Revue

Droit International, Commerce, Innovations & Développement

Année 1 – Numéro 2 – Novembre 2012

"La protection électronique de données personnelles et le habeas data"

CREDIMI - UNIVERSITE DE BOURGOGNE - CREDESPO

Editorial

Le deuxième numéro de la revue Droit international, commerce, innovations et développement (DICID) traite de la protection des données personnelles face aux technologies de l'information et de la communication, sujet que chacun s'accorde à regarder comme brûlant.

Le récent procès intenté à Google par des citoyens suisses à propos des « indiscrétions » commises par le système Google Street View présage que la justice peut dans une certaine mesure sauvegarder les droits des personnes (notamment leur droit à l'image). Cependant, les personnes sont le plus souvent désarmées face à la puissance des géants de l'Internet, faute d'outils de protection efficaces. Les potentialités d'atteintes à la vie privée, à l'image, ainsi qu'à la réputation, sont tellement importantes, que l'enjeu dépasse de simples considérations techniques : ce n'est rien moins que la place de l'individu dans une société hyper-communicante qui pose question.

Pourrait bien se mettre en place, si l'on n'y prend garde, un immense jeu planétaire qualifiable d'omni transparence. Dans cette utopie à rebours, tout le monde aurait la possibilité de voir tout le monde, la légitimité de l'ensemble reposant sur la réciprocité : de sorte que vouloir préserver son espace privé déconsidérerait voire éliminerait d'emblée toute prétention à utiliser le système.

Un tel raisonnement reposerait cependant sur un sophisme. En effet, les technologies de l'information et de la communication n'ont pas été conçues par les citoyens, elles n'ont été validées par aucune institution susceptible d'exprimer des valeurs morales ou juridiques. Il s'agit d'outils offerts de manières diverses, pour les plus puissants de manière directement ou indirectement marchande, et, comme en tout domaine, il n'existe aucune raison valable à nos yeux de ne pas protéger les utilisateurs, où qu'ils se trouvent.

Car dans ce domaine la protection doit avoir une visée internationale. A ce stade, il existe deux manières de voir la question. L'on peut d'abord se situer sur un plan non-marchand, ce qui nous conduit sur le terrain des droits de l'homme: dans les domaines où la puissance étatique s'exerce, notamment lorsque l'exercice de la justice pénale donne lieu à la collecte et au traitement de données personnelles, c'est la seule optique imaginable. Mais l'on peut aussi intervenir sur le terrain marchand, celui des puissants acteurs de ce qu'on peut nommer le marché électronique international, et, en passant par la logique contractuelle, réfléchir à l'émergence d'un corps de règles applicable au consommateur international de l'Internet.

Ces approches sont à notre sens complémentaires. Il convient cependant, dans l'un et l'autre cas, d'évaluer convenablement leur efficacité. C'est à cette réflexion que nous invite le présent numéro, qui s'inscrit totalement dans l'esprit de critique scientifique de la société internationale marchande, en vue de la comprendre et d'étudier les régulations possibles, que propose DICID.

Nous remercions vivement Laurence RAVILLON et Patrick CHARLOT, respectivement directrice du CREDIMI et directeur du CREDESPO, d'avoir bien voulu accueillir sur les sites de chacun des deux laboratoires le présent numéro.

Isabelle Moine-Dupuis

Maître de conférences

Université de Bourgogne

Centre de Recherches sur le Droit des Marchés et des Investissements Internationaux

Mot du directeur

S'il est banal de reconnaître les apports que les nouvelles technologies comportent pour la vie contemporaine, il l'est moins de mettre en relief les dangers que leur utilisation peut engendrer pour les droits fondamentaux. Cependant, et précisément grâce aux technologies de l'information, nous prenons tous les jours connaissance de nouveaux enjeux. Quel est le rôle de l'État face à cette problématique ? Sans doute, celui-ci doit protéger les droits de la personne, en trouvant un équilibre en dépit d'exigences contradictoires. Mais la réglementation est-elle la seule réponse ou bien est-il aussi possible d'envisager un remède dans l'autorégulation ?

Le premier des articles composant le présent numéro examine le régime juridique de l'utilisation de la vidéoconférence en matière pénale, tant en terme de droits internes comparés, qu'en terme de droit international ; il met en relief les avantages que cette technologie comporte dans la mesure où sont respectés les principes de contradiction et d'immédiateté.

Dans la deuxième contribution nous trouvons une analyse du cas *Google Street View* tel qu'il s'est présenté devant les autorités suisses. L'article nous fournit un examen très complet qui rappelle les fonctionnalités de *Google Street View* ainsi que les étapes qui ont conduit à la saisine du Tribunal fédéral suisse, avant de présenter de manière critique le jugement rendu par ce dernier tribunal. Cette réponse, émanant de la première cour suprême et se prononçant de la sorte sur la légitimité des procédés de Google, sera à n'en pas douter fondamentale pour les législations comparées.

Ensuite, les lecteurs trouveront une analyse du délit informatique et pourront s'étonner de l'absence dans la législation pénale mexicaine d'un encadrement des délits informatiques en raison de défauts d'ordre formel.

La quatrième contribution est l'oeuvre d'auteurs uruguayens analysant le droit à l'oubli sur l'Internet. L'article examine la notion même de droit à l'oubli, ses antécédents ainsi que son application pratique, mettant en relief de nombreuses situations, différentes de celles qui peuvent se présenter sur le réseau social Facebook, et dans lesquelles des informations personnelles peuvent être détournées. On trouvera aussi des développements sur la protection de ce droit par certaines législations, spécialement celle de l'Uruguay. Cette contribution nous éclaire aussi sur les différences entre le droit à l'intimité et le droit à l'oubli, celui-ci étant plus large.

Notre deuxième numéro s'achève sur l'analyse des notions de *privacy-by-design* et *privacy-by-law,* notamment pour démontrer les limites de la première: insécurité juridique, confusion des concepts et vulnérabilité des données personnelles, de l'intimité, de la dignité et même de la liberté. Les auteurs proposent enfin, un remède à ces dangers, avec le renforcement du droit à la vie privée à travers la réaffirmation d'une privacy-by-law.

Lusitania Villablanca Cerda
Avocate chilienne

Sommaire

Marco jurídico internacional de la utilización de videoconferencia en materia penal.*[1]

INTERNATIONAL LEGAL FRAMEWORK OF THE USE OF VIDEOCONFERENCE IN CRIMINAL MATTER.

Jorge Albornoz Barrientos.[2]

Marko Magdic[3]

En la siguiente investigación, presentamos un breve análisis de legislación Internacional y comparada que habilita la utilización de Videoconferencias como medio de Cooperación Internacional en Materia Penal. Se exponen algunos casos de países europeos y sudamericanos, como también un breve estudio del contexto jurídico chileno. Las fuentes utilizadas son principalmente documentos de trabajo, antecedentes jurisprudenciales y normativa interna de cada país.

In the following research, we introduced a brief analysis of international and comparative law that enables the use of Videoconference as media for International Cooperation in Criminal Matters. Exposed some cases of European and South American countries, as well as a brief study of the Chilean legal context. The sources used are mainly working papers, judicial precedents and internal regulations of each country.

PALABRAS CLAVE: Videoconferencia, Cooperación Internacional, Protección de Víctimas y Testigos, Globalización, Criminalidad Transnacional.

ABSTRACTS: Videoconference, International Cooperation, Protection of victims and witnesses, Globalization, International Criminality.

"Los mismos medios tecnológicos que fomentan la mundialización y la expansión transnacional de la sociedad civil, también proporcionan la infraestructura para ampliar las redes mundiales de la sociedad 'incivil', vale decir, la delincuencia organizada, el tráfico de drogas, el lavado de dinero y el terrorismo."

Kofi A. Annan.

Introducción

En la actualidad, en el ámbito de la persecución penal, a la Videoconferencia se le reconocen diversos usos y virtudes, entre los cuales destaca su importancia respecto de la mejor utilización de Recursos. V.gr., la utilización de ésta herramienta puede disminuir en gran medida la cantidad de audiencias suspendidas o procedimientos abandonados por la falta de ratificación de los cargos producto de la imposibilidad de los testigos o de las víctimas de concurrir a declarar al lugar de realización del juicio. Asimismo, se economizan recursos al no tener que montar grandes

* Cuando en el presente artículo se encuentre la abreviatura VC, nos estaremos refiriendo a Videoconferencia. Asimismo, se advierte que la sigla IP, se refiere a la abreviación del inglés *Internet Protocol*, mientras que la sigla ISDN, se refiere a la

operativos, por ejemplo cuando tiene que trasladarse a un imputado fuera de algún centro de reclusión para que declare en el tribunal en el contexto de algún procedimiento en el que participe, ya sea como testigo, informante o incluso como autor.

Asimismo, la utilización de este sistema contribuye a la mayor realización de variados fines dentro del proceso penal, como la protección de testigos y de víctimas que muchas veces, producto del temor que les infunde tener que encontrarse con un agresor, deciden abandonar el proceso o poner trabas para su participación en él.[4] En definitiva, su utilización permite acortar la brecha entre la disponibilidad de medios tecnológicos de que disponen los entes persecutores, por una parte, y por otra las organizaciones delictivas transnacionales.

En ese contexto, es que sus virtudes se han reconocido en gran cantidad de normativa Internacional y Comparada, como también abundante Jurisprudencia, y a pesar de eso se hace difícil encontrar alguna obra que estudie disposiciones internacionales que permitan su utilización como herramienta de Cooperación Internacional, o en su defecto normativa comparada que sea de utilidad al momento de solicitar la realización de la diligencia.

Precisamente, con este artículo pretendemos entregar a autores e intervinientes en el proceso penal, un estudio que sirva de referencia para nuevas investigaciones, ya que al menos bajo la perspectiva de su uso internacional, éste tema no ha sido tratado en ningún cuerpo de doctrina jurídica de circulación amplia.

Así las cosas, producto de la mencionada falta de material doctrinario, la bibliografía utilizada para la elaboración de ésta investigación consiste principalmente en documentos de trabajo más bien técnicos, en el sentido de ser ponencias, discursos, conferencias, reuniones de coordinación, etc. Así también, se expondrá normativa comparada e internacional, haciendo referencia a Tratados Internacionales tanto vinculantes en Chile, por ser el país de origen de los autores, como a otros en el círculo europeo que se refieren expresamente a la herramienta en estudio.

Respecto del Derecho Comparado Sudamericano, se expondrán antecedentes extraídos de fuentes directas de los ministerios públicos respectivos, relativas a su legislación interna e Internacional, fallos de sus tribunales, y antecedentes de la experiencia de sus estados. Para esto, se recurrirá a las respuestas del Cuestionario de Salvador de Bahía, que es un instrumento de trabajo de la Asociación de Ministerios Públicos del Mercosur (agrupación de países sudamericanos). Precisamente, en el último apartado del presente artículo, se expondrán los resultados entregados por la representación de la Fiscalía Nacional de Chile.

Realizado dicho análisis, y pudiendo llegar a una conclusión respecto del estado de la cuestión en lo relacionado con la Cooperación Internacional, se expondrán las perspectivas generales que pueden preverse sobre la herramienta estudiada.

En las conclusiones y reflexiones finales, esperamos fortalecer aún más la idea de que con la utilización de la Videoconferencia, no sólo no se vulnera ninguno de los derechos de los intervinientes en el Proceso Penal, sino que muy por el contrario, muchas veces se garantizan en mayor y mejor medida.

Análisis y definición del término videoconferencia

Se ha afirmado por la doctrina, que "la Videoconferencia es un sistema de comunicación interactivo que transmite simultáneamente la imagen, el sonido y los datos, permitiendo una comunicación bidireccional plena, en tiempo real, de tal manera que se posibilita un mismo acto o reunión a la que asisten personas que se encuentran en lugares diferentes"[5].

No obstante estar de acuerdo con dicha afirmación, consideramos que para formar una definición más completa, debe agregarse algunos elementos que se echan en falta. Por una parte, debe entenderse a como videoconferencia, no sólo al sistema que permite una reunión a distancia, sino que también a la reunión en sí misma. Así también, debe entenderse que una videoconferencia puede ser bidireccional, en donde existen dos puntos distantes que se comunican, o multidireccional, como veremos.

A. Interpretaciones del término Videoconferencia:

1. Interpretación amplia:

Nos podemos formar una idea general del significado del concepto, a raíz del desglose de la propia palabra, entendiendo como primera aproximación que se trata de una conferencia realizada por medio de video.

Sin embargo, entendiendo videoconferencia como concepto amplio, encontramos en primer lugar hay que tener presente que "la palabra 'Teleconferencia' está formada por el prefijo 'tele' que significa distancia, y la palabra 'conferencia' que se refiere a encuentro, de tal manera que combinadas establecen un encuentro a distancia".[6]

A su vez, entre la palabra Teleconferencia, y la palabra Videoconferencia, existe una relación de género y especie. De tal manera que debemos entender a la Videoconferencia como una especie de encuentro a distancia, que cuenta con la particularidad de llevarse a cabo mediante un dispositivo de video y audio, que a través de una conexión bidireccional o multidireccional, permite que dos o más personas puedan verse y oírse simultáneamente.[7]

Así, podemos apreciar que puede tratarse de una conexión bi o multi direccional, puesto que a través de videoconferencia pueden comunicarse dos o más partes. Si bien conceptualmente podría aceptarse la idea de que exista una videoconferencia unidireccional, veremos que por los principios del proceso penal, que exigen la posibilidad de contradicción de los declarantes, en éste ámbito no será admisible la declaración por medio de video y audio de una sola parte.

Por su parte, debemos destacar que lo que contrasta a una videoconferencia, de por ejemplo una llamada telefónica, es que en la primera cada una de las partes que en ella participan puede apreciar la imagen de las otras, lo que resulta de extrema importancia si consideramos que la gran mayoría de los mensajes que se perciben en una conversación frente a frente son no verbales.[8]

Para graficar la importancia que esto tendría para un sistema procesal penal, imaginemos la diferencia que constituiría producir una prueba mediante la lectura de la declaración de un testigo, versus la posibilidad de interrogarlo directamente. Por ejemplo, en el caso del interrogatorio a una víctima de abuso sexual, en el cual el correlato emocional a la declaración constituye parte importante del grado de convicción al que llegue el tribunal.

En Chile, nuestras magistraturas se han referido al respecto, sosteniendo que "en efecto, el tribunal apreció la prueba directa de la existencia del delito, constituida por el atestado del menor de iniciales J.I.R.T., quien a través del circuito de videoconferencia entregó al tribunal un relato hilado, pormenorizado, acabado, ubicado en tiempo y espacio, el cual iba acompañado de un correlato emocional compatible a los hechos que explayaba. El menor víctima pudo transmitir al

---

Ciencia Política y de la Administración de la Universitat de Valencia, ISSN 1135-0679, Nº 56, 2006, págs. 25-59. El autor cita a JOSÉ DE LA MATA AMAYA, en su ponencia denominada *La utilización de la videoconferencia en las actuaciones judiciales*, presentada en el seminario de formación continuada del CGPJ, realizado en Madrid, del 17 al 19 de septiembre del 2003.

[6] VÁSQUEZ GONZÁLEZ, SANTIAGO RAÚL, *Fundamentos de la Videoconferencia, y su implementación en el Ministerio Público del Paraguay*, Fiscalía General del Estado, Dirección de Informática, Administración de Redes y Sistemas. Documento de trabajo presentado en el primer taller sobre uso de la Videoconferencia en la Cooperación Jurídica Internacional, en el marco de la Reunión Preparatoria de la VII Reunión de Ministerios Públicos del MERCOSUR, celebrada el 28 de abril de 2009, en la sede del Ministerio Público del Paraguay, p.5.

tribunal los episodios vividos durante su convivencia al cuidado de su padre no sólo en forma verbalizada, sino que incluso pudo gesticular con sus manos a que era obligado a hacer, al tiempo que era capaz de describirlo con palabras. De ésta forma, el tribunal se cercioró que existe en el relato del menor, además de las características ya mencionadas, una coherencia entre lenguaje verbal, el corporal (…) y el emocional (un notorio cambio del estado emocional en los momentos en que éste se refería a cuestiones generales introductorias de su relato a aquellos en los que hacía referencia al episodio abusivo)."[9]

2. Sistema de Videoconferencia.

Además de denominarse Videoconferencia a una "especie de reunión" a distancia, tal como se expuso más arriba, se le da la misma calificación al "sistema" que permite que ésta se realice.

De esta forma, encontramos que en la segunda de las mencionadas acepciones, se entiende que "la Videoconferencia consiste básicamente en un sistema interactivo de comunicación que transmite simultáneamente y 'en tiempo real' la imagen, el sonido y los datos a distancia, permitiendo relacionar a un grupo de personas situadas en dos o más lugares distintos como si la reunión y el diálogo se sostuviese en el mismo lugar"[10].

3. Tipos de Sistemas de Videoconferencias:

Dentro de la concepción de Videoconferencia, entendida como sistema de conexión a distancia, podemos encontrar distintos tipos, los que a su vez harán variar diferentes factores en su utilización, como lo son la distancia a la que se podrá celebrar una reunión, calidad de la imagen, seguridad y privacidad en las comunicaciones y costos para su utilización.

A estos distintos tipos de sistemas, pasaremos revista brevemente:

a) Circuito Cerrado de Televisión:

Éste consiste en que en lugares ubicados a escasa distancia (como por ejemplo dos salas de juicio oral, ubicadas una al lado de la otra), se forma una línea de video a través de cableado, que permite que se transmita entre ellas lo que está sucediendo en ambas simultáneamente.[11]

b) Método IP (Internet Protocol):[12]

"Utilizando Internet, procedimiento de videoconferencias utilizando el *Video Phone* y la conexión a Internet, además del *software* y el equipamiento adecuado."[13]

Cabe señalar, que si bien mediante este sistema se obtiene una videoconferencia de manera prácticamente instantánea, y con un bajísimo costo, podrían producirse problemas tanto de conectividad como de lentitud y distorsión de imagen y/o sonido. Esto, debido a que en su utilización se depende de la capacidad de ancho de banda, y de la congestión de la línea utilizada en dicho momento.

---

[9] 7º Tribunal de Juicio Oral en lo Penal de Santiago, Chile, causa rit 246 – 2007, analizado junto a otra jurisprudencia chilena en ALBORNOZ BARRIENTOS, Jorge; MAGDIC, Marko, *La videoconferencia en el Proceso Penal Chileno. Evolución en su utilización como medio de Cooperación internacional*, en NEXUS IURIS, Revista del Centro de Estudios del Derecho de Arica, año 2012, N° 1, Abril/Arica, Chile. P. 38.p. 72.

[10] TIRADO ESTRADA, JESÚS J., *Videoconferencia y Equipos Conjuntos de Investigación*, Material elaborado por el autor en su calidad de Fiscal en la Unidad de Apoyo al Fiscal General de España, p. 4.

[11] Este sistema se utiliza, por ejemplo en el derecho inglés, en el caso en que "*si el testigo es un niño que comparece en un caso relativo a una infracción sexual o de violencia, puede declarar en una sala contigua a la de audiencias y su declaración será retransmitida por video.*" MIREILLE DELMAS-MARTY, *Procesos Penales de Europa (Alemania, Inglaterra y País de Gales, Bélgica, Francia, Italia), Association de Recherches Pénales Européennes* (ARPE), Traducción de MORENILLA ALLARD, Pablo, Editorial EDIJUS, Año 2000, p. 175.

Asimismo, puede sostenerse la posibilidad de utilizar dicha modalidad en el ordenamiento jurídico chileno, en virtud del universalmente aceptado principio del Interés Superior del menor, complementando así lo dispuesto en el artículo 310 de nuestro CPP, que dispone que "El testigo menor de edad sólo será interrogado por el presidente de la sala, debiendo los

Como precedente, cabe mencionar que "la aplicación de software y servicio propietario Skype fue empleada por primera vez en febrero de 2011 en Estados Unidos (caso de tráfico de drogas en el Estado de Georgia en que el abogado defensor del acusado, Arturo Corso, de Corso, Kennedy & Campbell, solicitó al juez y consiguió que se realizara declaración por Skype de un testigo que se encontraba en Texas).[14]

De todas formas, dichos problemas podrían salvarse si se contara con una línea exclusivamente dedicada a la práctica de la videoconferencia.

c) Método ISDN (Integrated Services Digital Network):

En español conocido como RSDI, por la traducción de su sigla (Red Digital de Servicios Integrados), es un conjunto de estándares de comunicaciones que permiten un único cable o fibra óptica para transportar voz, servicios de red digital y vídeo, en una conexión rápida dedicada a la transmisión de datos. Ésta se puede utilizar para tener acceso a Internet o a una video conferencia, en donde "la comunicación se produce en condiciones excelentes de seguridad, celeridad y calidad, gracias a la encriptación y a la elevada capacidad de los canales de transmisión que se utilizan".[15]

El ISDN, es la evolución de la línea telefónica normal, y presenta como gran diferencia que además de la señal de voz tradicional puede transportar otro tipo de datos, entre los cuales se puede considerar la imagen de la Videoconferencia.

Cabe destacar que en este sistema "las señales de audio y video que se intentan transmitir, se encuentran por lo general en forma de señales analógicas, por lo que para poder transmitir ésta información a través de una red digital, ésta debe ser transformada mediante algún método a una señal digital, una vez realizado esto, se deben comprimir y multiplexar estas señales para su transmisión. El dispositivo que se encarga de este trabajo es el CODEC, que en el otro extremo de la red, realiza el trabajo inverso para poder desplegar y reproducir los datos provenientes del punto remoto."[16] Es decir, el CODEC es el codificador y decodificador que se encarga de transformar las señales de audio y video analógicas en digitales en el punto de envío, y viceversa en el punto de llegada.

d) Cuadro Comparativo: [17]

Habiendo analizado las ventajas y desventajas de estos sistemas, podemos resumir que si se cuenta con una conexión IP de alta velocidad, es preferible su utilización para llevar a cabo una Videoconferencia, producto de que si bien el sistema de Circuito Cerrado de Televisión tiene menores costos, y mayor confiabilidad y seguridad, mientras su disponibilidad dependerá de la conexión que se haga en cada lugar que pretenda realizarse, éste es demasiado limitado en cuanto a alcance, lo que lo hace lisa y llanamente inutilizable para una videoconferencia internacional.

Asimismo, si comparamos entre los sistemas IP y ISDN, encontramos que si bien ambos tienen un alcance ilimitado mientras se cuente con los equipos necesarios, su disponibilidad varía en gran medida por los equipos utilizados, como de la existencia de una Línea ISDN, mientras que para la línea la utilización de IP basta con una línea telefónica, que en la actualidad puede encontrarse en la mayor parte de los países medianamente desarrollados.

Respecto de la Seguridad, encontramos que el sistema ISDN es más confiable que el sistema IP, pero menos que el circuito cerrado de televisión mientras que los costos de llevar a cabo una Videoconferencia mediante el sistema ISDN, muchas veces derivan en cifras astronómicas, mientras que para el sistema IP solamente debe considerarse la contratación permanente de una línea telefónica de alta velocidad. Esto, hace que aun siendo más segura la conexión mediante la primera de estas vías, sea muy preferible la utilización de la segunda.

Por todo esto, y tal como se grafica en el cuadro comparativo, parece evidente que el sistema más eficiente para utilizarse en una Videoconferencia Internacional, es el IP, aun cuando requiera de una línea de alta velocidad.

B. Características de la Videoconferencia.

Respecto de este punto, encontramos que la Videoconferencia principalmente "se caracteriza por ser:

a) Integral, ya que permite el envío de imagen (personas, video, multimedia, etc.), sonido (voz de alta calidad, música, etc.) y datos (ficheros automáticos, bases de datos, etc.)

b) Interactiva, pues permite una comunicación bi o multidireccional en todo momento;

c) Sincrónica, es decir, en tiempo real, pues transmite en vivo y en directo, desde un punto a otro o entre varios puntos a la vez."[18]

C. Definición de Videoconferencia.

Finalmente, luego de haber estudiado las distintas acepciones del concepto de Videoconferencia, como sus características, podemos ensayar una definición que podamos utilizar para el presente trabajo, y en donde se agreguen los requisitos esenciales de cada una de las definiciones estudiadas.

De ésta forma, podríamos decir que la Videoconferencia, es una especie de reunión a distancia, de dos o más personas, efectuada gracias al sistema tecnológico del mismo nombre, el cual produce un intercambio bi o multidireccional de imagen y sonido, permitiendo una comunicación en tiempo real, y prácticamente en las mismas condiciones que se darían si los interlocutores estuviesen en el mismo punto geográfico.

Finalmente, resulta válido entender videoconferencia, como "una especie de reunión a distancia de dos o más personas, efectuada gracias al sistema tecnológico del mismo nombre, el cual produce un intercambio bi o multidireccional de imagen y sonido, permitiendo una comunicación en tiempo real, y prácticamente en las mismas condiciones que se darían si los interlocutores estuviesen en el mismo punto geográfico."[19]

Normativa internacional sobre la utilización de videoconferencia en materia penal

Como se mencionó, existen numerosas razones que legitiman el uso de la Videoconferencia como medio de Cooperación Internacional en materia Penal, y precisamente es por sus virtudes, y por tanto beneficios que entrega a la comunidad internacional, que estas razones han sido recogidas en los textos internacionales de Derecho Público y en las regulaciones internas de derecho comparado que prevén su uso.

Así, el uso de la videoconferencia ha sido previsto legislativamente en numerosos países y en muchos otros se viene practicando conforme a habilidades genéricas de uso de las nuevas tecnologías y admisiones jurisprudenciales específicas. Por ejemplo, en "la mayoría de los países europeos la utilizan normalmente en los procesos judiciales. [Mientras que] en Latinoamérica su uso es cada vez más frecuente y con resultados altamente satisfactorios."[20]

En ese sentido, puede apreciarse un amplio número de Tratados Internacionales que reconocen el uso de la Videoconferencia como medio de Cooperación Internacional en materia Penal, y de todos estos, se expondrán aquellos considerados como más paradigmáticos o

Por otra parte, aquellos que no la reconocen expresamente, sí consagran el derecho a la defensa, plasmando principios que no sólo no constituyen un obstáculo para su uso, sino que muy por el contrario, sientan directrices y constituyen derechos que en muchos casos, tal como se expondrá en este apartado, pueden respetarse más cabalmente gracias a esta herramienta tecnológica.

