Datenschutz in der Informationsgesellschaft, Zeitschrift für Rechtspolitik (ZRP), 1996, pp. 206 y ss.

[44] Sentencia del Tribunal Constitucional Federal Alemán (Ley de Censos), BVerfGE 65, 1 (1), del 15 de diciembre de 1983, (Art. 2 I i.V.m. Art. 1 I GG).

concretamente en el caso del secuestro del señor Schleyer en 1977 por parte del grupo Rote Armee Fraktion, el mismo Tribunal Constitucional Federal Alemán, se refirió al compromiso del Estado de proteger la vida, y que para cumplir con este deber de protección debía tomar las medidas de carácter normativo y de hecho que fueran suficientes para tal objetivo[45].

Sin embargo, el equilibrio de derechos entre los intereses de la colectividad y los del ciudadano no es cosa fácil de alcanzar, aun cuando hay un acuerdo de que el derecho a la autodeterminación informativa debe ceder cuando haya un sobrepeso en interés de la seguridad. No obstante, las limitaciones que este derecho sufra han de contar con un suficiente basamento legal, y en la ley que así lo acuerde, se establezcan las ponderaciones derivadas del principio de proporcionalidad que resulten necesarias.

En el caso de las medidas contra el terrorismo, como cualquier otra medida que afecte el derecho a la autodeterminación informativa, debe el legislador preguntarse acerca de la idoneidad de la medida para alcanzar los fines legales. Es decir, debe preguntarse si no habrá otro medio, menos lesivo de derechos fundamentales que pudiera utilizarse para cumplir el fin legal. Una medida que genere, por ejemplo, cantidades exageradas de información, que las autoridades de la investigación penal no pueden procesar, sería una afectación directa al principio de proporcionalidad.

Igualmente debe preguntarse el legislador sobre la necesidad de las medidas. Es decir, que aún cuando resulten idóneas para cumplir el fin legal, habría que preguntarse acerca de su necesidad, y al respecto, si otros medios, en otra parte del ordenamiento jurídico, podrían atender las urgencias de un peligro como el del terrorismo, o, por ejemplo, si realmente existe un peligro tan serio como para exigir

[45] Sentencia del Tribunal Constitucional Federal Alemán (Caso Schleyer), BVerfGE 46, 160ff (164) del 16 de octubre de 1977.

medidas tan agresivas en los derechos fundamentales del ciudadano. Esta última es una pregunta central del principio de proporcionalidad en esta materia.

También ha de tomarse en cuenta el principio de claridad de las normas, el cual exige que las limitaciones al derecho a la autodeterminación informativa sean claras y entendibles para el ciudadano, especialmente sobre la extensión de las medidas y las consecuencias del procesamiento de datos. Aquí hay una cuestión de gran relevancia para la discusión jurídica, ya que esta función de claridad de las normas y de las medidas mismas debe reducirse o incluso eliminarse cuando por razones de la misma eficacia de las medidas deben conducirse las mismas en secreto, especialmente acerca del hecho de que se están acumulando datos personales de los ciudadanos con el fin de realizar sobre ellos específicas manipulaciones y tratamientos. No obstante, se mantiene, incluso en estos casos, la obligación de informar en las disposiciones generales de la regulación cuáles serán los objetivos del procesamiento, y cuáles datos, para cuál objetivo serán procesados[46]. Esto es muy importante, ya que el sometimiento del procesamiento de datos, con cualquier fin, debe hacerse para los objetivos especialmente indicados, y nunca para obtener datos "a beneficio de inventario", esto es, con el fin de acumularlos para un objetivo posterior, no definido.

Junto al principio de sometimiento al fin debe sumarse el principio de división de los poderes informativos del Estado, es decir, la necesaria diferencia entre un Estado totalitario donde hay una unidad de información en todas las instancias de control y vigilancia, así como de aquellas que cumplen funciones en la cotidianeidad de los ciudadanos, y donde no hay modo de controlar que intercambien y se comuniquen entre sí los datos personales que hayan recopilado[47]. En un Estado Democrático y Social de Derecho debe haber, forzosamente, una separación entre los poderes informativos del Estado, muy

---

[46] Bäumler, Die Gesetzesentwürfe über die Geheimdienste en: Bull (Editor), Sicherheit durch Gesetze?, Baden-Baden, Nomosverlagsgesellschaft, 1. Auflage, 1987, pp. 123 y ss. (especialmente, p. 125).