A. Autorización tácita a la realización de Videoconferencias en Tratados Internacionales, a través de los principios rectores del Proceso Penal.

El derecho al debido proceso es reconocido por los Tratados Internacionales con mayor relevancia a nivel del orbe, ocurriendo lo mismo con el derecho a la defensa jurídica. Ambos se concretizan en procedimientos penales regidos por principios que perfectamente pueden legitimar la utilización de la VC en el marco del proceso penal. Dentro de estos, encontramos por ejemplo principios como los de Inmediación y Contradicción.

1. Inmediación.

El principio de inmediación exige que el tribunal haya percibido por sí mismo la producción de la prueba, y aquí "parece conveniente apuntar que la inmediación –sustantivo compuesto, integrado por un prefijo 'in' y un núcleo 'mediación'- expresa, positivamente, la idea de una vinculación directa, vale decir, sin el tamiz de cosas ni de personas, [en definitiva] ausencia de intermediarios"[21]

"Desde luego la inmediación no necesariamente es, o debe ser absoluta, porque aunque se trate de un juicio oral, es posible introducir ciertos elementos de prueba por lectura o exhibiéndolos (fotografías, planos, etc.)"[22], ya que en realidad, éste principio "apunta a la aprehensión sensorial directa por el juez, de la información que emana de los órganos de prueba."[23] De ésta forma, respecto de la Percepción directa por parte del Juez, "si ésta comprende tanto la inmediata –física- como la mediata –intermediada por un mecanismo audiovisual-, entonces sería dable sostener que la declaración testimonial prestada a través de videoconferencia, respeta el principio de inmediación, en la medida que el Tribunal puede mirar y escuchar…"[24] al declarante.

Aquí, cabe hacer hincapié en que lo que más se busca evitar con la consagración de éste principio, es la reproducción del nefasto panorama que se daba en los procedimientos penales de antaño (aún vigentes en algunos países), donde a través de un funcionario judicial, el juez recibía una apreciación muchas veces parcial y subjetiva de la información producida a través de los medios probatorios y de confrontación de la prueba, además de posibilitar en mucho mayor medida las posibilidades de corrupción.[25]

La idea principal, entonces, es que toda persona tenga derecho al acceso directo ante el tribunal, sin intermediarios de ningún tipo.

En tal sentido se reconoce en la Declaración Universal de los Derechos Humanos, cuyo art. 10 prescribe que "toda persona tiene derecho, en condiciones de plena igualdad, a ser oída públicamente y con justicia por un tribunal independiente e imparcial, para la determinación de sus derechos y obligaciones o para el examen de cualquier acusación contra ella en materia penal", principio que es recogido en similar redacción por el pacto de san José de Costa Rica en su art. 8 Nº 1[26], y por el Pacto Internacional de Derechos Civiles y Políticos en su art. 14 Nº 1.[27]

---

[21] TAVOLARI OLIVEROS, Raúl, *Informe en Derecho, solicitado por el Fiscal Nacional Guillermo Piedrabuena Richard, sobre Videoconferencia*, Viña del Mar, Julio 2003, p. 6.

[22] CHAHUAN SARRÁS, Sabas, *Manual del Nuevo Procedimiento Penal*, Tercera edición actualizada y aumentada, Edit. LexisNexis

2. Contradicción.

"El principio contradictorio garantiza que la producción de las pruebas se hará bajo el control de todos los sujetos procesales, con la finalidad [de] que ellos tengan la facultad de intervenir en dicha producción, formulando preguntas, observaciones, objeciones, aclaraciones y evaluaciones, tanto sobre la prueba propia como respecto de la de los otros"[28]

En éste sentido, la Convención Americana sobre derechos Humanos, en su art. 8 Nº 2 letra f, reconoce el "Derecho de la defensa a interrogar a los testigos presentes en el tribunal y de obtener la comparecencia, como testigos o peritos, de otras personas que puedan arrojar luz sobre los hechos". A su vez, el Pacto Internacional de Derechos Civiles y Políticos consagra en su art. 14 Nº 3 letra e), el derecho "a interrogar o hacer interrogar a los testigos de cargo y a obtener la comparecencia de los testigos de descargo y que éstos sean interrogados en las mismas condiciones que los testigos de cargo".

Así, de la consagración en Derecho Internacional de los principios expuestos, puede percibirse que se reconoce el derecho de todas las personas a ser oídas por un juez o tribunal competente, como también a interrogar o hacer observaciones a las pruebas rendidas, quedando de manifiesto, atendida la naturaleza de los cuerpos jurídicos mencionados, que no se establece ni cómo debe ser oída la persona, ni en qué condiciones deben llevarse a cabo el interrogatorio cruzado y las observaciones a la prueba, sin perjuicio de las demás garantías existentes.

De esta forma, podemos apreciar que con la realización de la Videoconferencia para las diligencias mencionadas, no se están vulnerando los derechos garantizados por estos tratados internacionales, sino que muy por el contrario, en determinadas situaciones podrían protegerse en mayor y mejor medida. Por una parte, "el principio de contradicción no se vería afectado, puesto que la fiscalía como la defensa y el acusado pueden interrogar y contrainterrogar, respectivamente, al testigo desde la sala de audiencias, mediante la ventaja que importa el uso de tal sistema, cual es permitir estar en más de un lugar al mismo tiempo"[29]. Por la otra, el hecho de que el uso de videoconferencia permita que se realicen, por ejemplo, juicios orales que sin ella serían imposibles de llevar a cabo, contribuye a que se confirme el derecho con que cuentan las personas y se protejan con mayor efectividad.

B. Reconocimiento expreso de la práctica de Videoconferencia en normas Internacionales.

Como se adelantó, tal como podemos interpretar de los principales Tratados Internacionales de Derechos Humanos, que la realización de Videoconferencias en el marco del Proceso Penal es perfectamente válida, existen otros tratados, ciertamente más específicos y de aplicación eminentemente práctica, que tratan el tema de manera directa y expresa. Algunos de ellos, a saber:

1. Estatuto de la Corte Penal Internacional.[30]

Aprobado en el marco de la Convención de Roma, el 17 de julio de 1998, contempla en su art. 69.2 la posibilidad de que el testigo preste testimonio "por medio de una grabación de video o audio" y en su art. 68.2, habilita la presentación de pruebas "por medios electrónicos u otros medios especiales", cuando con esa medida se proteja a víctimas o testigos. Incluso, el art. 63.2, admite esta posibilidad respecto de los acusados, en el evento de que estando presentes perturbaren constantemente la realización del juicio, pudiendo hacérseles salir de la sala donde se desarrolle el

2. Convenio Europeo relativo a la Asistencia Judicial en materia Penal.

Aprobado el 29 de mayo de 2000 por el Consejo de Ministros de Justicia y Asuntos Exteriores (de la Unión Europea) –regula la práctica de las videoconferencias en su artículo 10.

Dicho artículo, está destinado a sustentar y facilitar la utilización de dicho sistema con vistas a superar las dificultades que pueden surgir en casos penales cuando una persona se encuentre en un Estado miembro y no sea oportuna o posible su comparecencia para ser oída en otro Estado miembro. En particular, éste artículo establece disposiciones relativas a las solicitudes y a la realización de audiciones por videoconferencia, y se aplica en general a las audiciones de peritos o testigos, si bien, bajo determinadas condiciones que figuran en el apartado 9, puede aplicarse también a las audiciones de personas inculpadas.[31]

3. Convención Europea de Asistencia Mutua en Materia Penal.[32]

La Convención Europea de Asistencia Mutua en Materia Penal, fue suscrita en Estrasburgo el 20 de abril de 1959 por los miembros del Consejo de Europa y entró en vigor el 12 de junio de 1962. Asimismo, se han agregado dos protocolos (1978 y 2001), que buscan modernizar e implementar nuevas estrategias a la convención.

Su objeto es que los Estados Partes se proporcionen la más amplia asistencia mutua en los procedimientos relativos a materias penales cuya represión en el momento de pedir la asistencia sea de competencia de las autoridades judiciales del país requirente. Se excluyen expresamente: las detenciones, ejecución de condenas o delitos de carácter militar que no estén contempladas con arreglo al derecho penal común y ha sido modificada y complementada por dos Protocolos Adicionales, suscritos con posterioridad a la misma.

En el artículo 9 del segundo de sus protocolos (Estrasburgo, 8 de noviembre de 2001), se establece la posibilidad de realizar videoconferencias en los siguientes términos:

'Si una persona estuviera en el territorio de una Parte y tuviera que prestar testimonio como testigo o perito ante las autoridades judiciales de otra Parte, ésta última, cuando no sea conveniente o posible que la persona que deba prestar testimonio comparezca en persona en su territorio, podrá solicitar que la audiencia se realice mediante videoconferencia."

Esto, según lo dispuesto en los párrafos 2 a 7 del mismo protocolo, los que se refieren a las condiciones necesarias para poder llevar a cabo la videoconferencia, y los requisitos formales, como las autoridades que deberán estar presentes, los antecedentes a acompañarse, los costos de la operación, etc.

4. Convención de las Naciones Unidas contra la delincuencia Organizada Transnacional.[33]

"La Convención de Palermo, consta de 41 artículos, forma parte del Derecho Penal Internacional y su importancia se debe a que, por primera vez, un instrumento penal internacional lograba unificar definiciones y establecer tipos penales en común para todos los Estados Partes"[34]. En su art. 24, se exige a los Estados Parte que adopten medidas apropiadas para una protección eficaz de testigos o de víctimas testigos en investigaciones de delitos materia de la Convención.

Entre las medidas pertinentes se reconoce la posibilidad de establecer normas probatorias que permitan las declaraciones sin hacer peligrar la seguridad de los testigos, dándose como ejemplo el uso para ello de diversa tecnología de la comunicación como videoconferencias y otras.[35]

[31] Informe explicativo del Convenio, de 29 de mayo de 2000, relativo a la asistencia judicial en materia penal entre los

Reconocimiento y legitimación jurídica de la utilización de la videoconferencia en el derecho comparado

En este apartado, se analizarán algunos casos europeos, para de esa manera formarnos una opinión a lo menos superficial respecto del estado de la VC, en lo relativo a su utilización y legitimidad de esta en el viejo continente, para posteriormente adentrarnos en la realidad sudamericana, que es la que más vincula a nuestro país, principalmente en el marco de la Reunión Especializada de Ministerios Públicos del Mercado Común del Sur (en adelante REMP), la que precisamente nos entregará el contexto para el análisis de las normativas comparadas de nuestros países vecinos.

A. Aproximaciones al caso Europeo.

Además de los convenios vinculantes en la Unión Europea estudiados con anterioridad, que constituyen el Derecho Internacional atingente, también en materia de Derecho comparado encontramos que importantes potencias han adoptado el sistema de VC como medio de Cooperación Internacional. A saber:

1. Italia.

En éste contexto, a Italia "corresponde el mérito de haber jugado un papel de país pionero en materia de regulación y uso de videoconferencia en el plano internacional, por motivo del art. 16 de la ley Nº 367 de fecha 5 de octubre de 2001"[36]. Dicha normativa, fue la que finalmente incorporó a su Código Procesal penal, como art. 205 ter, el uso de la VC con países extranjeros para la audición de testigos y peritos, así como de inculpados en el extranjero que no puedan ser transferidos a Italia.

2. Portugal.

Asimismo, "en Portugal, tanto la Ley de Cooperación Judicial Internacional 144/99 (…), como el Código Procesal penal –en sus arts. 317 y 318 en relación con el artículo 111- contemplan la posibilidad de empleo de la videoconferencia (…)"[37] en materia Internacional.

3. Francia.

Idéntico es el caso de Francia, donde en el art. 706-71 de su Código Procesal Penal, se señala que "cuando las necesidades de la investigación lo justifiquen, la audición o el interrogatorio de una persona así como una confrontación entre varias personas pueden ser realizadas en distintos puntos del territorio de la República encontrándose conectados por medios de comunicación". La misma norma, agrega en el párrafo segundo que dichas disposiciones son aplicables a casos internacionales, por motivos de solicitudes emanadas de autoridades judiciales extranjeras o de actos de cooperación realizados en el extranjero a solicitud de autoridades francesas.[38]

4. España.[39]

Finalmente, en el caso de España, el artículo 229 de la Ley Orgánica del poder Judicial, prescribe en el Nº 3 de dicha disposición, luego de reconocer los principios de oralidad, concentración e inmediación, que en éste marco, las "actuaciones podrán realizarse a través de videoconferencia u otro sistema similar que permita la comunicación bidireccional y simultánea de la imagen y el sonido y la interacción visual, auditiva y verbal entre dos personas o grupos de personas geográficamente distantes, asegurando en todo caso la posibilidad de contradicción de las

Ante el hecho de que ese artículo no prohíbe la realización de videoconferencia Internacional, pero tampoco lo permite expresamente, es que dicha disposición se ha visto complementada con un elevado número de tratados de asistencia jurídica mutua con diversos países, como se da por ejemplo, en los casos de México[41], Colombia[42] y Brasil.[43]

B. Realidad Sudamericana según el Cuestionario de Salvador de Bahía sobre Videoconferencia.

Tal como se expuso en la parte introductoria del presente apartado, en éste se expondrán las normativas más relevantes de nuestro cono sur americano, para lo cual, recurrimos eminentemente a los registros de la propia Reunión Especializada de Ministerios Públicos del Mercosur[44] (REMPM[45]), y específicamente, a su instrumento de trabajo denominado "Cuestionario de Salvador de Bahía sobre Videoconferencias"[46], el cual fue presentado y aprobado en la Reunión Preparatoria de la VI REMPM, en virtud de la proposición de la Delegación de Paraguay, la que "estimó pertinente revelar información referente al uso de dicha herramienta en los diferentes Ministerios Públicos, considerando la tendencia regional y la importancia de la implementación de la videoconferencia en la cooperación internacional."[47]

1. Argentina.[48]

Según las respuestas del Cuestionario de Salvador de Bahía antes aludido, Argentina cuenta con equipos para realizar videoconferencias y utiliza tecnología IP, con propia infraestructura y "desde su implementación, en mayo de 2008 [y hasta la fecha de presentación del cuestionario, 28 de abril de 2009], no se habían realizado videoconferencias en la materia que nos interesa".

Respecto a la legislación atingente, "la Constitución Nacional –al incorporar el bloque normativo supranacional, art. 75, inciso 22- autoriza la posibilidad de realizar declaraciones judiciales mediante el sistema de videoconferencias; […ya que se encuentra incorporada en] el estatuto de la Corte Penal Internacional"[49] y en la Convención contra la Delincuencia Organizada Transnacional[50], como asimismo, existe un proyecto de ley iniciado por moción parlamentaria en la República de Argentina, elaborado por la Secretaría General de Coordinación Institucional del Ministerio Público Fiscal de la Nación, que busca regular expresamente el uso de videoconferencia en dicho Estado, incorporando los artículos 246, 382 bis y 384 bis, como también, modificando los artículos 355, 359 y 391.

Sin perjuicio de la citada legislación, que incluye el uso de videoconferencia con fines judiciales de manera expresa, se sustenta el uso de ésta en que "constituye una forma de practicar la

---

[41] Entra en vigencia con fecha 26 de julio de 2007 en los Estados Unidos Mexicanos, y su artículo 18 está exclusivamente dedicado a la audiencia por videoconferencia. GODOY BERROCAL, María Elena, "Breves notas sobre Videoconferencia", documento de Trabajo para la Reunión Especializada de Ministerios Públicos del Mercosur.

[42] "La ley 1.179 de fecha 31 de diciembre de 2007, aprobó el Protocolo adicional al Convenio de Cooperación Judicial en materia penal entre la República de Colombia y el reino de España –celebrado el 29 de mayo de 1997- (…) que en su art. 6 Nº 2, prevé el uso de Videoconferencia entre ambos Estados." GODOY BERROCAL, cit (n.27).

[43] "Con fecha 22 de mayo de 2006, se celebró el convenio de cooperación jurídica y asistencia judicial en materia penal entre el Reino de España y la República Federativa de Brasil, en donde se estableció en forma expresa en el Capítulo III 'Formas de Asistencia', artículo 17 'Videoconferencia' que: '*Las partes podrán convenir en la obtención de declaración a través de videoconferencia con arreglo a las condiciones que se especifiquen en cada caso*'." GODOY BERROCAL, María Elena, cit (n.27).

[44] Que "surge de una decisión del Consejo del Mercado Común (CMC) del MERCOSUR reunido en la ciudad de Asunción el 19 de junio del año 2005 (…) por la necesidad de contar con un mecanismo ágil en el relacionamiento entre los (Ministerios) Públicos de los Estados Partes y Asociados, para lograr potenciar las acciones conjuntas para la prevención, investigación y represión del crimen organizado, narcotráfico y el terrorismo, entre otros."
http://www.ministeriopublico.gov.py/reunion/pdf/rempm.pdf , consultada el día 19 de Abril de 2012.

[45] Cuenta con Estados Partes, y Estados asociados, siendo los primeros de ellos, Argentina, Brasil, Paraguay, Uruguay y Venezuela, mientras que los segundos, son Bolivia, Chile, Colombia, Ecuador y Perú. Las REMP se organizan semestralmente, tendiendo a una reunión preparatoria previa a cada una, y la organización es responsabilidad de la Presidencia Pro Tempore.

[46] "Los objetivos de Dicho Cuestionario son: analizar la viabilidad técnica y jurídica de la implementación de la

contradicción, de materializar el derecho de confrontación y, por lo tanto, modo de ejercer el derecho a la defensa en juicio."

Todos estos argumentos, han sido recogidos en cierta manera por la jurisprudencia de los Tribunales Superiores de Justicia, por ejemplo, en el caso en que "La Cámara Federal de Mar del Plata ha tenido oportunidad de expedirse al respecto el 11/4/2005, en el marco de un recurso de apelación interpuesto por el representante del Ministerio Público Fiscal contra la decisión de primera instancia que había denegado la solicitud de recibir una declaración indagatoria en el trámite de solicitud de asistencia jurídica requerida por un juez penal de sentencia de la República del Paraguay.

El tribunal -integrado por los Dres. Ferro y Tazza- consideró que la recepción de la declaración indagatoria solicitada deviene una medida procesal que se halla incluida en la asistencia jurídica que la Nación se ha comprometido a prestar en el marco de los distintos instrumentos que reglan la materia, analizando el art. 17 en función del art. 2 Protocolo de Asistencia Mutua en Asuntos Penales entre los Estados Parte del Tratado de Asunción, como también que robustecen la amplia concepción que se propugna y las disposiciones de la Ley de Cooperación Internacional en Materia Penal 24.767 (LA 1997-A-29), aplicables como norma supletoria." Con lo que finalmente la autoriza.

2. Bolivia.[51]

En este caso, no existe legislación que prevea expresamente la utilización de la videoconferencia en materia de Cooperación Internacional ni en materia local. Sin embargo, en el último de los casos, "al referirse a los medios de prueba y libertad probatoria, la norma procedimental penal establece que el Juez admitirá como medios de prueba todos los elementos lícitos de convicción que puedan conducir al conocimiento de la verdad histórica del hecho, de la responsabilidad y de la personalidad del imputado. Pudiendo utilizarse otros medios además de los previstos en éste libro (Código de Procedimiento Penal), hecho que abre la posibilidad y permisibilidad de utilizar la herramienta técnica de la videoconferencia. Al respecto existe un instructivo emitido por la máxima autoridad del Ministerio Público por el que se instruye la recepción de declaración de peritos por videoconferencia aplicada a casos y procesos penales en el ámbito nacional".

En cuanto al equipamiento técnico, si bien el Ministerio Público no cuenta con los dispositivos necesarios para practicarla, se prevé la posibilidad de recurrir a empresas privadas que ofrezcan el servicio, aunque hasta abril del año 2009 (fecha de respuesta del cuestionario), no se había realizado ésta operación, ni tampoco recibido o solicitado dicha diligencia a en el marco de la Cooperación Internacional, por lo que tampoco existe jurisprudencia respectiva.

En éste sentido, se expresa que sin perjuicio de los tremendos beneficios que conlleva ésta práctica, sus posibles debilidades se enmarcan en la imposibilidad, por parte de dicho Ministerio Público, de contar con el equipamiento técnico en todos los distritos.

3. Brasil.[52]

Por su parte, Brasil permite de manera expresa esta práctica,[53] y su Ministerio Público cuenta con los medios técnicos para realizar videoconferencias, tanto en el ámbito Nacional como en el Internacional, utilizando respectivamente, tecnología IP e ISDN, y en las comarcas que no cuentan con dichos dispositivos, deben ser contratados mediante licitación pública, o en determinados casos de suma urgencia, por licitación privada. Asimismo, su frecuencia de uso es más importante a nivel estadual, y hasta abril del presente año [2009], se habían realizado 3.619

Respecto de la Jurisprudencia, se señala que existen precedentes contradictorios respecto de la utilización del sistema de videoconferencia en el marco de la justicia penal, por donde la mayor parte de los precedentes son contrarios a esta práctica, se deben a la falta de argumentación por parte de los requirentes. En éste sentido, en el área internacional, existen precedentes de requerimientos con resultados positivos, y sin embargo, se han producido inconvenientes respecto del sistema utilizado, ya que en la mayoría de las comarcas existe sistema con tecnología IP, mientras que en el ámbito europeo, se trabaja con tecnología ISDN, contando estos entre las debilidades del sistema según el emisor de las respuestas, además de posibles problemas técnicos, como por ejemplo, fallas en imagen y sonido.

Sin embargo, se estima que sin duda, el sistema de videoconferencia es más económico, más rápido y que no afecta los principios del debido proceso. Siendo estos puntos los que se aconseja fundamentar siempre en la solicitud de la diligencia, como también, se recalca la importancia de que MERCOSUR adopte las medidas para actualizar la legislación y así permitir de manera expresa la práctica de videoconferencia.

4. Colombia.[54]

La Fiscalía a nivel nacional, cuenta con siete equipos de videoconferencia que van rotando a los diferentes lugares de Colombia, y que si bien se utilizan con tecnología IP, también soportan el uso de ISDN.

Respecto de la frecuencia de uso, "al interior del país, a través de la red FISCATEL (que es la intranet nacional de la Fiscalía General de la Nación), se utiliza con frecuencia la videoconferencia, especialmente en la aplicación de la ley 975 de 2005 para transmitir las versiones libres de las personas postuladas al procedimiento y beneficios de la ley 975 de 2005 a aquellos lugares en donde se concentran las víctimas de su accionar delictivo.

También se han realizado Videoconferencias con otros países como Holanda y España, por solicitudes elevadas por los mismos. Actualmente la Fiscalía de Colombia se encuentra trabajando conjuntamente con Colombia Telecomunicaciones S.A. E.S.P., para convenir el servicio internacional de videoconferencia a fin de continuar la dinámica de los procesos iniciados a las personas extraditadas a los Estados Unidos de América y postuladas a la Ley de Justicia y Paz.

A su vez, respecto de la legislación existente, La Videoconferencia está establecida entre otros en los artículos 386 del Código de Procedimiento Penal *Impedimento del testigo para concurrir* y 486, referente al traslado de testigos y peritos. Asimismo, su uso se encuentra reglamentado mediante acuerdo 2114 de octubre 1 de 2003, proferido por la Sala Administrativa del Consejo Superior de la Judicatura.

En el ámbito internacional, Holanda requirió a la Fiscalía General de la Nación en el sentido de lograr una videoconferencia con un testigo que se encontraba en Colombia. Se llevó a cabo la diligencia solicitada por un término de dos días y la comunicación se dio en óptimas condiciones.

Por lo anterior, es que se considera a la videoconferencia como un medio rápido y efectivo, aunque sin la debida implementación, no es necesariamente económico.

5. Paraguay.[55]

Paraguay adquirió recientemente equipos para videoconferencias que utilizan tecnología IP, y con anterioridad, se recurrió a organismos internacionales, como las Naciones Unidas

expresa, su sustento jurídico sería la Libertad Probatoria, consagrada en el art. 173 del Código Procesal Penal.

En el ámbito de la jurisprudencia, si bien no existen precedentes de tribunales nacionales, si se ha producido Cooperación Internacional, entre otros casos, en una declaración de 8 de abril de 2003, en la cual "España solicitó la declaración del testigo de un hecho punible de Estafa, residente en Paraguay, y con dicha declaración se logró la condena de los inculpados." Cabe señalar al respecto, que se trata del "primer caso de declaración testifical mediante el sistema de videoconferencia realizado a través de Internet"[56]

Cabe también recalcar, que dicha declaración marca un precedente importantísimo, y que causó gran impacto mediático, donde se señaló que "una videoconferencia que duró unos cuarenta minutos, bastó para dar por concluida una instancia judicial que suele llevar semanas (cuando no meses) atravesando burocracias administrativas y diplomáticas."[57]

Presumiblemente, por ésta práctica, junto con los posibles altos costos, es que se señala como debilidad del sistema el posible uso indiscriminado, y se recalca que su uso debe ser responsable. Esto, no obstante, de que se reconocen sus cualidades, tales como adaptación a las necesidades impuestas en la práctica de los distintos actos procesales y que no afecta a los principios de Inmediación, Publicidad, Contradicción y Oralidad.

6. Uruguay.[58]

En éste caso, el Ministerio público no cuenta en el ámbito institucional con ésta herramienta, debiendo brindar el servicio la empresa Estatal de telecomunicaciones ANTEL, que dispone de tecnología IP e ISDN, existiendo salas especialmente habilitadas para la prestación de éste servicio. Asimismo, dicha herramienta se utiliza a nivel nacional, sólo en el ámbito de la capacitación.

Respecto a su regulación, el uso de ésta herramienta no está mencionado de forma expresa en él la Legislación Nacional, y sin embargo, se puede fundamentar su uso en el art. 173 del Código Procesal Penal, que admite "cualquier otro medio de prueba no prohibido por ley, que pueda utilizarse aplicando analógicamente las normas que disciplinan a los expresamente previstos".

Se debe agregar que Uruguay ratificó y aprobó por ley de la Nación, diversas normas supranacionales que prevén la utilización de la videoconferencia, así por Ej.: las leyes 17.861, (Convención de la ONU de Nueva York, contra la Delincuencia Organizada Transnacional) y la ley 18.056 (Convención de la ONU de Mérida, contra la Corrupción), y asimismo se puede tener como base el Protocolo de San Luis, ley 17.145, arts. 1 literal K), 2, 6, 13, 17 y 18, además del espíritu que posee toda solicitud de cooperación jurídica internacional, que no es otro que el de facilitar y no poner obstáculos a la cooperación para así combatir más eficazmente a la delincuencia transnacional, respetando por supuesto, el orden público de nuestro país. Por otra parte pueden invocarse como normas análogas, los arts. 222 y 224 del Código del Proceso Penal referidos a la recepción de testimonio fuera del lugar del Juzgado que tramita la causa o investigación penal, y sin embargo, no se han recibido solicitudes internacionales.

7. Venezuela.[59]

El Ministerio Público de Venezuela cuenta con las herramientas para realizar

sistema ISDN, utilizándola de manera interna una o dos veces por mes, y habiéndola utilizado en materia de Cooperación Internacional con Holanda, Italia y Guyana.

No cuenta con un cuerpo que se refiera expresamente al tema, pero se puede levantar una argumentación coherente con los principios del proceso penal, en virtud del Principio de Libertad de Prueba (198 CPP) regente en Venezuela, como del artículo 340 del CPP, y a su vez con la Ley de Protección de Víctimas y Testigos. Asimismo Venezuela es parte de la Convención de las Naciones unidas contra la Delincuencia Organizada Transnacional, la que, como se mencionare con anterioridad en la presente investigación, dispone la utilización de ésta herramienta como medio de Cooperación Internacional.

Finalmente, en el ámbito de la Jurisprudencia, "es pertinente citar el criterio de la Sala Constitucional del Tribunal Supremo de Justicia, respecto a dicho principio, expresado en la decisión Nº 1571, de fecha 22 de agosto de 2001, con ocasión a la acción de amparo interpuesta por la Asociación Civil Deudores Hipotecarios de Vivienda Principal –ASODEVIPRILARA- contra la Superintendencia de Bancos y Otros Institutos de Crédito y el Consejo Directivo del Instituto para la Defensa y Educación del Consumidor y el Usuario –INDECU- (caso 'Créditos Mexicanos')", que en sus considerandos 1º y 2º señala:

"Considera la Sala, que el principio de inmediación en su fase clásica: presencia del sentenciador en la incorporación (evacuación) de las pruebas, puede tener dos manifestaciones o grados:

a. Que, el juez presencie personalmente los actos de recepción de la prueba, en los cuales -de acuerdo a lo que se disponga en la ley- puede intervenir, no sólo dirigiéndolos, sino realizando actividades probatorias atinentes al medio (interrogatorios, etc.)…

b. *Que, el juez no presencie personalmente in situ la evacuación de la prueba, pero sí la dirige de una manera mediata, utilizando técnicas y aparatos de control remoto, que le permiten aprehender personalmente los hechos mediante pantallas, censores, monitores o aparatos semejantes (video-conferencias, por ejemplo), coetáneamente a su ocurrencia*"

C. Breve Referencia al Caso Chileno:[60]

El Ministerio Público de Chile tiene las herramientas técnicas para realizar videoconferencias a cualquier parte del país y del mundo, con conexiones de tecnología IP como ISDN aunque suele trabajarse más con ISDN por la nitidez de la información. Aún así, cuando en el país desde el cual se desea realizar una Videoconferencia no existe una contraparte institucional que tenga equipos, o habiéndola, ésta no es la encargada según su legislación interna de participar de la VC, en esos casos se recurre al arriendo del servicio procurando la utilización de Consorcios que tengan sucursales y/o redes de apoyo mundial en muchos países.

Respecto de la frecuencia a nivel nacional, esto es videoconferencias en las que tanto el origen como el destino de la señal se encuentran en Chile, se realizan un promedio de 2 diarias, esto es un promedio de 40 mensuales, dando un aproximado total de 480 VC anuales, mientras que por su parte, a nivel internacional, esto es videoconferencias en las que el origen o destino de la señal se encuentran fuera de Chile, se realizan un promedio de 7 VC anuales.

Por otra parte, en Chile no existe legislación que trate la Videoconferencia como medio de Cooperación Internacional de manera expresa. Sin embargo, su factibilidad puede extraerse del análisis de preceptos legales nacionales e internacionales vinculantes.

"Los testigos y peritos que, por algún motivo grave y difícil de superar no pudieren comparecer a declarar a la audiencia del juicio, podrán hacerlo a través de videoconferencia o a través de cualquier otro medio tecnológico apto para su interrogatorio y contrainterrogatorio. La parte que los presente justificará su petición en una audiencia previa que será especialmente citada al efecto, debiendo aquéllos comparecer ante el tribunal con competencia en materia penal más cercano al lugar donde se encuentren".

Cuando ésta norma exige la comparecencia ante el tribunal más cercano al lugar donde se encuentren los declarantes se refiere a la declaración por videoconferencia "nacional". La intervención del Tribunal tiene razón de ser por cuanto éste actúa como Ministro de Fe, velando no sólo por la identidad del declarante y por la participación libre y voluntaria del mismo, sino que también como garante de que el testigo que aun no ha declarado no presencie la declaración del que lo antecedió.

Desde luego que respecto de las Videoconferencias "internacionales" no es dable exigir la intervención del juez extranjero, pues muchas veces estos no participan en su realización, como en México, por ejemplo. Ocurrirá otras veces que algunos jueces sean de países que no hablen español por lo que no siempre su calidad de Ministro de Fe pueda ser bien cumplida. Si bien no se trata de descartar la participación de jueces, debe considerarse como una alternativa, mas no la única forma mediante la cual se presta declaración.

Es por eso que en todas las VC "internacionales" se ha solicitado a los cónsules chilenos como Ministros de Fe para los efectos ya descritos, incorporando a los jueces extranjeros sólo cuando la legislación del país requerido así lo ha exigido como condición de realizarse la VC, lo cual ha ocurrido en aquellos casos en los que los declarantes han sido funcionarios públicos extranjeros.

Por su parte, el artículo 192 del Código Procesal Penal, referente a la declaración anticipada, señala que:

"Si el testigo se encontrare en el extranjero y no pudiere aplicarse lo previsto en el inciso final del artículo 190 [traslado]*, el fiscal podrá solicitar al juez de garantía que también se reciba su declaración anticipadamente. Para ese efecto, se recibirá la declaración del testigo, según resultare más conveniente y expedito, ante un cónsul chileno o ante el tribunal del lugar en que se hallare."*

No ha habido inconveniente para aplicar éste artículo en declaraciones prestadas durante la misma audiencia de juicio oral, toda vez que ello iría en directo beneficio del respeto a las normas y garantías del debido proceso. Es decir, si se permite la intervención de un cónsul para asegurar la declaración de un testigo que está en el extranjero antes de la realización de juicio, en las fases tempranas de la investigación, cuando probablemente las partes tengas menos medios para contrainterrogar al testigo, y si se permite que luego esa declaración sea grabada e introducida de esa manera en el juicio oral mediante exhibición de video, entonces parece altamente deseable que el testigo pueda declarar ante el Cónsul durante la misma audiencia de enjuiciamiento, con la posibilidad de ser interrogado y contrainterrogado "en vivo y directo" sin necesidad de estar viendo video.

Toda vez que un Cónsul no puede tomar declaración en el extranjero tanto porque podría no tener la preparación jurídica como porque su accionar afectaría la soberanía del otro Estado vulnerando las Convenciones de Viena sobre Relaciones Diplomáticas y Consulares, la única forma de entender este artículo -y así lo han hecho varios fallos - es que la declaración se preste por VC y se reciba ante el Cónsul (no la toma el cónsul, la recibe), para que produzca efectos en tiempo real ante el Tribunal, en Chile.

Sería imposible pensar que el Cónsul chileno o un Tribunal extranjero tomen declaración

Por tanto, la fundamentación jurídica para viabilizar una declaración mediante videoconferencia en Chile, estaría constituida tanto por los artículos 329 u 192 del Código Procesal Penal relacionados con los artículos 297 y 323 del mismo cuerpo legal que consagran la libertad probatoria, admitiendo todo medio apto para producir fe.

Por otra parte, la jurisprudencia que existe en Chile al respecto, se debe a que cada vez que se realiza una VC durante un juicio oral, es porque ésta ha sido previamente autorizada por el Tribunal de manera que en el fallo, sea absolutorio o condenatorio, desde el momento en que pondera la declaración del testigo, víctima, perito o imputado, valida automáticamente la VC como medio de declaración.

Es importante destacar, un fallo de la Sala Penal de la Exma. Corte Suprema de Justicia de Chile, hace un análisis detallado acerca de la admisibilidad de la VC, señalando principalmente, que la comparecencia mediante Videoconferencia, es análoga a la comparecencia personal, y produce prácticamente los mismos efectos jurídicos.

Finalmente, cabe señalar que el MP de Chile ha solicitado la toma de declaraciones por Videoconferencia, en el marco de la Cooperación Internacional, a países como Australia, Nueva Zelanda, Panamá, Reino Unido, España, Holanda, Filipinas, Italia y Rumania entre otros, mientras que ha recibido solicitudes de países como España y Costa Rica.

Conclusiones y estado de la cuestión

Luego de los antecedentes expuestos, parece factible concluir que la Videoconferencia es una herramienta cuya utilización se encuentra permitida por algunos de los más importantes Tratados Internacionales de Derechos Humanos aplicables al proceso penal, los que como sabemos, nos entregan el marco dentro del cual debe desenvolverse toda la normativa y actividad jurídica nacional. En ese sentido, en el derecho comparado se reconocen las virtudes de la utilización de la videoconferencia, que puede significar grandes avances en materia de persecución y proceso penal.

En ese sentido, del estudio de la legislación, doctrina y jurisprudencia existentes en distintos países del cono sur, como Argentina, Bolivia, Brasil, Colombia, Paraguay, Uruguay y Venezuela, además, por supuesto, de la necesaria referencia al derecho nacional, podemos concluir que la Videoconferencia como herramienta de Cooperación Internacional, es un mecanismo generalmente aceptado de manera expresa dentro de los sistemas procesales penales de la región, y aun en aquellos en que no existe referencia legislativa expresa, ésta se puede realizar de todas formas, sea mediante la interpretación de los principios fundantes del debido proceso, sea en un análisis sistemático que haga referencia a las normas supranacionales.

Por su parte, en Chile, si bien la ley no ha reconocido la utilización de la Videoconferencia como instrumento de Cooperación Internacional de manera expresa, esta se puede utilizar en virtud de la interpretación de principios básicos del proceso penal, que apuntan a la mayor y mejor protección del derecho al debido proceso.

En el mismo contexto, parece pertinente advertir que si la VC puede servir de utilidad en el marco del proceso penal, el cual por sus características propias exige el más elevado *standard* de respeto y protección a principios como el de inmediación y contradicción, perfectamente podría utilizarse en otras ramas del derecho, cuyos procedimientos son similares.

Finalmente, uno de los objetivos del presente trabajo es precisamente ese, en virtud del viejo aforismo que afirma que "quien puede lo más puede lo menos", y aún cuando la idea se plantea de manera exigua y tangencial, imaginemos como la VC podría ser un adelanto que teniendo como base la discusión y aceptación que ha tenido en el ámbito del proceso penal, pudiese "exportarse" a áreas como el derecho de familias, y el derecho Internacional en General.

- CHAHUAN SARRÁS, Sabas, *Manual del Nuevo Procedimiento Penal, Tercera edición actualizada y aumentada*, Edit. LexisNexis, Santiago de Chile, año 2007.
- MINISTERIO PÚBLICO DE CHILE, DIVISIÓN DE ATENCIÓN A VÍCTIMAS Y TESTIGOS, *La Víctima y el Testigo en la Reforma Procesal Penal*, prólogo del Fiscal nacional Guillermo Piedrabuena Richard, editorial Fallos del Mes, Santiago de Chile, año 2003.
- MEHRABIAN, ALBERT, *Silent Messages: Implicit communication of emotions and attitudes*, 2ª edition, Wadsworth, Belmont, California.
- MONTERDE FERRER, FRANCISCO, *El proceso de introducción de las nuevas tecnologías en el ejercicio de la función jurisdiccional*, en *Cuadernos Constitucionales de la Cátedra Fadrique Furió Ceriol*, Revista Jurídica del Departamento de Derecho Constitucional y Ciencia Política y de la Administración de la Universitat de Valencia, ISSN 1135-0679, Nº 56, 2006, págs. 25-59.
- NEVADO, MARÍA TERESA, *Reflexión sobre la actualidad de la declaración electrónica en el proceso penal español. Especial consideración del proceso con menores*, en *Revista de Derecho Internacional, Comercio, Innovación y Desarrollo, DICID*, de la Universite Bourgogne, N° 1, Avril 2012, Francia. Disponible en http://es.scribd.com/doc/88033674/01-DICID

Informes en Derecho y Documentos de Trabajo:

- CANDIA AMARILLA, Rubén, *Palabras de bienvenida al I Taller sobre uso de la videoconferencia en la Cooperación Jurídica internacional, en su calidad de Fiscal General del Estado de Paraguay*, el día 28 de Abril de 2009, en la ciudad de Asunción.
- Cuestionario de Salvador de Bahía de la Reunión Especializada de Ministerios Públicos del Mercosur sobre Videoconferencia. Respondido por el Dr. Adrián O. Marchisio, Secretario de la Procuración general de la Nación Argentina.
- Cuestionario de Salvador de Bahía de la Reunión Especializada de Ministerios Públicos del Mercosur sobre Videoconferencia. Respondido por Abdiel Adin Andadre Urdinica, Fiscal de Materia, Coordinador en Cooperación Internacional y Extradiciones del Ministerio Público de Bolivia.
- Cuestionario de Salvador de Bahía de la Reunión Especializada de Ministerios Públicos del Mercosur sobre Videoconferencia. Respondido por Vladimir Aras, Procurador de la República de Brasil (Fiscal Federal).
- Cuestionario de Salvador de Bahía de la Reunión Especializada de Ministerios Públicos del Mercosur sobre Videoconferencia. Respondido Laura Benedetti Roncallo y Aydaluz Segrera Alarcón, Asesoras de la Dirección de Asuntos Internacionales, y revisado por el Dr. Luís González León, Fiscal Jefe de la Unidad de Justicia y Paz. Todos de la Fiscalía General de la Nación de Colombia.
- Cuestionario de Salvador de Bahía de la Reunión Especializada de Ministerios Públicos del Mercosur sobre Videoconferencia. Respondido por María Magdalena Quiñónez, Asistente Fiscal del Ministerio Público de Paraguay.
- Cuestionario de Salvador de Bahía de la Reunión Especializada de Ministerios Públicos del Mercosur sobre Videoconferencia. Respondido por Enrique Rodríguez Martínez, Fiscal Letrado Nacional, con la supervisión de la Fiscalía de Corte y Procuraduría General de la nación de Uruguay.
- Cuestionario de Salvador de Bahía de la Reunión Especializada de Ministerios Públicos del Mercosur sobre Videoconferencia. Respondido Juan Carlos Cabello Mata, Coordinador

- DE LA MATA AMAYA, JOSÉ, *La Utilización de la Videoconferencia en las actuaciones judiciales*, ponencia presentada en el seminario de formación continuada del CGPJ, realizado en Madrid, del 17 al 19 de septiembre del 2003.
- Documento de trabajo para el "I Taller sobre uso de la videoconferencia en la Cooperación Jurídica internacional", celebrado en la Fiscalía General del Estado de Paraguay, el día 28 de Abril de 2009, en la ciudad de Asunción.
- GODOY BERROCAL, María Elena, "Breves notas sobre Videoconferencia", documento de Trabajo para la Reunión Especializada de Ministerios Públicos del Mercosur.
- GRANADILLO, Nancy, *Marco Legal Internacional contra la delincuencia Organizada*, Ponencia expuesta por la autora durante el Tercer Encuentro Anual de Criminología (2006), efectuado en la Universidad Católica Andrés Bello – Caracas, Venezuela.
- PIEDRABUENA RICHARD, Guillermo, en su calidad de Fiscal nacional de la República de Chile, Oficio F.N. Nº 104, que informa sobre la ratificación y promulgación de la Convención de Palermo, Santiago de Chile, 1º de Marzo de 2005.
- TAVOLARI OLIVEROS, Raúl, *Informe en Derecho, solicitado por el Fiscal Nacional de Chile, Guillermo Piedrabuena Richard, sobre Videoconferencia*, Viña del Mar, Julio 2003.
- TIRADO ESTRADA, Jesús J., *Videoconferencia y Equipos Conjuntos de Investigación*, Material elaborado por el autor en su calidad de Fiscal en la Unidad de Apoyo al Fiscal General de España.
- VÁSQUEZ GONZÁLEZ, SANTIAGO RAÚL, *Fundamentos de la Videoconferencia, y su implementación en el Ministerio Público del Paraguay*, Fiscalía General del Estado, Dirección de Informática, Administración de Redes y Sistemas. Documento de trabajo presentado en el primer taller sobre uso de la Videoconferencia en la Cooperación Jurídica Internacional, en el marco de la Reunión Preparatoria de la VII Reunión de Ministerios Públicos del MERCOSUR, celebrada el 28 de abril de 2009, en la sede del Ministerio Público del Paraguay.

Páginas Web:

- Noticiasjurídicas.com
- Ministerio Público de Paraguay. Web Site Oficial. http://www.ministeriopublico.gov.py/reunion/pdf/rempm.pdf.

Clarín.com.

Heurs et malheurs de *Google Street View* devant les tribunaux suisses

Bertil Cottier professeur de droit de la communication, Université de la Suisse italienne, Lugano

Sébastien Fanti, avocat spécialisé en nouvelles technologies, Sion

I. Introduction

Comme dans de nombreux autres pays, *Google Street View* (ci-après GSW), le service de navigation virtuelle dans les espaces publics (rues, places, etc.) des localités, a suscité polémiques et controverses en Suisse : de nombreux citoyens se sont plaints non seulement de la mise en ligne, sans leur consentement, de photographies les représentant mais aussi de la manière tout sauf transparente dont les prises de vue étaient effectuées. Ces récriminations ont conduit le Préposé fédéral à la protection des données – notre autorité de surveillance en la matière, ci-après le Préposé - à intervenir pour ramener l'opérateur Google à plus de respect de la vie privée.

A ce stade rien de bien nouveau; à l'étranger aussi GSW s'est retrouvé dans le collimateur de plusieurs autorités nationales de protection des données. Ainsi, en 2011, la Commission française de l'informatique et des libertés a condamné Google à une amende de 100 000 Euros pour avoir tiré parti du passage des véhicules destinés aux prises de vues pour enregistrer des données privées (sites web visités, mots de passe des messageries électroniques ainsi que contenu des mails échangés) transitant par les réseaux Wi-Fi non sécurisés[61]. Dans d'autres pays (notamment en Autriche, en Grèce, au Japon, aux Pays-Bas et en République Tchèque), Google s'est vu imposer un code de conduite; ont été ainsi réglementés l'information des habitants sur la date et le périmètre des prises de vue, la hauteur maximale des caméras et le floutage des visages des personnes photographiées[62].

Cela dit, ce qui est particulier à la Suisse, c'est que la plus haute instance judiciaire du pays, le Tribunal fédéral, a été saisie de la controverse. Une première mondiale, car jusque-là aucune cour suprême n'avait eu l'occasion de se prononcer sur GSW ! Autant dire que la décision des juges fédéraux était très attendue en Suisse comme à l'étranger. Elle est tombée le 31 mai 2012[63]. Chose surprenante : les deux parties ont aussitôt crié victoire. Google, car son service de navigation n'a pas été interdit, ni même contraint de flouter à 100 % les images publiées[64]. Le Préposé, car la collecte et la mise en ligne des données personnelles ont été soumises à un catalogue de conditions très strictes[65].

Le Tribunal fédéral ayant procédé à une analyse approfondie des tenants et aboutissants de GSW, le présent jugement mérite d'être reporté et commenté en long et en large. Tel sera l'objectif de la présente contribution. Notre législation pertinente – d'une part la loi fédérale sur la protection des données (ci-après LPD[66]), d'autre part le droit à l'image tel que la jurisprudence l'a développé sur la base des standards, très vagues, de la protection de la personnalité posés par l'article 28 du

[61] Délibération 2011-035 du 17 mars 2011, accessible sur le site de la CNIL : http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/D2011-035.pdf.
[62] Pour un aperçu de la situation dans le monde, voir

Code civil suisse[67] - étant très semblable à celle des principaux pays européens, les enseignements que l'on peut tirer du jugement du Tribunal fédéral ont une valeur qui dépasse incontestablement les frontières de notre pays[68].

Mais avant de présenter dans le détail le raisonnement des juges fédéraux et leurs conclusions, il importe d'abord de rappeler les fonctionnalités de GSW et ensuite de passer en revue les diverses étapes (recommandation du Préposé, puis jugement de première instance du Tribunal administratif fédéral) qui ont conduit à la saisine de notre cour suprême.

II. Caractéristiques techniques et fonctionnalités de Google Street View

La société Google Inc. a développé différents outils de recherche géographique reposant sur des photographies satellites ou aériennes, ainsi que sur des prises de vue dans les voies et lieux publics. Elle a ajouté à ces outils cartographiques des fonctionnalités supplémentaires, telles que la géolocalisation, qui permet de déterminer la position de l'utilisateur du service. Durant l'année 2004, Google Inc. a lancé le service en ligne *Google Maps* qui permet de visualiser une zone géographique, aussi bien à l'échelle d'un pays qu'à l'échelle d'une rue. Les cartes proposées sont issues de données géographiques classiques (frontière, rue, autoroute, etc.) et d'images satellites ou aériennes très précises[69]. Durant l'année 2007, GSW a été intégré au service *Google Maps*.

GSW est un service qui permet de naviguer virtuellement dans les rues des grandes villes et d'explorer des sites touristiques. Il utilise une technologie qui fournit une vue de la rue à 360 degrés horizontalement (et 290 degrés verticalement) en n'importe quel point de cette rue.[70] Une voiture, usuellement baptisée *Google Car*, équipée de caméras (d'une hauteur de 2.75 m), circule dans les rues en prenant des images qu'un logiciel assemble ensuite pour donner l'impression de continuité. Google Inc. utilise désormais d'autres outils (un avion cartographe dénommé *Google Plane*[71], un vélo dénommé *Tricycle Street View*[72], le *Motoneige Street View* ou encore le *Chariot Street View*[73]) pour permettre la collecte d'images de lignes ferroviaires (Chemin de fer rhétiques[74]), de fleuves (l'Amazone[75]), de sentiers pédestres[76] ou encore de musées (*Google Art Project*[77]).

Concrètement, cela signifie que le développement de ce service, en tant qu'il ne connaît manifestement plus aucune limite technique, sera exponentiel et qu'il concernera prochainement tous les lieux sis sur notre planète (lacs, fonds marins, forêts, grottes, parcs naturels, etc.).

En Suisse, GGS a été mis en ligne à la mi-août 2009; il comportait plus de 20 millions d'images au prélude du litige[78].

Il convient à ce stade de relever que la description du service par le Tribunal fédéral est singulièrement brève (en tout et pour tout, sept lignes) et peu précise[79], à l'aune des décisions rendues par les autres instances judiciaires ou administratives saisies de cette problématique. L'impression qui s'en dégage est celle d'un arrêt qui n'envisage que les conséquences actuelles de ce service, pourtant tangiblement destiné à connaître un développement rapide. Au terme de notre

---

[67] Art. 28 CCS: « [1]Celui qui subit une atteinte illicite à sa personnalité peut agir en justice pour sa protection contre toute personne qui y participe. [2]Une atteinte est illicite, à moins qu'elle ne soit justifiée par le consentement de la victime, par un intérêt prépondérant privé ou public, ou par la loi. ».

[68] Ainsi la LPD se fonde sur la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

[69] Ce descriptif est celui retenu par la CNIL dans sa délibération n° 2011-035 (note 1).

[70] Cette technologie est intitulée *Mobile Mapping*.

[71] http://auto-net.fr/google-plane-les-avions-cartographes/

analyse du jugement du Tribunal fédéral, nous verrons que, heureusement, cette impression ne se confirmera pas ; bien au contraire, la décision a un caractère évolutif certain.

III. Le conflit se noue : plaintes de citoyens, puis recommandation du Préposé fédéral à la protection des données

A. Les pouvoirs limités du Préposé

Le Préposé à la protection des données helvétique ne dispose de prérogatives étendues que pour le secteur public. Ses compétences en matière privée ont certes été accrues en 2006, mais elles ne sont pas comparables à celles des autorités nationales de protection des données étrangères[80]. Ainsi, le Préposé ne peut pas infliger d'amendes administratives[81], ni sanctionner lui-même pénalement les contrevenants[82], ce qui par conséquent limite son champ d'action[83]. De même, il ne possède pas, pour l'heure, de pouvoir d'approbation préalable de certains traitements de données. Sa carte maîtresse consiste donc à émettre des recommandations, qui ont un effet préventif individuel et collectif indéniable. Si la recommandation n'est pas suivie, il lui est loisible de saisir le Tribunal administratif fédéral, selon une procédure qui sera exposée ci-après, ce qui générera une décision judiciaire en bonne et due forme à l'issue d'un procès classique respectueux des standards internationaux (en particulier les garanties posées par l'art. 6 CEDH).