[47] Cfr. Tinnefeld, Marie-Theres; Ehmann, Eugen, Einführung in das Datenschutzrecht, München, Wien, R. Oldenbourg Verlag, 2. durchges. Aufl., 1994, p. 36

especialmente entre aquellos que recopilan información con el fin de prevenir delitos y los que la recopilan con el fin de aplicar la ley y reprimir los delitos. La separación también cuenta entre los poderes civiles de policía y los servicios de seguridad.

Por lo anterior, y desde la perspectiva del derecho a la autodeterminación informativa, debe discutirse si hay posibilidad de intercambio de información entre lugares estatales de procesamiento que tienen diferentes funciones, muy especialmente en el caso de los servicios de seguridad del Estado, los que estarán siempre interesados en procesar datos provenientes de las recaudación de impuestos, de las actividades policiacas preventivas, de la información financiera y bancaria, información médica y de otras fuentes públicas, disponibles a través de acceso electrónico.

No hay duda que las posibilidades de lesión de la autodeterminación informativa del ciudadano son extensísimas en una vida cotidiana profundamente marcada y dependiente de los usos de la información. Por ello, resulta indispensable que los requisitos provenientes de la proporcionalidad (fundamentación de la intervención, y medición de la idoneidad y de la proporcionalidad en sentido estricto), así como la claridad de la legislación que permite la intromisión sean elementos sine qua non, sin los cuales no es pensable un estándar regulatorio en materia de investigación penal que sea idóneo[48]. , así como los regulaciones sobre obligaciones de información por parte de la agencias que hacen la recopilación de información, acerca de los objetivos y fines, así como sobre los deberes de eliminación o borrado de la información, luego de que se han cumplido los objetivos para los cuales fueron recopilados los datos.

[48] Por ejemplo, la ley de protección de datos personales que se discute en Costa Rica, actualmente, representa un paso esencial para acercarse a ese estándar regulatorio, sin embargo aun son indispensables las previsiones específicas en materia procedimental que den sentido a la actividad investigativa mediante mecanismos informativos de amplio espectro. Sobre las características de este proyecto de ley en Costa Rica y su contexto normativo y constitucional, cfr. Chirino Sánchez y Carvajal Pérez, El Camino, op. cit., pp. 241 a 256.

9. A manera de conclusión

Un importante campo de desarrollo para el derecho a la autodeterminación informativa lo constituye, sin duda, el proceso penal. Los cambios introducidos por la tecnología en la dimensión y estilo de las investigaciones criminales no sólo han traído mejoras en el trabajo cotidiano de las autoridades de la investigación, sino que también han acarreado nuevos retos y problemas al legislador y a la doctrina, a fin de tutelar también en este ámbito el derecho del ciudadano a controlar quién, cuando y bajo qué circunstancia toma contacto con sus datos personales.

La discusión en el ámbito europeo, en especial en la República Federal de Alemania, donde el tema es altamente sensible, se ha desarrollado en la dirección de más cambios legislativos en el sentido de introducir límites al procesamiento de datos personales en manos de la policía y el ministerio público. Estos límites tienen como objetivo proteger a la persona de excesos que lesionen el principio de proporcionalidad y su derecho a la autodeterminación informativa. No se desea limitar las posibilidades de investigación o de comprometer el interés público en la obtención de la verdad real, sino que lo que se desea es que la calidad e intensidad del procesamiento de datos personales en este campo respete las reglas impuestas por la Sentencia sobre la Ley de Censos de 1983 del Tribunal Constitucional Federal Alemán, que es en este país la "carta magna" del procesamiento de datos.