De longue date, les destinataires des recommandations du Préposé qui s'y opposaient devant les tribunaux ont développé une stratégie tendant à dénier à l'autorité de contrôle toute compétence d'intervention au motif soit que le droit suisse ne s'appliquait pas, soit que le Préposé avait excédé son pouvoir d'intervention, voire appliqué arbitrairement la loi. Le but est clairement de restreindre le champ d'action du gardien du temple des données que la législation helvétique avait pourtant déjà confiné à l'intérieur de limites légales très strictes. Google n'a pas manqué de s'engager lui aussi dans cette ligne de défense, soumettant le rôle du Préposé à un examen minutieux : chacune des mesures qu'il a recommandées a été auscultée, disséquée et contestée dans des proportions jamais égalées. L'issue du litige présente ainsi un intérêt considérable non seulement pour la question topique (la légitimité de GSW), mais également pour la délimitation des pouvoirs du Préposé. Nous évoquerons quelques guerres procédurales picrocholines ci-après (cf. infra 6.1 et 6.2) ; elles sont emblématiques de ce contexte de remise en question tous azimuts des pouvoirs du Préposé.

B. Les premières plaintes

Dès l'activation de GSW en Suisse, tant le Préposé que Google Suisse[84] ont reçu moult annonces concernant l'insuffisance ou l'absence de floutage des visages et des plaques d'immatriculation.[85] Et ce, bien que le Préposé avait posé un certain nombre de conditions préalables à la mise en service de GSW, telle la possibilité d'annoncer online les insuffisances de floutage ou de demander l'effacement des images dans un délai bref (entre 24 et 48 heures). De surcroît, Google avait accepté de communiquer à l'avance les lieux des prises de vue.

Après différentes vérifications, le Préposé devait constater la présence d'images problématiques et insuffisamment anonymisées ; il en a fait état publiquement le 21 août 2009

[80] Cf. à cet égard, Bertil Cottier, Les divers modèles d'indépendance des autorités nationales de protection des données, in

déjà.[86] Il s'agissait notamment de photographies prises dans des rues privées et d'images de jardins. Les informations sur les prises de vue données par Google étaient également lacunaires et imprécises. Le Préposé a alors alerté Google qui a proposé différentes mesures d'amélioration, dont l'implémentation d'une nouvelle version du logiciel destinée à améliorer le floutage. Google a par contre refusé d'anonymiser manuellement des données.

Ces améliorations sont apparues insuffisantes au Préposé, raison pour laquelle il a émis une recommandation le 11 septembre 2009 (art. 29 al. 3 LPD)[87].

La société Google n'ayant pas obtempéré, le Tribunal administratif fédéral a été saisi par requête du 11 novembre 2009 du Préposé fédéral à la protection des données[88]. Ce dernier exigeait, en substance, que les visages et les plaques d'immatriculation soient rendus méconnaissables, que l'anonymat des personnes photographiées à proximité d'installations sensibles soit garanti, que les photographies d'espaces privés ou prises à partir de rues privées soient retirées de GSW et que les villes et villages soient informés préalablement de l'intention de les photographier et de la mise en ligne[89].

C. Un accord sur des mesures provisionnelles

Le Préposé a requis du président de la cour du Tribunal administratif fédéral des mesures provisionnelles, ainsi que le lui permet l'article 33 al. 2 LPD[90]. Cette question a été débattue entre les parties qui sont, finalement, parvenues à un accord au terme duquel le régime temporaire suivant a été institué :

1. Google s'engage à ne publier sur Internet aucune nouvelle image prise en Suisse pour Street View, ni dans le cadre de son service en ligne Street View, ni dans le cadre d'aucun autre de ses produits, et ce jusqu'à ce que le Tribunal administratif fédéral ait statué et que l'arrêt soit entré en force.

2. Google s'engage à se soumettre à l'arrêt que le Tribunal administratif fédéral rendra dans cette affaire et à l'appliquer pour toutes les photographies prises en Suisse pour Street View, si et dans la mesure où le jugement devait l'exiger[91].

3. Google reste autorisé à poursuivre ses prises de vues en Suisse, à ses risques toutefois, eu égard à l'issue à venir de la procédure judiciaire en cours. Conformément au ch. 1 ci-dessus, les images concernées ne seront pas mises en ligne et, jusqu'à ce que le Tribunal administratif fédéral ait statué, resteront au sein du groupe Google et pourront être utilisées uniquement à des fins ou dans le cadre de produits ne se rapportant pas à des personnes.

4. Google annoncera en ligne et au plus tard une semaine à l'avance (au lieu d'un mois précédemment) les districts ou environs de villes où elle envisage de procéder à des prises de vues sur le domaine public.

5. Le PFPDT considère que les objectifs visés par les mesures provisionnelles qu'il avait demandé au Tribunal administratif fédéral de prendre sont atteints, ce qui l'amène à retirer la demande en question.

---

[86] Par le biais d'une information aux médias intitulée „Google Street View doit être retiré d'internet", cf.: http://www.edoeb.admin.ch/dokumentation/00438/00465/01676/01678/index.html?lang=fr.

[87] Cf. l'annonce de la recommandation: http://www.edoeb.admin.ch/dokumentation/00438/00465/01676/01681/index.html?lang=fr; la recommandation est disponible à l'adresse: http://www.edoeb.admin.ch/

6. L'accord conclu ne préjuge en rien les positions défendues par les parties dans le cadre de la procédure en cours.

Nous reviendrons ultérieurement sur le sort des images collectées par Google durant ce régime temporaire (cf. 5.8).

IV. Le jugement du Tribunal administratif fédéral (mars 2011)

On ne relatera pas dans le détail la longue (plus de cinquante pages !) décision du Tribunal administratif fédéral (ci-après TAF)[92]. En effet, la plupart de ses conclusions seront présentées dans la section consacrée au jugement final du Tribunal fédéral, vu qu'elles ont été purement et simplement confirmées par cette dernière instance[93]. On se contentera d'évoquer ici la seule divergence majeure entre les deux cours : l'étendue de l'obligation de flouter. Un point sur lequel le TAF s'est montré intransigeant. Les juges de première instance ont en effet imposé à Google une obligation *absolue* de flouter préalablement à la mise en ligne : aucun visage ni aucune plaque d'immatriculation de véhicules ne doivent pouvoir être identifiés par les utilisateurs de GSW.

Google pour sa part soutenait qu'il n'était pas en mesure de flouter automatiquement l'ensemble des données personnelles mises en ligne. Bien qu'il ait recours à un logiciel des plus performants, il concédait un taux d'erreur de 2 % des images (ce qui représente un taux d'anonymisation de 98 %). Partant, une certaine tolérance devait être de mise ; ce d'autant que le géant américain se déclarait disposé à flouter manuellement les données encore identifiables, sur demande individuelle des personnes concernées.

Le TAF est resté sourd à cette proposition de compromis; au motif que le floutage manuel n'intervenait qu'a posteriori. Entretemps le mal était fait : près de 400'000 images non floutées devenaient accessibles en ligne; partant une atteinte illicite à la personnalité de plusieurs milliers de personnes était commise par Google, atteinte qu'aucun intérêt public ou privé prépondérant n'excusait. Que GSW fasse le bonheur de nombreux utilisateurs en Suisse n'a notamment pesé d'aucun poids dans la balance. Au demeurant le TAF convient qu'un floutage manuel de tous les visages et de toutes les plaques d'immatriculation qui échappent au floutage automatique est une opération qui ne va pas sans de sérieux coûts supplémentaires[94]. Ces surcoûts, Google, qui n'est autre qu'une entreprise commerciale poursuivant un but lucratif, peut cependant pleinement les assumer; à défaut il lui est loisible de les répercuter sur ses utilisateurs, lesquels n'ont pas un droit à un service gratuit.

Pareille obligation de floutage absolu a été jugée disproportionnée par plus d'un. À témoin ce titre on ne peut plus éloquent d'un commentaire critique du professeur Meier de l'Université de Lausanne : *À l'impossible nul n'est tenu…sauf Google?* [95].

V. L'arrêt du Tribunal fédéral (mai 2012)

A. Remarques préliminaires

Contrairement à d'autres décisions importantes en matière de droit de la communication et de protection des données – à commencer par l'arrêt dit *Logistep* qui a banni la traque privée du téléchargement illégal sur les réseaux –, le jugement qui nous intéresse n'a pas été rendu en audience publique, mais par voie de circulation.

On regrettera donc de n'avoir pas pu entendre chaque juge s'exprimer individuellement sur la cause ; cela dit, on peut inférer de l'absence de débats que les propositions du juge rapporteur ont été acceptées à l'unanimité par les quatre autres membres de la première chambre de droit public[96].

On notera de surcroît que notre instance suprême a une haute estime de la décision qu'elle a rendue. Les juges ont en effet décidé de la publier dans le recueil officiel des arrêts du Tribunal fédéral (ATF) ; une collection à l'ancienne – i. e. sur papier - qui rassemble les seuls jugements susceptibles de faire date (moins de 10 % de l'ensemble des arrêts).

Par ailleurs, il y a lieu de relever que notre présentation critique de l'arrêt du Tribunal fédéral commencera par traiter de la question du floutage, pour passer ensuite à l'examen des considérants relatifs à la portée du droit à l'image et enfin aux restrictions des modalités de prises de vue décrétées par cette instance. Ce parcours n'est pas celui adopté par les juges dans leur décision ; il s'impose toutefois pour des raisons de clarté de l'exposé.

B. Floutage absolu ? non, mais…

On se souvient (cf. supra 4) que Le Tribunal administratif fédéral avait conditionné l'exploitation du service GSW à un floutage préalable de l'ensemble des visages des personnes représentées et des plaques d'immatriculation des véhicules. Le Tribunal fédéral a clairement désavoué les juges de première instance sur ce point, jugeant la mesure ordonnée excessive.

Or GSW est utile, reconnaît d'emblée note cour suprême. Même si ce service permet à quelques personnes de satisfaire une curiosité pas toujours de bon aloi, on doit convenir que de très nombreuses autres peuvent grâce à lui organiser leurs déplacements[97], se familiariser avec des lieux inconnus ou encore rechercher un bien immobilier. Partant, il faut impérativement, dans la pesée des intérêts en présence, prendre en compte l'intérêt public des utilisateurs à bénéficier d'un service de navigation « légitime et bienvenu »[98] et non, comme l'a fait à tort le TAF, réduire cet intérêt public à néant en le confondant avec l'intérêt privé de Google de commercialiser un service lucratif. De surcroît, les juges fédéraux ont tenu à minimiser la gravité des atteintes à la personnalité subies par les personnes représentées en soulignant que finalement la société moderne s'accommode dans une certaine mesure de la circulation d'un grand nombre de photographies personnelles (notamment sur les réseaux sociaux), un nombre si considérable qu'il n'est aujourd'hui plus possible de garantir à tout un chacun une pleine de protection de sa vie privée.

Il importe dès lors de trouver une solution réaliste qui ne conduise pas à une interdiction indirecte de GSW. Cette solution consiste à tolérer un taux d'erreur maximal du logiciel de floutage automatique de 1 % (considérant 10.7) ; ce seuil correspond au taux d'erreur du logiciel le plus performant à l'heure actuelle. Quant aux quelque 200'000 images qui échappent ainsi au floutage automatique, les personnes concernées doivent se voir offrir la possibilité de requérir, a posteriori, une anonymisation manuelle sur demande individuelle (sur les modalités, cf. infra 5.4).

On relèvera encore que ce seuil de tolérance de 1 % n'est pas coulé dans le bronze. De fait, il incombe à Google de veiller à régulièrement améliorer les performances de son logiciel et de tenir le Préposé au courant des progrès réalisés. Si l'obligation d'amélioration n'est pas respectée, le Préposé peut émettre une nouvelle recommandation tendant à réduire le taux d'erreur.

S'agissant des prises de vue à proximité des prisons, des hôpitaux, des écoles, des centres d'accueil de femmes battues, des maisons de retraites et des tribunaux, le Tribunal fédéral s'est

sensibles[99] doivent bénéficier d'une protection accrue de leur personnalité : Google ne peut dans ce cas mettre en ligne des images sans avoir procédé à une anonymisation totale des personnes représentées. Par anonymisation totale, on entend non seulement un floutage des visages et plaques d'immatriculation, mais aussi de tout trait caractéristique qui permettrait d'identifier indirectement une personne (handicap particulier, vêtement original, couleur de la peau, etc.). Si pareille anonymisation est difficile à réaliser, alors le caviardage de l'ensemble du périmètre sensible devra être effectué, quitte à créer des lacunes dans la représentation des localités (considérant 6.6).

C. Le droit à l'image et l'exception de statut accessoire

Suivant la conception traditionnelle du droit à l'image, la personnalité n'est pas protégée de façon absolue; ainsi, les personnes qui sont représentées sur une photographie d'une manière accessoire ou occasionnelle doivent tolérer une publication sans leur consentement[100]. Se fondant sur ce principe, Google soutenait que son service de navigation opérait en toute licéité: GSW a pour objectif premier de donner à l'utilisateur la possibilité de découvrir une localité comme le ferait un piéton ou le passager d'une automobile ; autrement dit l'intérêt de l'utilisateur se concentre sur les rues, les places et les édifices, et non sur les habitants ou les passants. En conséquence, les personnes représentées sur GSW se voyaient privées de la possibilité de s'opposer à la diffusion de leur image.

Le Tribunal fédéral (comme précédemment le TAF d'ailleurs) a rejeté cet argument. Il a en effet refusé de reléguer les personnes représentées sur les images publiées au rang de simples accessoires. Et ce, parce que la technologie de navigation mise à disposition par Google permet de se focaliser sur une personne: par le biais de la fonction « zoom », l'utilisateur peut agrandir une image et projeter la personne au premier plan. Avec, à la clef une atteinte illicite à sa personnalité en raison des possibilités d'observation précise qui en résulte (considérant 8.3).

Cela veut-il dire que le Tribunal jette désormais l'exception de représentation accessoire ou occasionnelle aux oubliettes ? nullement. Les juges ont simplement « recadré » sa portée : l'exception ne vaut pas pour des systèmes de publication générale à très grande échelle et à diffusion permanente, tel GSW, car leurs possibilités d'agrandissement et la haute résolution de leurs images favorisent la surveillance des personnes. Voilà qui rassurera les médias traditionnels (en particulier la presse et la télévision) qui craignaient, après la décision du TAF, de perdre notamment leur droit de diffuser des images de foule – on songe aux spectateurs d'une rencontre sportive ou aux touristes qui visitent un monument historique. Devoir flouter tous ces visages aurait fait perdre à ces représentations leur réalisme, et partant leur valeur informative ; valeur informative dont sont en revanche dénuées les personnes montrées par GSW.

D. Obligation de mettre sur pied un système de requête efficace d'anonymisation manuelle

L'un des griefs formulés relativement au service GSW avait trait à l'inefficacité du système de requête d'anonymisation. Le Tribunal fédéral exige désormais qu'un lien, avec la dénomination claire « requête d'anonymisation », soit mis en fonction (considérant 10.6.3) . À l'heure actuelle, il existe une fonctionnalité à peine visible intitulée « *signaler un problème* », sise en bas à gauche de la page de *Google Maps*. Force est toutefois de constater, ainsi que le relève opportunément le Tribunal fédéral, que : „ *Die zurzeit auf Street View bestehende kleine, kaum erkennbare Schaltfläche zur Meldung von Problemen genügt als Information über die Widerspruchsmöglichkeit nicht*".

requérant. Le Tribunal fédéral exige également que la possibilité d'émettre une requête d'anonymisation soit communiquée dans les médias « classiques » (comme la presse) à intervalles réguliers (au moins tous les trois ans).

Il incombe au Préposé de veiller au respect de ces exigences. Aux dires du Préposé suppléant à la protection des données[101], Google n'a pas encore concrétisé les nouvelles conditions d'exploitation du service GSW, bien que l'arrêt du Tribunal fédéral soit immédiatement applicable[102]. Le Préposé, conscient des difficultés techniques et des développements à entreprendre, a consenti à ce qu'un délai de grâce soit accordé à Google. Dans l'intervalle, la firme de Moutain View ne pourra pas publier de nouvelles images, ce qui devrait l'inciter à proposer rapidement au Préposé des solutions techniques innovantes (cf. infra 5.7).

E. Information sur l'horaire et le lieu des prises de vue

Le devoir d'information de Google dans le cadre de l'exploitation du service GSW a été considéré comme insuffisamment respecté (considérant 10.6.3.). Désormais, l'entreprise va devoir procéder à des améliorations significatives ; elles concerneront tant les droits des personnes intéressées que, préventivement, la collecte et de la diffusion des images.

S'agissant des droits des personnes concernées, le site suisse de GSW devra comporter des indications plus précises sur les modalités d'exercice du droit d'opposition; de plus Google devra également accepter les réclamations soumises par courrier postal, ce qui n'était pas le cas jusqu'à aujourd'hui. À cet effet, il devra indiquer une adresse postale en Suisse. Ces informations devront être actualisées de manière régulière. Au moment de la rédaction du présent article, soit durant la deuxième quinzaine de juillet 2012, le site ne comportait encore aucune des améliorations requises par le Tribunal fédéral[103]. Ainsi qu'il a été indiqué, le Préposé a consenti à attendre que les améliorations techniques soient développées, ce qui paraît légitime. Reste qu'en ce qui une démarche aussi simple que l'indication d'une adresse postale, on peut s'étonner de l'absence de réaction rapide de Google, qui, ce faisant, s'expose à l'action de tout citoyen n'étant pas au bénéfice d'une connexion internet.

Quant à la communication de la collecte des images, Google doit, une semaine à l'avance au minimum, indiquer quels sont les villages et les villes dans lesquels il envisage de prendre des photos et signaler, de surcroît, une semaine avant la mise en ligne quelles sont les localités concernées. Compte tenu du fait que certaines personnes ne disposent pas d'un accès à Internet, ces informations devront également faire l'objet d'une publication dans les médias locaux, soit dans la presse régionale et locale.

Le Tribunal fédéral a axé sa réflexion sur une vision géographique classique fondée sur les communes politiques, les cantons, voire les régions. Qu'adviendra-t-il lorsque la collecte d'image portera sur des cours d'eau ou des bisses chevauchant plusieurs communes, voire cantons ? Une diffusion dans un journal local sera insuffisante dès lors que celui-ci ne dispose que d'un lectorat restreint. Il serait alors judicieux de procéder à des publications dans les feuilles officielles publiées par les cantons, ce qui garantirait en sus une attention plus conséquente du lecteur. Les prochains mois seront à cet égard un révélateur efficace des intentions de Google, lequel pour éviter des contestations ultérieures serait bien inspiré de ne pas lésiner sur la communication.

F. Hauteur maximale des caméras

retient que les prises de vue d'espaces privés soustraits aux regards des passants ne peuvent pas être publiées sans le consentement des personnes concernées. Il limite expressément la hauteur des caméras à 2 mètres, ce qui correspond peu ou prou à la hauteur de l'œil d'un passant déambulant sur un trottoir. Cela permettra pour les nouvelles images réalisées d'assurer un niveau de protection similaire à celui représenté par une haie ou une clôture.

Si plusieurs autorités étrangères se sont prononcées fondamentalement sur la légalité GSW, rares sont celles qui ont actionné le couperet de la limitation de la hauteur de la caméra. Les autorités tchèques[104] ont requis que la hauteur de ces caméras soit revue à la baisse afin d'être à « *hauteur des yeux des piétons* ». A l'issue d'âpres négociations avec Google, la hauteur de la tour n'a été ramenée qu'à 2 mètres 30 – 40[105]. Autant dire que le Tribunal fédéral s'est montré très strict ; à notre connaissance, il est le seul à avoir imposé une hauteur de 2 mètres; hauteur limite déterminée par un calcul empirique, ce qui constitue souvent la meilleure solution à un problème de ce type.

Un bémol toutefois ! Le Tribunal administratif fédéral avait admis la possibilité pour les *Google Cars* d'emprunter des chemins privés pour la collecte d'images. Le Préposé n'ayant pas recouru à l'encontre de la décision du Tribunal administratif fédéral, l'arrêt est entré en force sur ce point, ce qui signifie que ces véhicules pourront effectuer des prises de vue dans des rues privées. À l'aune du développement relatif aux prises de vue d'espaces privés, on regrettera que le Tribunal fédéral n'ait pas pu se prononcer sur un problème dont l'acuité est évidente.

En toutes hypothèses, avec les *Google Planes*, la problématique de la hauteur des caméras sera reléguée au second plan; il conviendra alors de déterminer de nouvelles limites spatiales et juridiques.

G. Régime transitoire

Comme il a été exposé précédemment[106], durant la procédure les parties sont parvenues à un accord qui définit un régime d'exploitation provisoire. Il importait dès lors que le jugement final règle le sort des images réalisées dans l'intervalle, mais non publiées[107]. Parmi celles-ci figurent des images qui ne respectent pas les réquisits imposés par le Tribunal fédéral (en raison notamment de la hauteur de la caméra).

Pour les images déjà publiées, le Tribunal fédéral accorde un délai transitoire de trois ans afin de permettre la mise en conformité. Ce délai, s'il apparaît généreux, ne doit pas occulter le nombre considérable d'images concernées (la seule marge d'erreur de 1% génère 200'000 images à corriger). Quant aux images nouvellement publiées, respectivement à publier, elles doivent satisfaire immédiatement aux conditions fixées par le Tribunal fédéral. Reste à savoir si Google va axer ses efforts sur les images déjà en ligne ou préférera traiter prioritairement les images à publier.

VI. Remarques particulières

A. Droit applicable

Google a invoqué (parmi ses nombreux moyens) l'inapplicabilité du droit suisse et, *a fortiori*, l'incompétence du Préposé. Cette stratégie de défense, éculée devant de nombreuses juridictions étrangères,[108] était soumise pour la première fois en Suisse à l'examen méticuleux du Tribunal fédéral. L'argumentaire de la recourante était, de ce point de vue, intéressant. Dans la mesure où les images étaient assemblées en Belgique et publiées sur Internet depuis un serveur

images utilisées par GSW ont été réalisées en Suisse, relativement à des personnes, des routes et des places sises en Suisse et sont accessibles depuis la Suisse. Un lien prépondérant avec la Suisse doit donc être mis en exergue : la finalisation de la production des images hors de Suisse ainsi que leur publication depuis l'étranger ne jouent qu'un rôle accessoire qui ne saurait occulter ce rattachement décisif.

Le Préposé était donc fondé à émettre une recommandation (art. 29 LPD), en vertu du principe de territorialité. Cette décision aura des conséquences importantes. Dès lors qu'un lien suffisamment étroit avec la Suisse existe, il n'est plus possible d'exciper d'un traitement ou d'une publication à l'étranger pour tenter de se soustraire à un régime juridique moins favorable. Les *global companies* qui exercent régulièrement leurs activités dans plusieurs pays sont averties : elles ne pourront plus éluder les questions délicates du respect des normes en matière de protection des données en prétextant que le traitement est conforme au droit d'un pays tiers.

B. Qualité pour défendre de Google

L'un des éléments fondamentaux de la décision du Tribunal fédéral est la question de la qualité pour défendre de Google Switzerland Sàrl (légitimation passive). Cette ligne de défense désormais classique a connu un échec cuisant et définitif devant la Haute-Cour. Jusqu'à cette décision, Google Switzerland Sàrl avait régulièrement et dans plusieurs affaires (dont celle afférente à son service *Google Suggest*[109]) excipé de son absence de qualité pour défendre. Seule la société Google Inc. pouvait ainsi faire l'objet d'une procédure, sous d'autres réserves (absence de for en Suisse, droit suisse inapplicable, etc.). En première instance déjà, le Tribunal administratif fédéral avait retenu, nonobstant ces dénégations, qu'une recommandation pouvait être signifiée à cette société de droit suisse en raison de sa qualité de représentante dans notre pays de la société mère Google Inc. et compte tenu du fait que c'est elle qui traite les requêtes d'effacement[110]. Le Tribunal fédéral a quant à lui confirmé la qualité pour défendre de Google Switzerland Sàrl, reprenant pour l'essentiel l'argumentation développée par le Tribunal administratif fédéral (considérant 4). Il est précisé qu'il importe peu de savoir de quelle manière est organisée l'activité entre les deux sociétés s'agissant de la production et du traitement des images collectées dans le cadre du service GSW. Cette décision ouvre donc la voie à de nombreuses procédures à l'encontre de Google Switzerland Sàrl, relativement épargnée jusqu'ici en raison de décisions cantonales déniant sa qualité pour défendre[111].

C. Le lobbying indirect exercé par Google

On ne saurait terminer cette présentation de l'arrêt GSW sans mentionner la campagne de communication originale, dénommée *Et votre Google Street View*, que Google a entrepris en parallèle à sa saisine du Tribunal fédéral. Durant les mois qui ont suivi le dépôt du recours, Google Suisse a diffusé, à plusieurs reprises sur les chaînes de télévision nationale, un spot publicitaire tendant à démontrer l'utilité de son service de navigation. Ici on voit un entrepreneur planifiant une excursion à bicyclette, là une future mariée cherchant à se familiariser avec les lieux de la cérémonie ; sans oublier cette personne en fauteuil roulant qui souhaite repérer la place de parc pour handicapé la plus proche. Tous vantent les mérites du GSW ![112]

Conscient du fait que le lobbying des tribunaux est chose impensable – indépendance de la justice oblige -, Google s'est prudemment abstenu de faire toute allusion à l'affaire en cours dans la publicité diffusée. Reste que l'on ne peut s'empêcher d'observer que cette campagne inédite dans

l'utilité de GSW puisque cet argument a pesé lourd dans la balance; sans lui, l'obligation absolue de flouter les visages et les plaques d'immatriculation aurait été confirmée (cf. infra 5.1).

VII. Conclusion : and the winner is…

A. Un vainqueur-surprise

L'arrêt du Tribunal fédéral a suscité des réactions satisfaites de toutes les parties[113]. Notre Haute Cour a-t-elle exaucé les souhaits de chacun et rapproché les camps d'adversaires ayant respectueusement, mais sérieusement échangé leurs points de vue ? S'il s'était agi d'une joute de pugilistes, le Préposé l'aurait peut-être emporté aux points, vu que sa recommandation a été dans une large mesure confirmée. Qu'importe, car en réalité le Citoyen et le iCitoyen sont les vrais vainqueurs de ce procès historique [114]. Le iCitoyen, car il pourra continuer à utiliser le performant service GSW tout en bénéficiant d'une haute protection de sa personnalité en comparaison internationale; quant au Citoyen rétif aux nouvelles technologies, la protection de sa sphère privée sera assurée par des mécanismes classiques de publication, ce qui lui évitera les déconvenues liées à l'absence d'accès au web.

Le Tribunal fédéral a ainsi fait preuve d'une vision de la problématique à la fois profonde et dynamique. Il a non seulement posé de stricts garde-fous, mais il a aussi tenu compte des futurs développements de GSW. C'est réjouissant, car au début de la procédure, rien n'était acquis, ni même formalisé. Désormais, Google Inc. et Google Switzerland Sàrl devront respecter un code de conduite posant des conditions claires, évolutives et soumises à vérification quasi-permanente. Ce dernier point mérite également d'être salué : GSW est placé sous la tutelle du Préposé à la protection des données dont le rôle sort indiscutablement renforcé. Gageons qu'il saura assurer le « service après-jugement » face aux développements que cette technologie de navigation connaîtra sous peu.

B. Une implémentation qui sera difficile et dispendieuse

A Google, il incombe désormais d'assurer le respect des conditions posées par le Tribunal fédéral. Les surcoûts générés par un traitement manuel généralisé avaient été vivement critiqués, ce qui a emporté la conviction du tribunal. Reste que pareil traitement manuel devra être entrepris pour toutes les images déjà réalisées et ne respectant pas les réquisits jurisprudentiels. Cela concerne tant les images déjà publiées (avec par exemple une intrusion dans un espace privé) que celles déjà réalisées, mais pas encore publiées (soit celles soumises à l'accord sur les mesures provisionnelles). Sera-t-il moins coûteux de réaliser de nouvelles images sur la base des standards issus de la jurisprudence ou de traiter les millions d'images litigieuses ? La réponse à cette question permettra également de dire si le coût du traitement manuel était aussi disproportionné que le prétendait Google durant la procédure.

En bref, on peut se demander s'il n'eut pas été plus judicieux pour Google d'accepter la recommandation initiale du Préposé. Il aurait en effet gagné un temps précieux et aurait déjà pu mettre en ligne un panorama complet des localités suisses. Or celui est aujourd'hui lacunaire au point que, si Google ne procède pas rapidement aux adaptations et compléments requis, les consommateurs risquent de se détourner de GSW au profit de nouveaux concurrents tels que Bing Street Side[115].

Los delitos informáticos y su ausencia en la legislación penal mexicana[116].

Por Alberto E. Nava Garcés[117]

I. Informática jurídica y Derecho

Toda la historia de la humanidad y del derecho ha conocido el fenómeno de cómo el avance tecnológico se suele presentar antes que la regulación jurídica.

Esto es lo usual, en la convivencia humana y en el desarrollo del progreso al que el hombre está vocacionado se van presentando avances y creaciones tecnológicas. El riesgo de todo avance tecnológico siempre ha sido que el hombre quede al servicio de la tecnología y no al revés, el trastocar el fin por el medio es una amenaza omnipresente.

En las épocas en las que los avances tecnológicos espectaculares se separaban por largos espacios de tiempo el riesgo era más manejable, el hombre iba conociendo el despliegue científico poco a poco, los procesos de rechazo al cambio se desplegaban en el tiempo y poco a poco venían siendo combatidos por las inevitables ventajas del descubrimiento[118]

Curiosamente el cambio tecnológico que nos ocupa proporciona al Derecho una extraordinaria herramienta para ponerse al día con la época y responder mejor a los avances tecnológicos.

II. Delitos informáticos y su tratamiento

"La difusión de la informática en todos los ámbitos de la vida social ha determinado que se le utilice como instrumento para la comisión de actividades que lesionan bienes jurídicos y entrañan el consiguiente peligro social, o que sea la propia informática el objeto de atentados criminales: Estas facetas compendian la noción genérica del "delito informático", es decir, aquel conjunto de conductas criminales que se realizan a través del ordenador electrónico, o que afectan el funcionamiento de los sistemas informáticos." Dicho así por Pérez Luño, podemos entender entonces de la calificación de "delito informático", no como un delito *per se*, ya que el carácter esencial para el Derecho penal es la conducta.

A diferencia de lo señalado por Pérez Luño, consideramos que el problema no está en la constitución del delito sino en la forma de probar ese delito, en la forma de establecer fehacientemente el nexo causal. Ese es, en nuestra opinión el gran problema a vencer: lo etéreo de una página web, la manera tan sencilla de enviar un virus a la red desde cualquier lugar del mundo. El problema estriba en encontrar al autor de ese delito, saber dónde cometió el delito y donde afectó ese delito, aquí el principio *Lex Loci Comissi Delicti*, encuentra sentido, pero cabe preguntarse ¿se juzgara donde se fabricó el virus o donde hizo daño? ¿ambas legislaciones lo comprenden como delito?

---

[116] Este artículo está hecho bajo la dirección del Dr. Ricardo Franco Guzmán

[117] Doctor en Derecho, especialista en Derecho penal, Profesor de Teoría de la Culpabilidad en el posgrado de la Facultad de Derecho, UNAM; Profesor de Derecho penal en la Universidad Anáhuac; ex Director de Investigación del INACIPE, ha colaborado para el despacho Franco & Franco abogados. Autor, de: *El error en el derecho Penal*; *Delitos Informáticos; Ley de datos en posesión de particulares con comentarios* y *La prueba electrónica en materia penal*, todos de editorial Porrúa

[118] MÉJAN Luis Manuel C.; *El Derecho a la Intimidad y la Informática*, Porrúa, México 1994. P. 51.

Casi el 90% de los delitos informáticos que investiga tienen que ver con Internet. Esto nos enlaza directamente con los problemas de inexistencia de fronteras que aparecen constantemente cuando tratamos estos delitos: ¿Cuál es la ley a aplicar en multitud de casos?

La solución pasa por una coordinación internacional, tanto a la hora de investigar como a la hora de aplicar unas leyes que deben contar con un núcleo común. Es decir, hay que unificar criterios: difícil será actuar contra un delito que sí lo es en un país y no en otro. En este sentido está trabajando, por ejemplo, la Unión Europea. ¿pero que hay en la legislación mexicana?

Es cierto, de todas formas, que un delito informático puede ser simplemente un delito clásico en un nuevo envoltorio.

Como podemos observar, lo complejo del problema y el uso de las nuevas tecnologías traen aparejados nuevos problemas, pero sobre todo, el compromiso de no intentar resolver un problema global con respuestas regionales que de ello se valen los delincuentes informáticos para cubrirse en este rostro de impunidad que azota al hombre moderno.

III. Momentos del delito informático

Tres son las etapas en las que se funda la existencia de un delito informático: la de su inclusión en los catálogos penales (legislación), la forma en que se debe investigar (forense informática) y, la forma en que se acredita ante un juzgado o tribunal (prueba electrónica). En México aun no pasamos de enfrentar la primera.

Debemos partir de dos preguntas, la primera: ¿están legislados los delitos informáticos en todo el país? y, la segunda que pudiera parecer tautológica: ¿son federales todos los delitos del Código Penal Federal? La respuesta a ambas interrogantes es no.

Los delitos informáticos previstos en el Código penal federal, sólo son aplicables en los supuestos del artículo 50 de la Ley Orgánica del Poder Judicial de la Federación.

El legislador tiene, entre otros pendientes, legislar y unificar el tratamiento que deberá darle a los llamados delitos informáticos con el fin de no dejar vacíos que son aprovechados por la criminalidad "en línea" o informática. Lo hemos señalado antes: "El sueño de un mundo automatizado se puede volver en la pesadilla de quienes han puesto sus bienes al alcance de cualquier medio electrónico".

IV. La legislación sobre la materia

En 1999, cuando el Código Penal Federal regía en el Distrito Federal para los delitos de fuero común se incluyó el catálogo de delitos (pero sirva recordar: sólo para el Distrito Federal y sólo para los delitos del fuero común) en el Título Noveno denominado "Revelación de Secretos y acceso ilícito a sistemas y equipos de informática" (artículos 211 bis 1 al 211 bis 7**.**

Pero, ese mismo año, la legislación en materia penal quedó como una facultad a cargo de la Asamblea legislativa, la cual fue ejercida y se promulgó el efímero Código Penal para el Distrito Federal, cuya vigencia se extendió hasta 2002, cuando se publicó el entonces Nuevo Código Penal para el Distrito Federal[119], entre cuyas características destacó la ausencia de legislación en materia informática, con la salvedad del mal hecho artículo 231, fracción XIV que hace referencia a

[119] Que en 2006 suprimió la parte de su título que decía"Nuevo".

transferencias por medio electrónico (Recientemente la Corte se pronunció sobre el particular, pero refiriéndose a la incompetencia de la Asamblea Legislativa del Distrito Federal para crear leyes que se refieran, como acontece, respecto al sistema financiero mexicano).

Por lo que respecta a las legislaciones de los estados y por cuanto hace a los delitos informáticos, tenemos que en los códigos penales de Aguascalientes y Tabasco establecen dichas figuras entre los Delitos contra la seguridad en los medios informáticos y magnéticos; Baja California los establece en los Delitos contra la inviolabilidad del secreto; Chiapas, en los Delitos en contra de las personas en su patrimonio; Colima, Puebla, Querétaro, Zacatecas y Morelos, en los Delitos contra la moral pública; Oaxaca, en los Delitos contra la moral pública y en los Delitos contra la libertad y violación de otras garantías y; Tamaulipas, en los Delitos de revelación de secretos y de acceso ilícito a sistemas y equipos de informática.

Por su parte dentro de los códigos penales de Baja California Sur, Campeche, Chihuahua, Coahuila, Durango, Estado de México, Guanajuato, Guerrero, Hidalgo, Jalisco, Michoacán, Nayarit, Nuevo León, Quintana Roo, San Luis Potosí, Sonora, Tlaxcala, Veracruz Llave y Yucatán, no se contiene disposición relativa sobre el particular.

Frente a esta ausencia legislativa, es común que se petenda dar efectos extensivos a los delitos informáticos contenidos en el Código Penal Federal, sin embargo, ya la Corte se ha pronunciado sobre el particular, advirtiendo la incompetencia en la que incurren los agentes del Ministerio Público de la Federación o los Tribunales Federales cuando el afectado no cumple con las hipótesis contenidas en el artículo 50 de la Ley Orgánica del Poder Judicial de la Federación.

V. Conflicto competencial

Por lo que si las conductas se despliegan en el ámbito local, no hay fundamento que permita federalizar dichas conductas con la aplicación del Código punitivo federal. Robustece lo anterior lo señalado en la siguiente tesis:

"Novena Época

"Instancia: Primera Sala

"Fuente: Semanario Judicial de la Federación y su Gaceta

"Tomo: XI, marzo de 2000

"Tesis: 1a./j. 3/2000

"Página: 119

"**Competencia Penal**. Aun cuando no se hubiere planteado correctamente, procede resolverla. Las cuestiones de competencia son de interés general, se rigen por el derecho público que reglamenta el orden general del estado en sus relaciones con los gobernados, los demás estados y cuando son entre autoridades judiciales se traduce en un reflejo de los atributos de decisión e imperio de que están investidas, por lo que no debe existir tardanza en establecer en qué fuero radica o a qué juzgador corresponde el conocimiento de determinada causa penal. Esta primera sala de la Suprema Corte de Justicia de la Nación, considera que la decisión de declarar la inexistencia del conflicto competencial, cuando alguna autoridad judicial no se pronunció sobre si es o no competente para conocer de una causa penal, o de ordenar la reposición del procedimiento, cuando no se siguieron las formas previstas para el planteamiento del conflicto produciría demora injustificada en perjuicio del interés general, del ofendido y del probable responsable, tal criterio debe aplicarse en los casos en que obran en el expediente los

elementos suficientes para dictar la resolución correspondiente y no hubiere duda para establecer el fuero en que radica la competencia, así como al órgano juzgador que corresponda su conocimiento, atendiendo a las reglas respectivas; en cambio, no es aplicable ese criterio en aquellos procesos penales en que exista duda sobre la determinación de la competencia, ya que ocasionaría el efecto contrario al que se pretende, porque retardaría la decisión que debe emitirse sobre el particular.

"Competencia 157/98. suscitada entre el Juez Décimo Segundo de Distrito en Materia Penal en el Distrito Federal, el Juez Vigésimo Segundo Penal del Distrito Federal y el Juez Primero Penal de Primera Instancia del Sexto Distrito Judicial del Estado de Morelos. 1o. de julio de 1998. cinco votos. ponente: Juan N. Silva Meza. Secretaria: Guillermina Coutiño Mata.

"Competencia 124/98. suscitada entre el Juez Primero de Distrito en el Estado de Sinaloa y el Juez Tercero de Distrito en Materia Penal en el Distrito Federal. 14 de octubre de 1998. Unanimidad de cuatro votos. ausente: Juan N. Silva Meza. ponente: Olga Sánchez Cordero de García Villegas. secretario: Jorge Carreón Hurtado.

"Competencia 427/98. Suscitada entre el Juez Segundo Penal en el Estado de Aguascalientes y la Juez Vigésimo Octavo Penal en el Distrito Federal. 4 de noviembre de 1998. unanimidad de cuatro votos. ausente: Juan N. Silva Meza. ponente: José de Jesús Gudiño Pelayo. secretario: Ismael Mancera Patiño.

"Competencia 158/99. Suscitada entre el Juez de lo Penal del Distrito Judicial de Chiautla de Tapia y el Juez Cuarto de Distrito, ambos en el Estado de Puebla. 26 de mayo de 1999. unanimidad de cuatro votos. ausente: José de Jesús Gudiño Pelayo. ponente: Humberto Román Palacios. secretario: Miguel Ángel Zelonka Vela.

"Competencia 288/99. Suscitada entre el Juez Primero Penal de Primera Instancia del Distrito Judicial de Uruapan, Michoacán y el Juez Cuadragésimo Noveno Penal en el Distrito Federal. 25 de agosto de 1999. Cinco votos. ponente: Juventino V. Castro y Castro. Secretaria: Rosalba Rodríguez Mireles.

"Tesis de jurisprudencia 3/2000. Aprobada por la Primera Sala de este alto tribunal, en sesión de primero de marzo de dos mil, por unanimidad de cinco votos de los señores ministros: presidente José de Jesús Gudiño Pelayo, Juventino V. Castro y Castro, Humberto Román Palacios, Juan N. Silva Meza y Olga Sánchez Cordero de García Villegas."

Estas hipótesis que se refieren a las reglas que deben tomarse en cuenta para la resolución de un conflicto competencial, deben concatenarse con los supuestos en que debe conocer del asunto un órgano jurisdiccional del fuero federal; esto es, con los supuestos contenidos en el artículo 50 fracción I, de la Ley Orgánica del Poder Judicial de la Federación, que a la letra dispone:

"ARTICULO 50. Los jueces federales penales conocerán:

"I. De los delitos del orden federal.

"Son delitos del orden federal:

"a) Los previstos en las leyes federales y en los tratados internacionales. En el caso del Código Penal Federal, tendrán ese carácter los delitos a que se refieren los incisos b), a l) de esta fracción;

"b) Los señalados en los artículos 2 a 5 del Código Penal;

"c) Los cometidos en el extranjero por los agentes diplomáticos, personal oficial de las legaciones de la República y cónsules mexicanos;

"d) Los cometidos en las embajadas y legaciones extranjeras;

"e) Aquellos en que la Federación sea sujeto pasivo;

"f) Los cometidos por un servidor público o empleado federal, en ejercicio de sus funciones o con motivo de ellas;

"g) Los cometidos en contra de un servidor público o empleado federal, en ejercicio de sus funciones o con motivo de ellas;

"h) Los perpetrados con motivo del funcionamiento de un servicio público federal, aunque dicho servicio esté descentralizado o concesionado;

"I) Los perpetrados en contra del funcionamiento de un servicio público federal o en menoscabo de los bienes afectados a la satisfacción de dicho servicio, aunque éste se encuentre descentralizado o concesionado;

"j) Todos aquéllos que ataquen, dificulten o imposibiliten el ejercicio de alguna atribución o facultad reservada a la Federación;

"k) Los señalados en el artículo 389 del Código Penal cuando se prometa o se proporcione un trabajo en dependencia, organismo descentralizado o empresa de participación estatal del Gobierno Federal;

"l) Los cometidos por o en contra de funcionarios electorales federales o de funcionarios partidistas en los términos de la fracción II del artículo 401 del Código Penal, y

"m) Los previstos en los artículos 366, fracción III; 366 ter y 366 quáter del Código Penal Federal, cuando el delito sea con el propósito de trasladar o entregar al menor fuera del territorio nacional.

"II. De los procedimientos de extradición, salvo lo que se disponga en los tratados internacionales.

"III.- De las autorizaciones para intervenir cualquier comunicación privada."

Lo transcrito significa que, dentro de las hipótesis normativas que le dan la competencia al órgano federal, no se encuentra ubicada la que le permita juzgar supuestos hechos ocurridos entre particulares, cuya calidad de sujetos activos o pasivos, no los ubica tampoco en el ámbito federal.

El Código Penal Federal es una ley federal, no obstante para poder considerar su contenido como "ley federal" en términos del artículo 104, fracción I constitucional, o dicho de otro modo, para poder estimar como federales los tipos que en él se prevén, es necesario que la conducta tipificada como tal corresponda a alguna de las materias respecto de las cuales la Federación tiene alguna facultad para legislar en toda la República o, porque se trate de un tipo en el que la Federación sea el sujeto pasivo, dado que la calidad de federal de un "delito" no proviene de que se encuentre previsto en el mismo, así como tampoco puede considerarse como ley federal el Código Penal Federal por el hecho de así denominarse, sino que, será ley federal en cuanto prevea delitos relacionados con las fracciones XXI y XXX y demás relacionadas, del artículo 73 constitucional.

En ese tenor, nuestro más alto Tribunal consideró de manera correcta en su ejecutoria:

"**Supuestos de competencia de los Tribunales Federales que establece el artículo 104, fracción I de la Constitución Federal:**

El artículo 104, fracción I de la Constitución Federal establece textualmente:

Art. 104.- Corresponde a los Tribunales de la Federación conocer:

I.- De todas las controversias del orden civil o criminal que se susciten sobre el cumplimiento y aplicación de leyes federales o de los tratados internacionales celebrados por el Estado Mexicano. Cuando dichas controversias sólo afecten intereses particulares, podrán conocer también de ellas, a elección del actor, los jueces y tribunales del orden común de los Estados y del Distrito Federal. Las sentencias de primera instancia podrán ser apelables para (sic) ante el superior inmediato del juez que conozca del asunto en primer grado.

El artículo en estudio establece supuestos de competencia para los Tribunales Federales y locales y, la concurrencia de ambos órdenes.

Primer supuesto de competencia, **tribunales federales,** los que serán competentes si concurren los siguientes requisitos:

a) Que se trate de controversias del orden civil o criminal;

b) Que las mismas versen sobre el cumplimiento o aplicación de leyes federales o tratados internacionales.

c) No es relevante si el interés que se afecta es particular o no, en ambos casos se surtirá la competencia.

Segundo supuesto de competencia, **tribunales locales,** los que serán competentes si concurren los siguientes requisitos:

a) Que se trate de controversias del orden civil o criminal;

b) Que las mismas versen sobre el cumplimiento o aplicación de leyes federales o tratados internacionales y,

c) Que **sólo afecten intereses particulares**, y el actor elija los tribunales locales, en obvia exclusión del orden federal, para que se dirima la controversia.

La controversia criminal tiene como objetivo determinar si cierta conducta es constitutiva de delito, así como la responsabilidad en su comisión; en ese sentido es relevante tener en consideración que el delito si bien ataca los derechos de cierto individuo, también atenta, sea en forma mediata o inmediata, contra los derechos del cuerpo social, por lo que en tal supuesto si bien existe el interés del particular afectado, lo cierto es que también se afectan intereses públicos, ya que es de incumbencia del Estado sancionar las conductas constitutivas de delitos. […]

En otras palabras, los tipos penales previstos en el Código Penal Federal serán "delitos federales", si se refieren a alguna materia, respecto de la cual la Federación tenga atribuida alguna facultad y/o, cuando el sujeto pasivo del ilícito lo sea la Federación.

En ese estado de cosas, el artículo 50, fracción I, de la Ley Orgánica del Poder Judicial de la Federación, es el precepto legal que recoge el sistema de competencias expuesto, pues caracteriza los tipos penales que deberán ser considerados como federales cuando no se encuentren contemplados en una ley federal (ley específica que desarrolle alguna materia respecto de la cual el Congreso de la Unión cuente con facultad para legislar en toda la República), además de los tipos que, por contenerse en una ley referida a una de tales materias, lo son.[…]

VI. Conclusión

Por tanto, si un cierto tipo penal previsto en el Código Penal Federal no se encuentra caracterizado como "delito federal" en el artículo 50, fracción I, de la Ley Orgánica del Poder Judicial de la Federación, no podrá ser considerado como tal y por ende, si no se encuentra previsto en la legislación local, implicará su derogación tácita, ya que, como ha quedado de manifiesto, la facultad de legislar en materia penal es de incumbencia local, y, sólo en caso de que el sujeto pasivo lo sea la Federación o, que el supuesto de hecho tenga relación directa con alguna de aquellas materias respecto de las cuales ésta tiene facultad de legislar, podrá ser caracterizado como federal.

Así nuestro máximo Tribunal consideró que para resolver el problema de interpretación citado se determinó que el artículo 104 constitucional en su fracción I, cuando alude a "controversias del orden criminal que se susciten sobre el cumplimiento o aplicación del leyes federales" se refiere a los asuntos que surjan en virtud de tipos penales relacionados con las materias atribuidas a la Federación o las facultades para legislar que le estén conferidas constitucionalmente.

Y en ese tenor los delitos informáticos, son materia de cada legislación estatal o del Distrito Federal, por lo que su ausencia, en tratándose de particulares afecta sólo a los particulares mismos y si recurren a la intancia federal para eludir este vacío, no sólo no prosperará su acusación, sino que quedará sujeta a otra decisión que ya ha tomado la Corte respecto de actuaciones realizadas ante autoridad incompetente: la nulidad de dichas actuaciones y por ende, el final del camino por cuanto hace a este tema.

Cuando se haga la revisión legislativa se deberá tomar en cuenta que día a día existen nuevas amenazas en la red, conductas que están partiendo de esa misma naturaleza etérea con la que está hecha la supercarretera de la información (vocablo que está desapareciendo para referirse a internet).

Viejos recuerdos, nuevos finales: el derecho al olvido en el siglo XXI

María Eugenia Cabezas Velasco[120]
María Paula Garat Delgado[121]
Paula Rodríguez Medalla[122]
Stefanía Rainaldi Redón[123]
Daniela Risso Leites de Moraes[124]

Este trabajo fue realizado en el marco de las IX Jornadas Interuniversitarias de Derecho Constitucional y Derechos Humanos, celebradas en la Universidad Andrés Bello, Santiago de Chile, en Setiembre del año 2011, y presentado dentro del eje temático: *"Nuevos Derechos Fundamentales reconocidos en los ordenamientos jurídicos de Iberoamérica"*.

Introducción

Viejos recuerdos son los datos que conservamos en nuestra memoria, que han ocurrido en el pasado, muchos de los cuales queremos compartir con otros, otros que preferimos no divulgar. Sin dudas, muchos de nosotros hemos sido protagonistas de conductas inmorales o ilegales, las que no queremos recordar. La difusión de esta información, y los derechos humanos involucrados, han tenido un trascendental cambio desde el advenimiento de nuevas tecnologías, y particularmente con la aparición de Internet, lo que dificulta que estos viejos recuerdos sean olvidados.

Nos proponemos aquí presentar un derecho que se pone en juego a diario, en nuestras acciones cotidianas, y que, sin embargo, parece olvidado. Si bien pueden plantearse diversos ejemplos en torno a este derecho, limitaremos el presente trabajo a lo que refiere exclusivamente a las implicancias que Internet y las nuevas tecnologías traen aparejadas, dejando de lado otros temas de importancia, los que también poseen vinculación con el olvido.

Seguramente muchas veces hemos puesto nuestro nombre en el buscador de Google, o incluso, observamos frecuentemente cómo otros ven nuestro perfil de Facebook o la página de Twitter. Sin embargo, no son tantas las veces en que nos hemos preguntado: ¿qué ocurriría si junto a nuestro nombre, en los resultados de Google o Yahoo, aparecieran calificativos deshonestos, malas acciones, o imágenes no autorizadas? ¿Cómo garantizar los derechos humanos cuando nos referimos a los nuevos avances tecnológicos?