En otros países europeos esta discusión se ha iniciado tarde o con otros intereses políticos, sobre todo en el marco de la creación de la EUROPOL, que sin duda será un tema de interés en los próximos años, no sólo en cuanto a la cooperación policial a lo interno de la Comunidad Europea, sino también en la medida en que pueda demostrarse un compromiso de esta organización por proteger la autodeterminación informativa de los ciudadanos de la Comunidad Europea y sobre todo de los extranjeros, quienes siguen manifestando, en materia de protección de sus datos personales, una situación jurídica de segunda categoría.

América Latina, y en concreto Costa Rica, no parecen escapar a la evolución tecnológica, la cual también ha llegado un poco más lentamente y con rezago también a la policía y al ministerio público. Los problemas que se puedan presentar en este campo aún podrían ser tema de especulación, sin embargo, resulta necesario reflexionar ahora sobre los mismos, con el fin de que el proceso penal no presente en este campo lesiones a principios constitucionales no previstos en virtud del carácter incruento, sutil y hasta apetecido de los medios tecnológicos que pueden tener incidencia en el éxito de una investigación criminal.

Hemos podido observar que el tema de la tutela de la autodeterminación informativa o libertad informática en el ámbito de la administración de justicia penal apenas cobra vigencia e importancia en el ámbito legislativo. Además, las leyes de protección de datos personales transcurren lentamente en el cauce legislativo y no parecen contar con un ambiente político propicio, mucho menos las regulaciones de carácter especial en materia de seguridad, que equilibren las condiciones del desarrollo tecnológico de las investigaciones penales y los derechos de los afectados.

Algunos proyectos de ley intentan una regulación de posibles lesiones al debido proceso cuando se utilicen pruebas obtenidas mediante violación a los principios del derecho de la persona a ser protegido frente al procesamiento de sus datos personales. Esta oferta legislativa constituye, por ello, un importante aporte al derecho comparado, el cual, por lo menos en el ámbito latinoamericano, no ha tomado posición acerca de los problemas de tutela de la persona frente al procesamiento de sus datos personales en la administración de justicia.

Queda por discutir y analizar en concreto los diversos medios tecnológicos utilizados por la policía y por el ministerio público para la investigación criminal, a fin de determinar las posibles lesiones al derecho a la autodeterminación informativa y al principio de proporcionalidad, así como el ámbito de problemas

que han de resolverse, para ello juega un papel importante una investigación sobre el nivel de tecnología instalada en el sistema penal, el tipo de instrumentos utilizados y software, así como también la política institucional de manejo de datos. También resulta esencial la reflexión sobre el papel que pueden cumplir aquí las prohibiciones probatorias, un tema apasionante y de radical importancia en este ámbito.

Resulta muy prometedor, y augura un interesante desarrollo de la discusión científica, el creciente interés por el problema de la tutela de la persona frente al tratamiento de sus datos personales. Sólo cabe esperar en este campo no sólo un vigoroso esfuerzo legislativo sino también una reflexión a lo interno del sistema de justicia penal, a fin de evitar que esta herramienta tecnológica se constituya en un medio más para aumentar la violencia del funcionamiento del sistema de justicia penal, en este caso una violencia peligrosísima, por su carácter casi intangible y seductor.

Para que haya un futuro posible para la protección de datos en el equilibrio de necesidades de seguridad y prevención del delito, habrá de trabajarse fuertemente en las siguientes direcciones:

- Buscar el uso más inmediato del principio de necesidad, casi como un imperativo categórico, en la discusión de todos los cambios proyectados en el proceso penal y en las leyes penales propias de la criminalidad organizada y del terrorismo.
- Proponer una política de ahorro de datos y de evitación de informaciones como efectos inmediatos de las políticas informativas de los órganos del control penal, principalmente de la policía, en lo que se refiere a temas de prevención de delitos.
- Una división técnica entre las informaciones derivadas del proceso penal con fines de la investigación penal y aquellas que cumplen fines de evitación policíaca de peligros y que son orientadas también a la prevención.

- Incluir en los Códigos Procesales regualciones específicas acerca de las averiguaciones y pruebas que se obtienen de forma causal a través de herramientas e instrumentos de las TIC´s.
- Incluir, además, prohibiciones probatorias específicas cuando se haya afectado el derecho a la autodeterminación informativa de ciudadanos acusados.