Lejos de plantearnos situaciones que, sin duda, demuestran gran trascendencia, pero por las que no estamos acostumbrados a transitar; abordaremos aquí una problemática que, si

---

[120] Estudiante de Cuarto año de Derecho de la Universidad Católica del Uruguay.
[121] Doctora en Derecho, Universidad Católica del Uruguay. Aspirante a Profesor de Derecho Constitucional de la mencionada Universidad.
[122] Estudiante de Quinto año de Derecho de la Universidad Católica del Uruguay.
[123] Estudiante de Cuarto año de Derecho de la Universidad Católica del Uruguay.
[124] Doctora en Derecho, Universidad Católica del Uruguay.
Las autoras, actuales egresadas y estudiantes de la Facultad de Derecho de la Universidad Católica del Uruguay, agradecen muy especialmente la coordinación a cargo de la Dra. Alicia Rodríguez Galusso y el Dr. Edgardo Amoza, profesores de Derecho Constitucional de la mencionada Facultad, por la disposición, la ayuda y el apoyo brindado.

bien se vislumbró desde hace ya algunos años, se encuentra en nuestra actualidad con vehemencia, particularmente, desde la aparición de nuevas tendencias tecnológicas, y del uso de las redes sociales en Internet.

¿Qué ocurre con la información brindada a diversas páginas de Internet que ya no queremos compartir? ¿Es posible eliminar los *metadatos* obtenidos, esto es, la información que deriva indirectamente de los "me gusta", las fotografías o nuestros comentarios en Facebook u otras redes?

Cuando incorporamos una imagen, demostramos inclinación por un grupo de música o un restaurant, colocamos un enlace, o comentamos una noticia, se están adquiriendo datos de nosotros, ya sea de forma consciente o inconsciente. Estos datos, a su vez, pueden ser retransmitidos, y construir, a partir de ello, diversos rasgos de nuestra personalidad. Es información referente a nuestro círculo de privacidad que permanecerá, aún sin saberlo, años y años en Internet.

Incluso sin Internet, en la época actual, se transmite información al realizar acciones que parecen no tener mayor transcendencia, como una compra con una tarjeta que acumula puntos, con una tarjeta de crédito, o al utilizar el sistema de transporte colectivo abonando el pasaje con una tarjeta magnética.

Por consiguiente, el conocimiento que se adquiere, va más allá de la información que proporcionamos directa y conscientemente; el uso que el dominio de la página web o el titular de la base de datos le puede dar escapa, sin dudas, a nuestra imaginación. En este marco, el derecho a la intimidad ha quedado desprovisto ante tal avance tecnológico, necesitando de nuevas herramientas para su tutela; y aún, esta situación, ha originado la necesidad de reconocer nuevos derechos en pugna.

Son muchos los acontecimientos personales que no queremos difundir, sea por considerarlos dentro de nuestra privacidad individual, por encontrar acciones pasadas embarazosas, o, simplemente, por querer que nuestra conducta del pasado, o nuestras fotografías, no sean conocidas por otros. Imágenes vergonzosas, fallos jurisprudenciales, y muchos datos más pueden ser asociados a nuestra persona en tan solo un *click* de distancia. En el mundo de la transparencia, que parece ser Internet, cancelar esta información, quitarla, o eliminarla se presenta como una tarea complicada. Entonces nos preguntamos: ¿Tenemos un derecho al olvido?

La evolución tecnológica, la masividad que apareja Internet, sumado a las dificultades para controlar la información reinante en las nuevas tecnologías, fueron propicias para el surgimiento del derecho al olvido, un nuevo derecho, vinculado a la intimidad, privacidad y honor.

Nos proponemos abordar aquí la situación actual y la importancia que este derecho conlleva para la misma, estudiando sus antecedentes, su aplicación práctica, así como el reconocimiento y las garantías existentes para su tutela, atendiendo, en este último punto, a los particularismos que presenta el caso uruguayo.

El derecho al olvido, concepto y antecedentes

La palabra "olvido" deriva del verbo "olvidar", proveniente del latín *"obitare"*, que implica quitar de la memoria algo que se tenía[125]. El derecho al olvido aparece, entonces, como un derecho que posee todo sujeto a eliminar los datos o información que se conserva de su

[125] Diccionario de la Real Academia Española

persona. Mientras que el derecho a la intimidad protege la obtención de los datos referidos a nuestra esfera personal; el derecho al olvido cumple un rol posterior, enfocándose en la supresión de datos que ya se han hecho públicos, con o sin consentimiento del titular.

Este derecho, tal como señala la doctrina, no es nuevo ni reciente, sino como decía Nietzsche: *"toda acción exige el olvido, así como todo organismo tiene necesidad no apenas de luz, sino también de oscuridad"*[126].

Sin embargo, y si bien antes de Internet poseíamos un amplio caudal de información disponible, no sólo el acceso a la misma se veía limitado, sino que eran muy pocos los aspectos de la vida de una persona que llegaban a conocimiento público. Ello llevó a que la consagración del derecho al olvido estuviera específicamente relacionada con las bases de datos crediticias y penales; pues, éstos eran los aspectos más relevantes para la conducta del sujeto.

En tal sentido, el derecho al olvido fue reconocido, primeramente, en estas dos áreas. En Argentina, por ejemplo, la jurisprudencia por Sentencia del año 1999[127], hace mención al mismo. El actor requería que se eliminara información, con más de cinco años de antigüedad, de una base de datos que lo inhabilitaba para operar por cuenta corriente en todo el territorio del Estado. La parte demandada sostuvo que al no estar reglamentada la actividad, no había norma alguna que le impusiera la supresión y no difusión de dicho dato, luego de transcurridos cinco años. La Sala hace lugar a la demanda, invocando el derecho al olvido, y realizando una analogía con el artículo 51 del Código Penal Argentino, que dispone que el registro de sentencias condenatorias caduca después de transcurridos cinco años desde su extinción para las sanciones de inhabilitación.

El reconocimiento de este derecho, en Argentina, se hizo necesario, y se consagró en el artículo 26 inciso 4 de la Ley 25.326, sancionada el 4 de Octubre del 2000. Esta norma alude al deber de utilizar únicamente los datos personales de los últimos cinco años, para evaluar la solvencia económica del sujeto. En este punto, puntualiza la doctrina que: *"El acopio de información crediticia tiene una limitación temporal establecida por la ley con el propósito de permitir la recuperación de quien superó una situación adversa y procura reinsertarse en la actividad económica. Se lo exime así de quedar 'prisionero de su pasado'"*[128].

En Costa Rica, por otra parte, la Sala Constitucional ha desarrollado la noción del derecho al olvido en materia crediticia, estableciendo un límite de cuatro años para el almacenamiento de datos referentes al historial de incumplimientos financieros, lo que llevó a modificar el reglamento para la calificación de deudores[129].

Anteriormente a ello, este derecho tuvo consagración expresa en la *Fair Credit Reporting Act*, de Estados Unidos, en 1970; y más recientemente, en la Ley 19.628 de Chile.

En Uruguay, por su parte, el derecho al olvido fue reconocido por el artículo 9 de la Ley 17.838, al establecer que los datos personales relativos a obligaciones de carácter comercial sólo podrían ser conservados por un plazo de cinco años, contados desde su incorporación. Este mismo plazo es el previsto, posteriormente, en el artículo 22 de la Ley 18.331, sancionada el 11 de agosto de 2008, la que continúa vigente.

---

[126] SCHWOB, Marc. *Como conservar e desenvolver sua memoria*. Rio de Janeiro, Ediouro Publicaciones, 2005, p. 94.
[127] Sentencia del Juzgado Nacional de Primera Instancia en lo Civil, No. 36/1999, dictada el 12 de noviembre de 1999, en la causa: *"Camjalli, Alberto c/ Organización Veraz S.A. s/ Habeas Data (No. 7678/99)"*.
[128] DRUCAROFF AGUIAR, Alejandro. *Información crediticia, derecho al olvido e interés general.* Artículo Publicado en Revista La Ley Online, consultado en: *www.laleyonline.com.uy*
[129] Consejo Nacional de Supervisión Financiero. Reforma del Reglamento para Calificación de Deudores. Acta de Sesión 607-2006, celebrada el 12 de Octubre de 2006.

Asimismo, vinculado a la esfera penal, el Tribunal de Apelaciones en lo Civil de Segundo Turno, de Uruguay, expresó: *"En la actualidad el derecho al olvido se encuentra establecido por el art. 329 de la Ley No. 16226 que dice: 'En los casos en que el proceso penal finalice mediante revocación del procesamiento y absolución, el Registro Nacional de Antecedentes Judiciales eliminará de las planillas que expida posteriormente, toda referencia al hecho que determinó el enjuiciamiento'"*[130]. Sin embargo, se enlaza también, en este caso, al derecho al olvido con los medios de comunicación, ya que éste es invocado tras los perjuicios que aparejó la publicación de los antecedentes penales de un sujeto en un periódico nacional.

En este punto, la Suprema Corte de Justicia entendió que: *"La afirmación de que la indicación de antecedentes no supuso invasión de la privacidad del actor no es aceptable, ya que consistió en una publicación de antecedentes personales reservados (existencia de un Tribunal de Honor y un proceso penal) con un fin espurio y sin interés público que lo legitime. Todo ello sin duda, supone una agresión al derecho a la dignidad, atributo de la personalidad humana…"*[131].

Con ello, entonces, se vislumbra la existencia del derecho al olvido, como un derecho vinculado al honor y a la intimidad, que tuvo especial aplicación en lo que refiere a los medios públicos de comunicación, y que adquirirá, hoy en día, mayor reconocimiento en lo que atañe, específicamente, a la problemática vinculada a las nuevas tecnologías, las que afectan su efectividad. En el presente análisis, nos concentraremos en el estudio de esta nueva dimensión, dejando de lado su aplicación en otros ámbitos.

En definitiva, definimos al derecho al olvido como aquel derecho humano que posee todo individuo de poder suprimir o eliminar todo tipo de datos o información sobre su persona, que exista o esté almacenada en cualquier tipo de soporte, y que afecte o vulnere su intimidad, honor, imagen, seguridad o algún otro derecho inherente a su personalidad. El derecho al olvido comprende no solo aquella información publicada, almacenada, o emitida por un tercero, sino también los datos que voluntariamente se han hecho públicos y que ya no se quieren compartir.

Los derechos ante una nueva era tecnológica: la realidad actual

En 1944, Jorge Luis Borges escribió un breve relato que incluyó en su obra denominada "Artificios", la que se incorporó al gran libro "Ficciones". Contaba la historia de Irineo Funes, un joven que después de un accidente descubre que posee una memoria infalible, capaz de recordarlo todo.

Borges cuenta como Funes: *"…no sólo recordaba cada hoja de cada árbol, de cada monte, sino cada una de las veces que la había percibido o imaginado"*. Esto, lejos de ser una virtud, creaba una constante confusión en el mundo de Funes, ya que su memoria no le permitía ir más allá de lo fáctico y relacionarse con sus pares. Funes vivía del recuerdo, y, como concluye el autor: *"…no era muy capaz de pensar. Pensar es olvidar diferencias, es generalizar, abstraer. En el abarrotado mundo de Funes no había sino detalles, casi inmediatos"*[132].

Lo que Borges no sospechaba, al momento de publicar dicho relato, es que la era digital vendría a recrear su fantasía, instituyendo una plataforma universal, capaz de aglomerar

[130] Sentencia del Tribunal de Apelaciones en lo Civil de Segundo Turno, dictada el 24 de Febrero de 1992, en el caso *"González Sacco, Hugo contra Diario Matutino "La República" (Reg S.A.); Federico Fassano y otros. Daños y Perjuicios"*, Ficha No. 238/91.
[131] Sentencia de la Suprema Corte de Justicia, dictada el 8 de Diciembre de 1993, en el caso *"González Sacco, Hugo contra Diario Matutino "La República" (Reg S.A.); Federico Fassano y otros. Daños y Perjuicios"*, Ficha No. 238/91.
[132] BORGES, Jorge Luis. *Ficciones.* Buenos Aires, Emece, 1956.

información personal acerca de todos los individuos, acumulando datos sensibles de manera inmediata, y conservándolos por períodos de tiempo indeterminados.

Asimismo, Borges tampoco imaginaba que nuestras acciones cotidianas pudieran ser objeto de diversas bases de datos que incluyeran nuestras compras, trayectos, inclinaciones, entre otras. Pues, hoy en día, al igual que en Funes, no hay sino detalles.

A. El olvido en Internet

Habiendo nacido como una red interna de la Universidad de Harvard, creada por Mark Zuckerberg, Facebook fue abierta para Estados Unidos en el año 2007, y llega, actualmente, a su cúspide, teniendo, en 2011, más de 750 millones de usuarios activos. Apareció así, como una red social que revolucionó la comunicación interpersonal y los hábitos de sus miembros. Anteriormente a ésta, otras redes han sido creadas, aunque no con tanta difusión, como Fotolog, Linked In, My Space, MSN Spaces, Hi5, Flickr y Orkut. Hacia el año 2006, llegarían también Twitter, Xing, y Tuenti, entre otras.

Internet y la comunicación por esta vía se han convertido en el nuevo fenómeno de nuestro tiempo, característico de la época actual. El uso de Internet se ha acrecentado considerablemente, tanto en lo que atañe a compartir información, como en lo que hace a la investigación y al enriquecimiento del conocimiento. Para esto último, la labor de los buscadores resulta fundamental, como canal de difusión de los diversos datos que se encuentran contenidos en las páginas webs. En este marco, el avance en los procedimientos que llevan a indexar información, así como las búsquedas sugeridas y los nuevos mapas satelitales, son las recientes novedades de Google, Yahoo, Bing, y otras páginas que, en un 80%, hacen llegar la información al usuario de la red.

Sin embargo, tantos datos contenidos en las páginas, lleva a cuestionar el derecho a la intimidad de los individuos. Muchos son los casos en los que ello ha llegado a organismos administrativos y aún jurisdiccionales. Anteriores procedimientos de tutela, como el habeas data, se presentan como insuficientes, ante las particularidades de esta nueva etapa. Tal como ya había señalado nuestra doctrina: *"El avance de la tecnología y la afirmación de los derechos del hombre en la democracia, exigen hoy nuevas reglas de derecho que, dentro del respeto de aquellos principios constitucionales, extiendan el amparo legal a situaciones que no pudieron preverse en su momento"*[133].

Un ejemplo de ello, lo constituye la afectación de muchas familias, al no poder cerrar la cuenta de Facebook de un miembro luego de su defunción, sino después de numerosos trámites. Pues, al no tener conocimiento de la contraseña del fallecido, se les hace engorroso ponerle un fin a las publicaciones, que les resultan por demás dolorosas.

Estas, y muchas otras situaciones, no fueron previstas por la protección a los datos consagrada en la normativa específica aplicable a la materia. La ligera y constate evolución en lo que refiere a Internet, hace que muchos mecanismos de tutela hayan resultado insuficientes, habiendo surgido nuevos derechos para amparar su particular problemática, como ocurre con el derecho al olvido.

En algunos casos, son los propios afectados los que publican los datos que, luego de algunos años, se vuelven lesivos para su personalidad, originando un estigma muy difícil de

[133] CORREA, Carlos, NAZAR, Félix, CZAR, Susana, BATTO, Hilda. *Derecho Informático.* Buenos Aires, Depalma, 1987, p. 243.

sobrellevar. En otros, esta difusión se hace mediante terceras personas, y refiere a información que no es verídica, o que, aún siendo verdadera, su titular no desea que llegue al conocimiento público. El derecho al olvido recae, como veremos, en la posibilidad de eliminar el recuerdo de un sujeto, habiendo sido proporcionado voluntariamente o no, almacenado de forma consciente, o aún sin saberlo.

En España, por ejemplo, se demandó al Ayuntamiento de Monterrubio de Armuña, en Salamanca, para que quitara de su página web los datos referidos al expediente y decretos de despido de tres denunciantes, por las perjudiciales consecuencias que la difusión por este medio apareja[134]. Asimismo, en otro supuesto, se pretendió la eliminación de los videos con imágenes del hijo de la denunciante y de su familia, así como los comentarios realizados al respecto, incorporados en las páginas cuyo dominio pertenecía a Facebook y a Youtube[135].

Se presentaron hipótesis aún más graves, considerando las consecuencias del "Street View" creado por Google. Con esta aplicación, es posible obtener imágenes reales, recorriendo ciudades y calles. Organismos protectores de datos, en Suiza y Alemania, han proclamado su preocupación al respecto, tras la información sensible que pudieran obtener[136]. En Estados Unidos, este supuesto fue planteado, entre otros, en "Boring vs Google"[137], reclamando el derecho a la privacidad y la injerencia en su derecho a la propiedad por influjo de esta nueva invención.

Por otra parte, los individuos también se sienten lesionados en su honor al descubrir que los buscadores recomiendan búsquedas relacionadas a su nombre que resultan dañosas, asociadas con acciones cometidas en el pasado, que quisieran no recordar. Es este el caso de un ciudadano francés, que descubrió que al buscar su nombre en Google, se arrojaba como primer resultado "violador"[138]. Lo mismo ocurrió con una docente, quien al redactar su nombre en el buscador, éste mostraba enlaces de un video pornográfico que ella había realizado cuando tenía 18 años[139].

En España, un caso similar fue el iniciado por la Sociedad General de Autores y Editores, la que se entendió perjudicada ante la asociación de su organización con la palabra "ladrón", lo que fue tratado en los órganos jurisdiccionales de Madrid[140]. En Italia, una compañía advirtió que al colocar su nombre en esta misma página, la búsqueda sugerida la relacionaba con los sustantivos "estafador" o "estafa", lo cual fue procesado ante el Tribunal de Milán, el que amparó la demanda[141]. Lo mismo ocurre en muchos otros casos. Por ejemplo, si escribimos "Ballymascanlon Hotel", un Hotel ubicado en Dundalk, Irlanda, se nos sugiere la palabra *"receivership"* lo cual indica una insolvencia económica. Dicha compañía entabló una demanda contra el sitio, la que continúa actualmente en trámite[142].

---

[134] Resolución No. R/01815/2010 de la Agencia Española de Protección de Datos, del 20 de Setiembre de 2009.
[135] Resolución No. R/00668/2011 de la Agencia Española de Protección de Datos, del 7 de Abril de 2011.
[136] Noticia publicada en el Diario El País, Barcelona, el 26 de Febrero de 2010, titulada: *La UE quiere limitar el empleo de imágenes en Street View. El servicio ofrece recorridos en video por las calles de más de cien ciudades,* consultado en: *www.elpais.com*
[137] Boring v. Google Inc., tramitado ante la United State District Court for the Western District of Pennsyilvania.
[138] RODRÍGUEZ, Vanesa. *Google, condenado en Francia por "difamación" en los resultados de búsqueda.* Noticia publicada en RTVE, el día 27 de Setiembre de 2010, consultada en: *www.rtve.es*
[139] SALVATIERRA, Blanca. *Francia obliga a Google a cumplir con el derecho al olvido digital.* Artículo publicado el 17 de Marzo de 2011 en Diario Público, Madrid, consultada en el sitio: *www.publico.es*
[140] Sentencia de la Undécima Audiencia Provincial de Madrid, dictada el 31 de Marzo de 2011, en el Procedimiento Ordinario No. 743/2007.
[141] Sentencia del Tribunal de Milán, dictada el 24 de Marzo de 2011.
[142] Noticia publicada en el Diario ABC, Madrid, el día 21 de Junio de 2011, titulada: *SGAE, Ramoncín, Coca-Cola…Cómo gestionar la mala reputación en internet*, consultado en *www.abc.es*

Si bien Google alega en estas situaciones que las páginas surgen de publicaciones de terceras personas en la red, lo que su sitio simplemente indexa o recopila, actualmente, varias sentencias alrededor del mundo lo han condenado, ordenando la eliminación de estos datos.

La Agencia Española de Protección de Datos, por ejemplo, procesa diariamente denuncias que refieren al tratamiento de datos en Internet, las cuales han llegado al dictado de resoluciones administrativas desfavorables para Google, Yahoo o Facebook. Estos casos transitan, incluso, en expedientes de Tribunales Jurisdiccionales, lo que ha ocurrido en igual medida en Francia, Italia o Bélgica.

Aún sin ir tan lejos, en Argentina, Brasil, Chile y Uruguay se iniciaron varias pretensiones vinculadas al cese de la utilización y a la cancelación de datos en Internet.

En el primero de estos países, son varios los personajes públicos que reclaman la supresión de la información injuriante hacia su persona, así como la eliminación de la asociación de su nombre con páginas inmorales[143]. También se procesaron casos de sujetos no famosos que al poner su nombre en el buscador se los relacionaba con expresiones altamente injuriantes, lo que repercutía en su entorno personal y profesional[144].

En Brasil, fue destacado el caso de un estudiante de química que dio inicio a una acción contra Google y Yahoo, con la intención de que dichos buscadores retiraran la vinculación de su nombre con el delito de interceptación ilegal de datos telemáticos, tras haber sido acusado de invadir la computadora de una de sus profesoras y, desde allí, retirar materiales con contenido erótico. Sin embargo, posteriormente, la investigación fue dejada sin efectos por la Comisaría de Represión de Delitos Informáticos, debido a la ausencia de pruebas suficientes. La defensa alegó que el derecho a la imagen, a la intimidad y al olvido eran garantías fundamentales del individuo, por lo que, los buscadores deberían ser responsabilizados por los daños causados[145].

Ha sido un avance a nivel mundial, la reforma realizada en este país, con la adopción del proceso digitalizado mediante la Ley 11.419 del año 2006. Con la misma, se instaura la posibilidad de que la totalidad de los actos procesales sean realizados vía web. Esta nueva realidad, presenta como ventajas una mayor celeridad del proceso, transparencia, efectividad y accesibilidad. Sin embargo, el lado negativo de este "e-pro", -como es llamado-, es que uno de los principios básicos del derecho procesal, como lo es la publicidad es llevado a otro nivel. Un proceso que transita libremente por Internet (salvo los exceptuados bajo secreto judicial), puede atentar contra la dignidad de los involucrados.

Con esto, el derecho al olvido se ve desconocido, ya que una causa aún concluida, estará en Internet por tiempo indeterminado. Ocurre, en muchas oportunidades, y particularmente en Uruguay desde la aplicación de la Ley de Acceso a la Información Pública No. 18.381 en el año 2008, que los organismos públicos informan sus resoluciones en Internet, pero luego éstas son revocadas, sea de oficio o en vía jurisdiccional. Sin embargo, la resolución original permanece incambiada, no vinculada con los nuevos hechos que acontecieron en torno a esta.

---

[143] Ver, por ejemplo: Sentencia del Tribunal CNCIV Sala L, dictada en Buenos Aires, el 18 de Junio de 2009, en el caso *"Mazza, Valeria Raquel c/ Yahoo de Argentina SRL y otros s/ Medidas precautorias"*, en el Expediente No. 67.068 (23.392/07).
[144] Por ejemplo, Sentencia dictada el 4 de Diciembre de 2009, por el Juzgado Federal de Primera Instancia de Santa Fe, Argentina, en el Expediente No. 86.630, autos *titulados "T.S c/ Google Argentina s/ Daños y Perjuicios*"; y Sentencia dictada el 15 de junio de 2010, por el Tribunal CNCIV Sala III, en el Expediente No. 8.805/09, autos titulados *"García Cornejo Mariquena Rosario c/ Yahoo de Argentina SRL y otros/ Medidas cautelares"*.
[145] Noticia publicada en el Diario DCI de Brasil, el día 30 de Junio de 2006, titulada: *Direito ao esquecimento gera ação contra sites de busca*, consultada en: www.dci.com.br

En este punto, en nuestro país, las consecuencias del tratamiento de los datos en Internet no se hicieron esperar. Así por ejemplo, un estudiante de la Facultad de Ingeniería de la Universidad de la República, quien había sido suspendido a consecuencia de una falta grave, solicitó que la resolución administrativa que decidía la sanción, -la que había sido impugnada y se encontraba en estudio ante el Tribunal de lo Contencioso Administrativo[146]-, fuera quitada de Internet. Pues, al escribir su nombre en el sitio Google, la primera página encontrada era la de la Universidad, conteniendo la Resolución, lo que sería determinante tanto para su posterior vida académica, como para su actividad laboral[147].

Por último, se presentaron casos en los que estos medios se utilizan para difamar o injuriar a un sujeto[148]; medios que, por la rapidez en la propagación de la información, son mucho más agraviantes que la palabra o que las tradicionales formas de comunicación; el ingreso de un dato a la web parece ser sinónimo de perpetuidad, ante la imposibilidad de ser olvidado.

B. Implicancias de las nuevas tecnologías: la vigilancia invisible

El derecho al olvido no se ve afectado, únicamente, en las hipótesis en las que intervienen redes sociales, buscadores e Internet. Existen innumerables situaciones, más cotidianas aún, en las que se extraen datos de nosotros, datos que se conservan por años, que hacen cuestionar nuestro derecho a ser olvidados.

Viajar en ómnibus, ingresar al lugar de trabajo, ir al supermercado, comprar ropa, o simplemente transitar por los lugares públicos, son acciones que años atrás pasaban completamente desapercibidas, sin ser objeto de nuestra atención. Con el advenimiento de nuevos medios tecnológicos, dichas conductas adquieren una nueva dimensión, dejando de ser intracendentes.

De esta manera, se obtienen datos de nosotros que parecen no importarnos, pero que en su conjunto permiten construir un perfil económico o social; pues, podrían deducirse estilos de vida, salud, poder adquisitivo, o hábitos de compras. ¿Cuántos datos personales están actualmente almacenados sin darnos cuenta? Los gustos, los lugares a visitar, las horas de salida, y tanta información más es obtenida de forma tan instantánea, que hasta escapa de nuestra conciencia y control.

Un ejemplo de ello son las tarjetas magnéticas utilizadas para el pago del transporte colectivo. En Montevideo, mediante el Sistema de Transporte Metropolitano, el Gobierno Departamental posee un registro nominal de los viajes que realiza una persona, al hacer uso del transporte público. Lo mismo sucede en Argentina, con el sistema denominado "Sube", o en Santiago de Chile con la "Tarjeta bip", la que va aún más allá y tiene la opción de ser bancaria, esto es, asociada a una tarjeta de crédito.

Con el uso de las mismas, y de forma inconsciente, el individuo otorga información referida a los viajes que realiza y a los lugares por los que transita. En la mayoría de los sistemas se registra únicamente el ingreso al bus o metro, pero existen otros en los que, además, se extraen datos acerca del recorrido realizado, como la Tarjeta "Metroval" de Valparaíso.

---

[146] El Tribunal de lo Contencioso Administrativo, en Uruguay, es el órgano jurisdiccional competente para entender en las acciones de nulidad, entabladas por razones de ilegalidad, de los actos dictados por la Administración.
[147] Sentencia No. 349/2005 del Tribunal de Apelaciones en lo Civil de Cuarto Turno, dictada el 30 de Noviembre de 2005, en la Ficha: 2-36518/2005.
[148] Por ejemplo, Sentencia Interlocutoria del Juzgado Letrado de Primera Instancia en lo Penal de 18º Turno No. 408/2011, dictada el 11 de Marzo de 2011.

Lo mismo ocurre con el uso de otros dispositivos, como las tarjetas de "puntos" ofrecidas por la mayoría de los supermercados, o con las tarjetas de crédito, las que dejan rastros de nuestros hábitos de compra, y, mediante ello, pueden contribuir a caracterizar nuestra personalidad.

Esta realidad se vio acrecentada considerablemente desde el uso de la radiofrecuencia para el seguimiento de bienes. El código de barras de los productos que se ofrecen en el mercado está siendo sustituido progresivamente por las llamadas "etiquetas inteligentes", dispositivos basados en la radiofrecuencia (RFID) que permiten el almacenamiento masivo de datos extraídos de la ubicación de los mismos. Mediante este sistema, *"…podría identificarse al comprador y recopilar hábitos y preferencias mientras la persona se encuentra en el establecimiento, incluido el tiempo dedicado a cada sección o el número de veces que se visita el centro comercial sin realizar ninguna compra, por ejemplo. De hecho los lectores del centro comercial podrían detectar a una persona cuando entra en el establecimiento. Ello podría activar políticas de marketing directo u otras reacciones en función de los datos vinculados a la tarjeta del cliente preferente"*[149].

¿Cómo quitar nuestros datos almacenados? La obtención y recepción de esta información derivada de nuestras acciones cotidianas, la falta de consentimiento para el almacenamiento y el diverso e inimaginable uso que se le puede otorgar a la misma, esto es, la vigilancia invisible, incide en la efectividad de los derechos en pugna. Ello hace necesario el reconocimiento del derecho al olvido y la atención por sus mecanismos de tutela, los que parecen dificultarse de forma significativa en esta nueva era digital, y que se acrecentará en los próximos años. *"De cara al futuro, no sabemos qué nuevos desarrollos nos aportará la tecnología, la informática e Internet, pero lo cierto es que los actuales desarrollos en estos terrenos nos deben prevenir ya de las amenazas que para los derechos constitucionales, y muy fundamentalmente para todos los vinculados con la privacidad suponen estos avances"*[150].

Justificación y necesidades del derecho al olvido. la diferenciación con otros derechos

A. La problemática en su vinculación con el Derecho. Los Derechos Humanos Involucrados

La protección de los datos que se ingresan en Internet, su uso, así como su eliminación, parecen ser temas que escapan a la regulación que había sido prevista en la materia. Basta recordar, en este punto, la pretensión de Carolina de Mónaco, que intentaba quitar las fotografías obtenidas con sus hijos en su esfera íntima; la que tardó casi diez años en ser amparada, llegando incluso, a la jurisdicción del Tribunal Europeo de Derechos Humanos[151].

Todo ello aparejó que organismos internacionales, como la Comisión Europea[152], cuestione la legislación existente (en su caso la Directiva 95/46/CE) aludiendo a una pérdida del control de la información individual contenida en la red, así como a los rápidos avances tecnológicos, vinculados a la globalización. Por ello, y como recomendación al Parlamento

[149] ROIG, Antoni. *Derechos Fundamentales y Tecnologías de la Información y de las comunicaciones (TICs).* Barcelona, Bosch Editor, 2010, p. 43.
[150] DIAZ REVORIO, Francisco. *Los derechos humanos ante los nuevos avances científicos y tecnológicos.* Valencia, Tirant Lo Blanch, 2009, p. 209.
[151] Sentencia del Tribunal Europeo de Derechos Humanos, dictada el 24 de Junio de 2004, en el caso *"Von Hannover c/ Alemania"*, No. 59320/2000.
[152] European Commission. Communication From The Commission to the European Parliament, The Council, The Economic and Social Committee and the Committee of the Regions. *A comprehensive approach on personal data protection in the European Union.* Brussels, 4 November, 2010.

Europeo, se propuso consagrar el *"right to be forgotten"* (derecho al olvido), definiéndolo como el derecho que posee todo individuo de que su información sea eliminada cuando ya no es necesaria para fines legítimos. Como por ejemplo, cuando es el propio sujeto el que dio su consentimiento para procesar ciertos datos, pero luego, esta difusión ya no es su deseo. Se pretende, entonces, un reconocimiento expreso por el Parlamento Europeo, que conlleve la afirmación de este derecho, propendiendo a la protección de los individuos frente a las nuevas invenciones tecnológicas.

¿Cuáles son los nuevos riesgos por los que atraviesa nuestra información? ¿Cuáles son los fundamentos de esta nueva tutela?

Conforme a un informe publicado por la ya mencionada Agencia Española de Protección de Datos[153] la intimidad de los usuarios de las redes sociales corre peligro en tres instancias. En primer lugar, a la hora de registrarse como usuario, donde se deberá configurar el nivel de privacidad que se quiere otorgar al perfil. En segundo lugar, el llamado momento de participación, en donde la publicación de datos e imágenes pueden afectar la privacidad tanto personal como de terceros. Finalmente, al tiempo de darse de baja, pues suele ocurrir que aún así los datos del usuario continúen publicados.

Otro riesgo a la privacidad señalado es el hecho de que en la gran mayoría de las redes sociales se permite a los buscadores de Internet indexar en sus búsquedas los perfiles de sus usuarios (incluyendo información personal, como, por ejemplo, la lista de amigos), lo que, a su vez, dificulta el proceso de cancelación de la información en Internet.

Por consiguiente, la piedra angular del tratamiento de datos personales es, sin lugar a dudas, el consentimiento que habilita al uso y difusión de la información aportada. Consentimiento, etimológicamente, significa acuerdo de voluntades. En tal sentido, una persona que lo brinda, estaría de acuerdo con determinada situación o con la realización de cierta actividad. El problema se plantea con las características que debe poseer dicho consentimiento, lo que implica que, para ser válido como expresión de voluntad, debe ser libre, expreso e informado.

El contrato proporcionado en la web de Facebook regula y especifica el tratamiento que este dominio realizará de los datos que brindamos. Como es sabido, esta red posee diversos niveles de privacidad, pudiendo optar, el usuario, entre compartir la información únicamente con sus amigos, o publicarla al alcance de cualquier navegador. Igualmente, ello no contempla las referencias que se extraen de forma indirecta; los llamados "metadatos", definidos como datos que proporcionan nuestros hechos, o nuestras imágenes. Así entonces, de cada acción que realizamos, o de cada información agregada, es posible obtener cierta información que podríamos denominar "oculta".

Señala el contrato de Facebook que: *"Realizamos un seguimiento de las acciones que llevas a cabo"*, *"Cuando accedes a Facebook desde un ordenador, teléfono móvil u otro dispositivo, podemos obtener información de dicho dispositivo sobre tu tipo de navegador, ubicación y dirección IP, así como las páginas que visitas"*, *"Cuando te conectes a un sitio web o una aplicación de la plataforma, nos suministrarán información, incluida la información acerca de las acciones que realizas"*, aludiendo finalmente a que: *"Podremos recopilar información acerca de ti a partir de otros usuarios de Facebook*

[153] Agencia Española de Protección de Datos e Instituto Nacional de Tecnologías de la Comunicación. *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online,* publicado en los sitios: *www.inteco.es* y *www.agpd.es*.

(como cuando un amigo te etiqueta en una foto, un video o un lugar, proporciona detalles de vuestra amistad o indica su relación contigo)"[154].

Esta realidad se agrava al considerar la problemática creada por el uso de las tarjetas de puntos, crédito o transporte, en donde, en algunos casos, ni siquiera es recabado el consentimiento del titular de los datos para su almacenamiento, o, cuando sí es obtenido, se confiere mediante contratos de adhesión, en los que la voluntad dista de ser clara y precisa. En estos supuestos, los usuarios no son informados del uso de sus datos personales, siendo total el desconocimiento de que por medio de la utilización de estos dispositivos se está recopilando información nominal. Por consiguiente, corresponde preguntarnos: ¿cómo ejercer el derecho al olvido sobre la información que ignoramos que ha sido almacenada?

A esto corresponde sumar la existencia de nuevos medios tecnológicos cada vez más invasivos, como es el sistema de reconocimiento facial lanzado por Facebook. Esta aplicación posibilita que la web etiquete fotos de individuos sin intervención de otros usuarios. La red es capaz de vincular la imagen de una persona con su nombre y cuenta de Facebook, mediante la utilización de su base de datos[155]. Todo ello, repercute enormemente en el derecho a la intimidad, así como hace necesario el reconocimiento del derecho al olvido.

Además de la intimidad, y como consecuencia de la vulneración a la privacidad, y de la imposibilidad de ejercer el derecho al olvido, muchos son los derechos humanos que pueden ser violentados. Por ejemplo, el derecho al honor implica la posibilidad de proteger la consideración que se tiene de un individuo, que será lesionado cuando se le impute algo que para éste sea indecoroso, pero que también lo sea conforme a la valoración media de la colectividad.

Asimismo, el aspecto físico constituye el primer elemento configurador de la esfera personal, por lo tanto, con arreglo a los anteriores, el individuo es titular de este derecho que consiste en la posibilidad de impedir la obtención, reproducción o publicación de su aspecto, sea cual sea la finalidad perseguida por quien difunde la imagen[156].

Adentraremos, a continuación, en el análisis del derecho a la intimidad en su vinculación específica con el tratamiento de datos personales y su diferenciación con el derecho al olvido, para estudiar luego las necesidades de éste último, y los conflictos que genera su reconocimiento.

B. El derecho a la intimidad

El derecho a la intimidad puede ser definido como el conjunto de datos y circunstancias relativas a la vida de una persona que quedan fuera del conocimiento de los demás, salvo que medie un expreso deseo de comunicarlo o ponerlo de manifiesto. Este derecho protege la obtención de los datos; el derecho al olvido cumple un rol posterior, enfocándose en la eliminación de los mismos, cuando ya se han hecho públicos, habiéndose afectado o no la intimidad.

A los efectos de la caracterización del derecho a la intimidad, se utiliza la teoría de las esferas elaborada por Hubmann en 1953. Según esta concepción, basada en círculos concéntricos, la intimidad se protege en tres ámbitos: en un ámbito mínimo del individuo a estar consigo mismo (*right to be alone*); en lo que realiza en la esfera familiar, fuera de la vista de

[154] Información proporcionada en: *www.facebook.com*
[155] MILLAN, Mark. *Facebook let users opt out of facial recognition.* Artículo publicado en CNN Tech, el 7 de Junio de 2011.
[156] v. Sentencia del Supremo Tribunal Constitucional Español No. 81/2001.

los demás; y, en tercer lugar, se tutelan aquellas situaciones que, aunque se desarrollen en lugares públicos, el individuo no tiene interés en que se propaguen[157].

Estas esferas poseen tutela, tanto en lo que respecta a las personas privadas, como a las públicas, aunque en estos últimos los límites parecen ser más flexibles, invocando el interés público y el derecho a la información. Los conflictos de derechos humanos, como analizaremos luego, se rigen por la técnica de la armonización que obliga a salvaguardar el contenido esencial de cada uno de los derechos implicados, sin preferir uno sobre otro, y a descartar la aplicación del método de la subsunción. En este marco, y con la debida ponderación, cuando se trate de un personaje público, los círculos de la intimidad podrían ser menores, aunque sin afectar lo medular de su privacidad.

Este derecho es reconocido en innumerables pactos internacionales, tales como el artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos. Este último establece que: *"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio, su correspondencia, ni de ataques ilegales a su honra y reputación"*.

En la Unión Europea, la Directiva No. 95/46/CE vincula a la intimidad específicamente con el tratamiento de datos personales. En la misma se unifica la regulación europea en la materia, atendiendo especialmente a los principios que deben sistematizar el tratamiento de datos, la recopilación y acceso a la información, estableciendo también normas sobre su seguridad y eliminación, esto último aplicable en algunos supuestos. De especial interés es el artículo 6, al disponer que los datos personales deben ser: "*e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente"*.

Estas orientaciones fueron tomadas por el derecho interno, por ejemplo, en la Ley Orgánica de Protección de Datos de Carácter Personal de España, No. 15/1999; o en la Ley Alemana sancionada el 15 de noviembre de 2006, denominada *Bundesdatenschutzgesetz*. Ello, sin perjuicio de su reconocimiento constitucional, por ejemplo, en el artículo 18 de la Constitución Española de 1978.

En esta norma, es de destacar su numeral 4, en cuanto establece que: *"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"*. Sobre él, el Tribunal Constitucional Español ha señalado que la Constitución incorporó una nueva garantía, como respuesta ante una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, fundamentalmente el honor y la intimidad, pero también un instituto que es, en sí mismo, un derecho o libertad fundamental, *"el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama «la informática»"*[158].

En Latinoamérica, este derecho está reconocido en el artículo 11 del Pacto San José de Costa Rica. La Corte Interamericana de Derechos Humanos, puntualizó que dicha norma: *"…prohíbe toda injerencia arbitraria o abusiva en la vida privada de las personas, enunciando diversos ámbitos de la misma como la vida privada de sus familias, sus domicilios o sus correspondencias"*. También señala que el artículo reconoce que toda persona tiene derecho al respeto de su honra,

[157] RISSO FERRAND, Martín. *Derecho Constitucional I*. Montevideo, FCU, 2005, p. 536.
[158] Sentencia del Supremo Tribunal Constitucional Español No. 254/1993, dictada el 20 de Julio de 1993, en el Recurso de Amparo N. 1827/1990.

prohíbe todo ataque ilegal contra la honra o reputación *"…e impone a los Estados el deber de brindar la protección de la ley contra tales ataques"*. Por último, la Corte mantuvo que el ámbito de privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros[159].

En el ámbito constitucional, este derecho se entiende consagrado en los artículos 18 y 19 de la Constitución Argentina; en el numeral 4 del Artículo 19 de la Constitución de Chile; así como en los artículos 10, 28 y 72 de la Carta Uruguaya. Asimismo, posee consagración expresa desde la reforma de 1988 en la Constitución de Brasil, en el artículo 5 numeral 10, que dispone: *"Son inviolables la intimidad, la vida privada, el honor y la imagen de las personas, asegurándose el derecho a indemnización por el daño material o moral derivado de su violación"*.

En el ordenamiento infraconstitucional, son varias las leyes que regulan el tratamiento de los datos en ficheros o bases de datos, como las ya nombradas leyes Nos. 25.326 de Argentina, 19.628 de Chile, y 18.331 de Uruguay. En estas normas, además de reconocerse y explicitarse el derecho a la intimidad, se establecen mecanismos de protección para su tutela, lo que será objeto de un análisis específico en el capítulo siguiente. Pues, como dice Bidart Campos: *"…para la eficacia, efectividad o vigencia sociológica de los derechos humanos, hacen falta las vías tutelares, a cuyo enriquecimiento está encaminado el derecho constitucional procesal"*[160].

C. La diferenciación de la intimidad con el derecho al olvido: Los nuevos Finales

La intimidad, en lo que atañe específicamente a la protección de datos, se ha relacionado con el derecho de autodeterminación informativa, el que es considerado un derecho con igual raíz[161], y que es definido, siguiendo a Herrán Ortíz[162], como la facultad de disponer sobre la revelación y utilización de los datos personales. En este sentido, se ha entendido, como un concepto básico del derecho a la intimidad, que *"el hecho de que una persona en el pasado haya divulgado datos íntimos de su vida no inhibe que sea ella la que acote el ámbito de su intimidad personal y familiar y que esto aparezca como límite infranqueable para la libre información"*[163].

Esta noción se corresponde con la jurisprudencia del Tribunal Constitucional Español, el que por Sentencia No. 115/2000[164], dispuso que si bien la demandante en su calidad de persona pública había revelado, en entrevistas anteriores, datos de su vida privada, esto no significaba que haya disminuido su esfera de privacidad, sino que la misma sigue siendo protegida en todo lo que la perjudicada no haya revelado con anterioridad.

El derecho a la intimidad protege a las distintas esferas de privacidad del individuo, impidiendo la obtención de datos, imágenes, o información de cualquier índole que pertenezca a dicho ámbito. Como producto de ello, la información no divulgada por el sujeto que afecte su intimidad, no puede ser obtenida ni difundida sin su voluntad. Por consiguiente, el consentimiento constituye el centro sobre el que gira este derecho, tal como lo sostiene el fallo citado.

---

[159] Corte Interamericana de Derechos Humanos. Caso Tristán Donoso vs. Panamá. Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia de 27 de enero de 2009, párr. 55. Caso de las Masacres de Ituango vs. Colombia. Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia del 1 de julio de 2006, párrs. 193 y 194.
[160] BIDART CAMPOS, Germán. *Teoría General de los Derechos Humanos*. Buenos Aires, Astrea, 1991, p. 29.
[161] GARECA PERALES, Pedro. *El hábeas data en la Constitución de Bolivia.* En: Anuario de Derecho Constitucional Latinoamericano, Año 11º, Tomo II, 2005, Konrad Adenauer Stiftung, p. 477.
[162] HERRÁN ORTIZ, Ana Isabel. *El derecho a la intimidad en la Nueva Ley Orgánica de Protección de Datos Personales.* Madrid, Dykinson, 2002, p. 70.
[163] RISSO FERRAND, Martín. *Algunas Reflexiones sobre los derechos al honor, a la intimidad, a la propia imagen y la libertad de prensa,* en: Anuario de Derecho Constitucional Latinoamericano, 2002, Konrad Adenauer Stiftung, p. 299.
[164] Tribunal Constitucional de España. Sentencia No. 115/2000, dictada el 5 de Mayo de 2000.

A diferencia de la intimidad, el derecho al olvido es más amplio y se utiliza en una etapa posterior, cuando los datos ya han sido revelados, voluntariamente o no, y se desea su supresión. Se agrega, entonces, en una nueva dimensión, la protección a la información que se hubiera revelado anteriormente de forma consciente, o bien se obtuvo ilegítimamente, vulnerando la intimidad, el honor, la imagen, u otro derecho fundamental.

Sin perjuicio de ello, es de destacar la vinculación que posee el derecho al olvido con la intimidad, pues la significación de estos derechos se corresponde en su finalidad, pudiendo entenderse, al primero, como una dimensión posterior del segundo, no prevista antiguamente.

Dice la Agencia Española de Protección de Datos, que: *"la informática posibilita almacenar todos los datos que se obtienen a través de las comunicaciones y acceder a ellos en apenas segundos, por distante que fuera el lugar donde transcurrieron los hechos, o remotos que fueran éstos. (…) Aún más: El conocimiento ordenado de esos datos puede dibujar un determinado perfil de la persona, o configurar una determinada reputación o fama que es, en definitiva, expresión del honor; y este perfil, sin duda, puede resultar luego valorado, favorable o desfavorablemente, para las más diversas actividades públicas o privadas, como pueden ser la obtención de un empleo, la concesión de un préstamo o la admisión en determinados colectivos"*[165].

En este punto, la legislación ha quedado disminuida ante tal realidad. La propia Directiva de la Unión Europea No. 95/46/CE previó que las ordenanzas y principios contenidos en ella, deberían luego completarse, "*…sobre todo en determinados sectores, mediante normas específicas conformes a estos principios".*

Con ello, se vislumbra allí que a pesar del marco regulatorio general, para algunas actividades, y, sobre todo, para el advenimiento de nuevas necesidades, sería necesario una regulación específica, con especiales tutelas, y aún, con la garantía de particulares derechos.

El derecho a la intimidad y, como veremos, su principal medio de tutela, el habeas data, se centran en la posibilidad que tiene el individuo de acceder, rectificar, o actualizar la información que otro sujeto conserva de sí en un banco o base de datos. Sin embargo, la protección a los datos, en lo que refiere específicamente a su eliminación, continúa, actualmente, siendo parcial.

En la nueva era tecnológica, la efectividad del derecho al olvido, supone trascender las fronteras del anterior derecho a la intimidad y de los actuales mecanismos de protección, erigiéndose como el derecho que posee todo individuo a que toda la información que se contiene sea quitada. Esto incluye tanto a los datos existentes en una base de datos, como a aquellos que se conservan en forma no sistematizada y en otros soportes, como Internet; tanto a los proporcionados de forma directa, como a los metadatos, características fotográficas, o hábitos de consumo; tanto a la información contenida en una página agregada por el propio titular, como la comentada por terceros; y tanto a los datos indexados, recogidos por los buscadores, como a los obtenidos mediante el uso de las recientes invenciones, del los cuales somos o no conscientes de su almacenamiento.

Este derecho, además, envuelve casos que bajo la perspectiva tradicional estarían por fuera del ámbito de intimidad de la persona; como son algunos datos de interés público, y la información que ha sido publicada por el mismo perjudicado. En el caso del derecho al olvido, el paso del tiempo nos impone redefinir la existencia del interés público, así como la subsistencia del consentimiento del sujeto interesado.

[165] Agencia Española de Protección de Datos. Resolución No. R/01815/2010, dictada el 20 de Setiembre de 2010, p. 11.

No obstante, ello no implica que sea un derecho absoluto, debiendo recurrir a la armonización para su conjunción con los demás derechos, como veremos en el apartado siguiente. En este punto, recordando al artículo 19 de la Ley Fundamental de Bonn, tanto el derecho al olvido como la intimidad, no podrían ser afectados en su contenido esencial, lo que parece ocurrir en la realidad actual.

Por último, el derecho al olvido implica, asimismo, la protección de los datos que, a primera vista, parecen irrelevantes, pero que en conexión con otros, unidos, pueden llegar a caracterizar al individuo. Es lo que refiere Nogueira Alcalá al mencionar la teoría del mosaico: *"al igual que ocurre con las pequeñas piedras que forman los mosaicos, que en sí no dicen nada, pero que unidas pueden formar conjuntos plenos de significado"*[166].

D. El conflicto con otros Derechos: La necesaria armonización

El reconocimiento del derecho al olvido apareja, como consecuencia, la contraposición de éste con otros derechos fundamentales. El acceso a la información, la libertad de expresión y comunicación, y la seguridad, son algunos de los derechos que, en los supuestos prácticos, se podrían ver en pugna. El derecho a la información está implícito en los diversos textos internacionales y nacionales *"como una faceta de las libertades de pensamiento, opinión y de expresión"*[167]. La libertad de expresión posee especial implicancia en nuestro Estado de Derecho, y se identifica, siguiendo al Tribunal Constitucional Español en su Sentencia No. 6/1988, con los pensamientos, ideas y opiniones, creencias o juicios de valor que se manifiesten; estando consagrado en el artículo 13 de la Convención Americana, sin perjuicio de otros textos normativos.

Un conflicto similar ocurre en el caso del derecho al olvido crediticio, donde se podría contraponer la seguridad jurídica, en el interés de conocer la lista de deudores. Otros supuestos, en los que interviene el interés público en la conservación de los datos, también pueden colisionar con este derecho. Ante estos conflictos es necesario cuestionarse: ¿Cuándo se es titular del derecho al olvido?

No se debe preferir el derecho al olvido por sobre todo otro, haciendo primar su aplicación. De lo contrario, los conflictos de derechos humanos deben ser resueltos por la técnica de la armonización, recurriendo, asimismo, a los principios de razonabilidad y proporcionalidad que se establecieron en Estados Unidos y en Alemania, respectivamente, y que son reconocidos por la comunidad occidental como garantías de los derechos humanos, siendo recibidos por nuestra Constitución de acuerdo al artículo 72[168].

Cuando nos encontramos en el conflicto entre el derecho a eliminar la información y otro derecho involucrado, como por ejemplo, el de acceso a la misma atendiendo a un interés legítimo y especialmente importante, corresponde analizar, como forma de armonización, la idoneidad, necesidad y ponderación de la medida.

Así entonces, la legislación podrá, por ejemplo, tutelar la conservación de cierta información, aún sin el consentimiento de su titular, si ésta atiende a otro derecho

[166] NOGUEIRA ALCALÁ, Humberto. *Autodeterminación informativa y hábeas data en Chile e información comparativa*. Ob. Cit., pp. 450 y 451.
[167] SHEFFER TUÑÓN, J. *Constitucionalización del derecho a la información, su acceso y tutela*. Guatemala, Konrad Adenauer Stiftung, 2007; p. 27, citado por: DURÁN MARTÍNEZ, Augusto, *Derecho a la protección de datos personales y al acceso a la información pública.* Montevideo, Editorial Amalio M. Fernández. 1ª Ed., 2009, p. 90.

[168] Este artículo establece: *"La enumeración de derechos, deberes y garantías hecha por la Constitución, no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno"*.

especialmente contemplado. Sin embargo, corresponde cuestionar, si el sacrificio del derecho al olvido es la única medida para alcanzar la tutela del otro derecho en cuestión, si se logran estos otros fines con la no supresión de la información, y, asimismo, corresponderá realizar una ponderación en sentido estricto, midiendo el grado de satisfacción del interés, su importancia, así como preferir los medios que, salvaguardando al otro derecho, incidan de menor forma en la tutela del derecho al olvido.

Por ejemplo, si en el caso de las tarjetas de transporte se conserva la información para optimizar el servicio, se pude llegar al mismo resultado utilizando tarjetas que no sean nominales. Si, de lo contrario, se comprobare que no existe otro medio menos lesivo para el derecho, se deberá proceder a la ponderación o armonización de los intereses, como podría ser almacenar la información, pero por un período determinado de tiempo, previamente establecido por ley, o restringir el acceso a la misma a aquellos sujetos que tengan un verdadero interés legítimo.

Por último, corresponde profundizar, como lo hace Alexy[169], en que el contenido esencial del derecho no debe ser afectado, siendo éste el límite para su desnaturalización. El contenido esencial se manifiesta como el último ámbito intangible que caracteriza al derecho, el cual, acorde con la jurisprudencia del Tribunal Constitucional Alemán, no puede ser vulnerado.

LA CARACTERIZACIÓN CONCEPTUAL Y SU INCIPIENTE RECONOCIMIENTO

El derecho al olvido, como ya estudiamos al analizar sus antecedentes, si bien había sido contemplado en el ámbito de las bases de datos crediticias y penales, adquiere singular importancia para resguardar los derechos de los usuarios en la llamada era 2.0. Pues, como dice la varias veces citada Agencia Española de Protección de datos: *"El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y acceso a los mismos ha expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida"*[170].

El autor argentino Palazzi, fundó el derecho al olvido, aún antes de que sea reconocido jurisprudencialmente, en varias premisas. En primer lugar, en que toda persona tiene derecho a rearmar su vida incluso aunque haya cometido errores. En segunda parte, que el dato en cuestión, cuando era muy antiguo, ya no cumplía la finalidad para la cual había sido recopilado. Por último, se fundamenta en que el derecho a la privacidad de las personas también incluye ciertos hechos pasados[171].

Por tanto, la principal finalidad del derecho al olvido es brindar la posibilidad, al sujeto, de rearmar y reorganizar su vida, incluso cuando en el pasado haya realizado alguna conducta éticamente cuestionable o ilegal.

Este derecho ha sido reconocido judicial, y, aún, en algunos supuestos, normativamente, como un derecho a que datos actuales y pasados de una persona, considerados lesivos, sean eliminados. La nueva realidad plantea la necesidad de ampliar el contenido de la intimidad y reconocer este derecho al olvido, para que pueda tutelar el nuevo escenario tecnológico.

[169] ALEXY, Robert. *Teoría de los Derechos Fundamentales*. Madrid, Centro de Estudios Constitucionales, 1993, p. 286.
[170] Agencia Española de Protección de Datos. Resolución No. R/01815/2010, dictada el 20 de Setiembre de 2010, p. 11.
[171] PALAZZI, Pablo. *Informes Comerciales.* Buenos Aires, Ed. Astrea, 2007.

Su antecedente más remoto puede ubicarse en Estados Unidos, en el leading case, Melvin v. Reid del año 1931. En el mismo, una actriz que había sufrido acusaciones de prostitución y tentativas de homicidio, accionó contra una película que siete años después de su absolución narraba su verdadera historia utilizando su nombre original, revelando su pasado, luego de haber logrado superar esta situación. Acorde a lo anteriormente expuesto, el Tribunal concluyó que "el uso y difusión de un dato verdadero puede ser violatorio de la intimidad y reserva de un individuo cuando este tiene cierta antigüedad" [172].

El derecho al olvido viene a reconocer, entonces, que el paso del tiempo impone una nueva valoración del consentimiento, así como una nueva consideración del interés público. Cuando el consentimiento ha desaparecido, resulta abusivo y hasta injusto seguir proporcionando información del individuo.

En este sentido, se ha pronunciado en Italia el Tribunal de Roma, considerando inexistente toda finalidad informativa calificable como esencial al interés de la colectividad, en la publicación del nombre u otros datos identificatorios de personas involucradas, o consideradas involucradas, en procesos judiciales que forman parte del pasado[173].

El Tribunal Constitucional Español, por su parte, expresó que la protección de datos implica el poder de disposición y control sobre los mismos, lo que se concreta jurídicamente en la facultad de decidir cuáles datos proporcionar, cuáles pueden ser recabados de su persona, "…y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso"[174]. Se visualiza aquí la existencia del derecho al olvido como una especial facultad que posee todo individuo, como titular de datos obtenidos de cualquier forma, y se diferencia de la intimidad.

En otro orden, la Agencia Española de Protección de Datos ha entendido al derecho al olvido inserto en la regulación de la Ley de Servicios de Sociedad de la Información, No. 34/2002, al comprender a Google dentro de estos entes prestadores de servicios. En este caso, el artículo 8 de dicha norma, entiende que en el supuesto que determinado servicio atente o pueda atentar contra el principio de respeto a la dignidad de la persona o de no discriminación, los órganos competentes para su protección podrán adoptar las medidas necesarias para que se interrumpa su prestación o para retirar los datos que los vulneran. Con este marco, dicha Agencia ha entendido que los buscadores o redes sociales deben realizar las gestiones necesarias para retirar los datos o vedar el acceso a los mismos, cuando así les sea requerido[175].

En Argentina, por otra parte, y mediante el acogimiento de medidas cautelares, los tribunales han sido contestes en afirmar que la existencia de información dañosa para el sujeto, hace responsable al buscador por la facilitación del acceso a los datos, por lo que cabe ordenar su eliminación[176]. Asimismo, y demostrando la falta de regulación específica, también se mencionan otras normas, como la Convención Internacional sobre la Eliminación de Todas las Formas de Discriminación Racial, para justificar la intervención inmediata de los Estados en la eliminación de toda incitación a la discriminación: "…prima facie, la facilitación por la

[172] PALAZZI, Pablo. Ob. Cit., p. 156.
[173] Tribunal de Roma, Sentencia del 20 de Noviembre de 1996, citada por: RUFFINI GANDOLFI, María Leticia. *Divulgación de hechos privados y responsabilidad de los medios masivos de comunicación*, en: Estudios Jurídicos Nº 6. Facultad de Derecho Universidad Católica del Uruguay, 2006, p. 255.
[174] Sentencia del Supremo Tribunal Constitucional Español No. 292/2000, dictada el 30 de Noviembre del 2000.
[175] Agencia Española de Protección de Datos. Resoluciones Nos. R/00668/2011 del 7 de Abril de 2011 y R/00508/2011 del 16 de Marzo de 2011.
[176] Sentencia dictada el 4 de Diciembre de 2009, por el Juzgado Federal de Primera Instancia de Santa Fe, Argentina, en el Expediente No. 86.630, autos *titulados "T.S c/ Google Argentina s/ Daños y Perjuicios*"

demandada de enlaces a contenidos existentes en páginas de Internet y/o inclusión en los suyos de directorios o instrumentos de búsqueda de contenidos (…) podrían enmarcarse o tipificarse como actos discriminatorios", por lo que se resuelve ordenar su eliminación[177].

La legislación actual reconoce al olvido de forma parcial. Las nuevas tecnologías, que permiten la recopilación de información derivada de nuestros actos cotidianos escapan a esta regulación. Son varias las limitaciones que se disponen amparando la no eliminación de la información. Señala Herrán Ortiz que contrariamente a lo que pudiera pensarse, no se le reconoce al interesado un derecho de oposición con carácter general en la Directiva 95/46/CE de la Unión Europea[178]. Lo mismo ocurre, en Latinoamérica, con las fórmulas más o menos amplias que han adoptado los Estados en su legislación interna.

En Uruguay, por ejemplo, por aplicación de la ley 18.331, únicamente se obliga a los responsables de las bases de datos a eliminar la información personal en aquellos casos de: a) perjuicios a los derechos e intereses legítimos de terceros; b) notorio error o falsedad y c) contravención a lo establecido por una obligación legal. Como es de ver, más allá de la amplitud que pueda tener la tercera causal, la taxatividad de las mismas conspira contra la posibilidad de ejercer el derecho al olvido en su plenitud, con la amplitud señalada en este trabajo.

Sin embargo, dadas los mayores requerimientos en la protección, son varios los proyectos que prevén la consagración expresa de este derecho. Como ya adelantamos, en una reciente comunicación de la Comisión Europea se plantea la necesidad de clarificar y reconocer el derecho al olvido[179].

Asimismo, este tema también ha sido planteado particularmente en Francia y en Italia. En el primero de estos países, el derecho al olvido o *"droit à l`oubli"* fue implícitamente reconocido, en diversas leyes, como la No. 78-17 del 6 de Enero de 1978. Luego, el artículo 5 de la Ley No. 2004-801, del 6 de Agosto de 2004, introdujo específicamente el derecho de oposición. A su vez, dada la problemática actual, el 6 de Noviembre de 2009, los Senadores Détraigne y Escoffier presentaron un proyecto de ley cuyo artículo 6 contempla especialmente el derecho al olvido en lo concerniente a la protección de datos.

En Italia, por su parte, el *"diritto all`oblio"* se consagró en los artículos 7 y 11 del Código de Protección de los Datos Personales (Ley No. 196/2003), así como había sido nombrado anteriormente en fallos jurisprudenciales, como el No. 5259 de 1984 de la Corte Suprema. El 20 de Mayo de 2009 ingresó al Parlamento la propuesta de ley No. 2455, que consagra el derecho al olvido en Internet para las personas que están sujetas a investigación o han tenido acusación en un juicio penal.

En Argentina, asimismo, se está desarrollando un proyecto de ley que garantiza el derecho al olvido en la web, el cual fue iniciado el 22 de febrero de 2011, en el trámite No. 208. Éste dispone en su Artículo 3 que toda persona podrá promover una medida ante el juez con competencia en su domicilio con el objeto de "solicitar judicialmente que se elimine y/o se restrinja y/o se bloquee el acceso a uno o más contenidos específicos -sea en forma de texto, sonido, imagen o cualquier otra información o representación- que lesionen derechos o garantías reconocidos por la Constitución Nacional, un tratado o una ley…".

---

[177] Sentencia del Juzgado Nacional en lo Civil No. 46 de Argentina, dictada el 16 de Mayo de 2011, en la Causa *"Delegación de Asociaciones Israelitas Argentinas c/ Google Inc s/ medidas cautelares"* Expediente No. 34023/2011.
[178] HERÁN ORTÍZ, Ana. Ob. Cit., p. 159.
[179] European Commission. Communication From The Commission to the European Parliament…. Ob. Cit. Brussels, 4 November, 2010.

Este incipiente reconocimiento, aunque pretende ser un gran avance, continúa siendo parcial, escapando a la totalidad de la problemática actual, dejando de lado, por ejemplo, la tutela del derecho en lo que respecta al almacenamiento de información a partir de nuestras acciones más cotidianas. En el caso Uruguayo, como vimos, aún no se ha planteado, en el ámbito parlamentario, el reconocimiento desde el punto de vista genérico. Sin embargo, por el aumento de casos administrativos y jurisprudenciales en la materia, así como por la preocupación existente en el derecho comparado, estimamos que se prestará especial importancia a esta área, no demorando en demasía su reconocimiento.

Las garantías: de los viejos recuerdos al olvido. una aproximación al caso uruguayo

Como ya hemos analizado, el reconocimiento de los derechos no asegura su completa eficiencia, sino con el establecimiento de verdaderas garantías para su tutela. En este sentido, sostiene la doctrina que no basta con que los derechos sean incorporados en la legislación, sino que también se hace necesario configurar un sistema complejo de protección de las personas, que permitan tutelar la efectividad de su cumplimiento[180].

A. La tutela mediante la acción de Habeas Data. Su insuficiencia.

Como mecanismo de protección del derecho a la intimidad, ha surgido el recurso de habeas data. Señala el autor chileno ya citado Nogueira Alcalá que: "La expresión habeas data literalmente significa "tengas los datos" y su objeto es asegurar el acceso a la información que de la persona afectada tengan registro o bancos de datos públicos o privados, con el objeto de proteger la vida privada, intimidad, imagen, buena reputación u honra de las personas"[181].

Este término fue utilizado, primeramente, por el artículo 35 de la Constitución Portuguesa de 1976, incorporándose, en Latinoamérica, a la Constitución de Brasil, del año 1988, en su artículo 5. Esta norma, en su numeral 71 establece: "Se concede hábeas data: a) para asegurar el conocimiento de informaciones relativas a la persona del solicitante contenida en registros o bancos de datos, de entidades gubernamentales o de carácter público; b) para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto o de carácter judicial o administrativo".

Luego de ello, el habeas data adquirió carácter constitucional en diversas Cartas, como la Colombiana de 1991 (artículo 15), Paraguaya de 1992 (artículo 135), Peruana de 1993 (artículo 2), Ecuatoriana de 1996 (artículo 94), Venezolana de 1999 (artículo 28), y Boliviana en 2004 (artículo 23).

En Argentina, Bidart Campos expresa que el artículo 43 de la Constitución amplió el ámbito de tutela de este mecanismo, abarcando la protección de todos los derechos que se vulneren mediante el uso de datos contenidos en un registro[182]. Además, la Ley Argentina de Protección de Datos, No. 25.326, establece los principios sobre los que se deben asentar las bases de datos, sean manuales como informatizadas, reconociendo el derecho al acceso y corrección.

---

[180] ARRIETA, Raúl; ORTIZ, Claudio y otros. *Chile y la protección de datos personales. ¿Están en crisis nuestros derechos fundamentales?* Chile, Universidad Diego Portales, 2009, p. 17.
[181] NOGUEIRA ALCALÁ, Humberto. *Autodeterminación informativa y hábeas data en Chile e información comparativa*, en: Anuario de Derecho Constitucional Latinoamericano, 11º Año, Tomo II. Konrad Adenauer Stiftung, 2005, p. 458
[182] BIDART CAMPOS, Germán. *Tratado elemental de derecho constitucional.* Buenos Aires, Ediar, 1994.

Particularmente en Uruguay, esta garantía se entiende prevista en el artículo 72 de la Constitución, así como contemplada especialmente por la Ley 18.331 de Protección de Datos Personales.

Según Dromi y Menem[183], esta acción persigue cinco objetivos básicos: 1) Que una persona pueda acceder a la información que sobre ella conste en un registro o banco de datos; 2) que se pueda exigir que se actualicen datos atrasados; 3) que se rectifiquen los datos inexactos; y 4) que se borre del registro la información que se pueda considerar sensible.

En este marco, le otorga a toda persona física o jurídica el derecho para solicitar, a los responsables de bases de datos, la rectificación, actualización, inclusión o supresión de los datos personales incluidos en las mismas. Éstos tendrán un plazo máximo de cinco días hábiles para actuar en consecuencia o para informar las razones por las que estime que no corresponde. Dicho procedimiento será un requisito de admisibilidad, para que, en el caso de incumplimiento, el titular del dato pueda promover la acción de hábeas data.

Sin embargo, dicha acción resulta insuficiente para contemplar la problemática actual. Como vimos, únicamente se obliga a los responsables a eliminar la información cuando hubiere perjuicios a los derechos e intereses de terceros, notorio error o falsedad, o contravención a lo establecido por una obligación legal.

Tampoco en Chile la acción posee previsión constitucional expresa, encontrándose contemplada en la Ley No. 19.628; y también allí el amparo del derecho al olvido se contempla únicamente de forma parcial. En efecto, el artículo 12 prevé la posibilidad de exigir la eliminación de los datos, cuando su almacenamiento carezca de fundamento legal o cuando éstos hubieren caducado. Asimismo, y, con mayor alcance que la Ley Uruguaya, establece que: "Igual exigencia de eliminación, o la de bloqueo de los datos, en su caso, podrá hacer cuando haya proporcionado voluntariamente sus datos personales o ellos se usen para comunicaciones comerciales y no desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal".

La acción de habeas data se presenta, entonces, como la tutela que efectivizará este derecho de forma parcial, únicamente cuando se trate de eliminar la información contenida en una base de datos, y cuando además, se cumplan con los especiales requisitos exigidos por la legislación de cada Estado.

B. Otras vías jurisdiccionales de protección

Actualmente, se hace necesario abarcar no sólo aquella dimensión del derecho al olvido que esté amparada por el habeas data, sino también la información o datos que se encuentran almacenadas en otros soportes, los metadatos y características fotográficas, la información extraída del uso de tarjetas personales, la contenida en una página agregada por el propio titular, la comentada por terceros, entre otros supuestos no contemplados por este mecanismo de tutela.

Como acciones alternativas al habeas data, se presentaron, en la práctica, la solicitud de eliminación de la información mediante una medida cautelar, en Argentina y Uruguay, así como la acción de amparo.

[183] DROMI, José Roberto y MENEM, Eduardo. *La Constitución Reformada: Comentada, Interpretada y Concordada.* Buenos Aires, Ediciones ciudad Argentina, 1994, p.169. Cf. LAMAS, Mario Daniel. *Estudio sobre el nombre, la imagen, la intimidad, la identidad, el honor y la reputación como derechos personales y como derechos patrimoniales.* Montevideo, CIKATO, 2004, p.288.

La medida cautelar no es, como ya lo establece su nombre, una medida autosatisfactiva, por lo que, en estos casos, la cancelación de los datos siempre quedará sujeta a un procedimiento posterior, que asegure el derecho del individuo, así como la responsabilidad del demandado. Por otra parte, se erigen como condiciones de procedibilidad para la efectividad del derecho al olvido los requisitos propios de las medidas cautelares, como la verosimilitud del derecho o el peligro en la demora. Ello, sin dudas, apareja graves consecuencias a la hora del ejercicio del derecho al olvido.

La acción de amparo en Uruguay, como veremos, posee consagración Constitucional implícita en los artículos 7 y 72, y está reglamentada por la Ley 16.011, dictada el 19 de Diciembre de 1988. Según ésta, para que el amparo pueda ser promovido se exige: a) un acto, hecho u omisión; b) que lesione, restrinja, altere o amenace un derecho o libertad; c) provocando al titular del derecho o libertad un daño irreparable; d) que ese derecho esté reconocido expresa o implícitamente por la Constitución; e) que exista manifiesta ilegitimidad; y f) que no se encuentren en el ordenamiento jurídico otros medios judiciales o administrativos que permitan obtener el mismo resultado.

La configuración de estos requisitos es analizada, por la jurisprudencia, de forma estricta, siendo dificultosa la obtención de un resultado favorable. Por ejemplo, en la Sentencia No. 349/2005, del Tribunal de Apelaciones en lo Civil de Cuarto Turno, se desestimó la demanda de amparo, que pretendía la cancelación de los datos contenidos en una página web, por entender que no se presentaban todos los elementos de la figura legal. Dice el Tribunal que en el caso no se configura el requisito de ilegitimidad manifiesta, debido a la objetividad y generalidad con que fue publicada la información, esto es, sin otra finalidad ostensible; *"…pues, la ilegitimidad debe ser clara, evidente, inequívoca, grosera…".*

Otra gran dificultad que advertimos para poder hacer plenamente efectivo este derecho, lo constituye el hecho de que muchas veces se desconoce al sujeto responsable del soporte en donde se encuentra la información que se quiere suprimir; o, en su caso, la ausencia de un lugar físico en nuestro país, en donde se asiente la empresa multinacional, a los efectos de llevar a cabo las notificaciones o emplazamientos correspondientes.

Las garantías de los derechos humanos, hoy en día, no son solo internas, sino también internacionales, debido a la protección que de ellos realizan la Corte Europea de Derechos Humanos, y la Corte Interamericana de Derechos Humanos. En este punto, la labor de estos organismos resulta fundamental, tanto en lo que refiere a la efectividad del derecho en los casos jurisdiccionales, como a los estudios y recomendaciones que pudieren realizar en la materia para su reconocimiento. Se hace necesario, entonces, una mayor regulación y control, a nivel no sólo nacional, sino también internacional. Si bien las garantías son de extrema utilidad para tutelar los derechos, como bien dice Ferrajoli[184], éstas no son de esencia de los derechos fundamentales, en el sentido de que no por ello debemos dejar de reconocer la existencia de un verdadero derecho al olvido.

C. El control administrativo y la labor de los obligados

Para salvaguardar la libertad del hombre es necesario que se aseguren garantías suficientes para el respeto a los derechos inherentes a todos los individuos, sean éstas jurisdiccionales o administrativas. Para lograr esta finalidad es pertinente la actividad del

[184] FERRAJOLI, Luigi. *Los fundamentos de los derechos fundamentales.* Editorial Trotta. Madrid. 2005.

Estado, que es el único ente capaz de controlar la labor de los particulares, a efectos de proteger a las personas de posibles violaciones a sus derechos, y particularmente en nuestro caso, proteger a los sujetos en su derecho al olvido. En este marco, la intervención del Estado debe estar sujeta al principio de subsidiariedad, desarrollado por la doctrina social de la Iglesia Católica, particularmente en la Encíclica Cuadragésimo Anno, de Pio XI. La actuación estatal, por tanto, debe estar ceñida de eficiencia y eficacia, realizando "…todo aquello que es de su exclusiva competencia, en cuanto que sólo él puede realizar, dirigiendo, vigilando, urgiendo y castigando, según el caso requiera y la necesidad exija"[185].

La Directiva de la Unión Europea, No. 95/46/CE, previó en su Capítulo VI, la existencia de Autoridades de Control, a los efectos de vigilar la aplicación en su territorio de las disposiciones adoptadas internamente. Estas autoridades fueron instituidas en los países Europeos, creándose, en el marco de esta Directiva, Agencias con total independencia, dotadas de poderes de investigación, de intervención, de asesoramiento, con capacidad procesal, y sujetas al control jurisdiccional.

Aparecieron, por ejemplo, la *Commission Nationale de l`informatique et des Libertés* de Francia, la *Dutch Data Protection Authority* de Holanda, y la *Comissào Nacinal* de Potecçào *de Datos informatizados* de Portugal, entre otros.

En España, la ya varias veces nombrada Agencia Española de Protección de Datos, fue creada por la Ley 15/1999, como un ente de Derecho Público, con personalidad jurídica propia y plena capacidad. Sus funciones se basan en el control del cumplimiento de la legislación sobre protección de datos, particularmente en lo referido a los derechos de información, acceso, rectificación, oposición y cancelación de los mismos. La actuación de esta Agencia ha sido constante en lo que respecta específicamente al tratamiento de la información, recibiendo y procesando las denuncias de los usuarios y dictando resoluciones y recomendaciones al efecto, muchas de las cuales fueron citadas en este trabajo.

Por otra parte, no sólo cumple una labor esencial en los litigios sobre casos de lesión al derecho al olvido, sino que, además, ha elaborado una Declaración sobre Buscadores de Internet[186], en la cual se consideró que los buscadores tratan información que, según la Ley Orgánica de Protección de Datos, tienen la consideración de datos personales y, además, como ya dijimos, son servicios regulados en la Ley de Servicios de la Sociedad de la Información. En consecuencia, se dispuso que "(…) tales tratamientos de información deben cumplir con el sistema de garantías que ambas normas establecen en beneficio de los ciudadanos y de los destinatarios de servicios de la Sociedad de Información". En el marco de esta Declaración, la Agencia Española ha iniciado diálogos con entidades como Google, a fin de garantizar los derechos en materia de privacidad de los usuarios, procurando que el buscador se ajuste a la normativa española sobre protección de datos[187].

Es de destacar que, para su actuación, posee completa independencia de la administración pública. Esta independencia también se constata en la mayoría de los órganos reguladores, pertenecientes a otros países, como el Instituto Federal de Acceso a la Información Pública y Protección de Datos de México. Sin embargo, concentrándonos en el caso Uruguayo, la Unidad Reguladora y de Control de Datos Personales (en adelante URCDP) no posee tal

[185] Carta Encíclica Cuadragésimo Anno de su Santidad Pío XI, Roma, 15 de Mayo de 1931.
[186] Agencia Española de Protección de Datos. Declaración sobre buscadores de Internet, dictada el 1 de diciembre de 2007.
[187] Agencia Española de Protección de Datos. Nota informativa – Google asegura a la AEPD que la información facilitada a los usuarios puede y va a ser mejorada, dictada el 23 de Abril de 2010.

autonomía. La Ley 18.331 la crea como un órgano desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), esta última, integrante del sistema centralizado, y por tanto, sujeta a jerarquía de Presidencia de la República.

Por consiguiente, entendemos necesaria, a los efectos de la eficiencia en su actuación, que se prevea la autonomía de esta Unidad y su neutralidad, lo que se traduce en una independencia orgánica y funcional de la Administración. Sin embargo, y a pesar de las falencias en la naturaleza, señala el actual integrante de su Comité Ejecutivo, Felipe Rotondo[188], que la Unidad posee atribuciones propias, actuando en ellas con discrecionalidad, no recibiendo, en los hechos, órdenes ni instrucciones para el ejercicio de sus actividades.

Al analizar la actividad realizada hasta la fecha por la URCDP, podemos identificar casos en los cuales la misma ha manifestado su preocupación por la tutela del derecho al olvido. En este sentido, mediante un informe elaborado en el año 2010, se estudió el sistema de publicación en Internet de deudores del Banco Central del Uruguay[189], manifestando su desaprobación. De este modo, se alega que el mismo incumple el artículo 22 de la Ley 18.331, denunciando que el sistema permite extraer datos personales no solamente actuales, sino también históricos.

Por otra parte, en un dictamen referente a un Proyecto de modificación del Artículo 22 de la ley 18.331[190], la URCDP manifestó su concordancia en lo que hace a la eliminación de los datos del deudor una vez que salde su deuda. En este sentido, se expresa que la anotación o continuidad en un registro de aquél sujeto que finalmente saldó una deuda, "*termina siendo habitualmente perniciosa por más que se haga constar su calidad de cumplidor*", aplicándose, entonces, con el derecho al olvido.

La tutela administrativa de los derechos de los usuarios, como vía alternativa, previa, y muchas veces, preferente a la jurisdiccional, se presenta como una posibilidad que sería altamente satisfactoria, al ser, la labor de esta Unidad, significativamente positiva. Las consecuencias del tratamiento de nuestros datos, con las nuevas tecnologías, pueden ser sumamente lesivas, por lo tanto, en este punto, la promoción, publicidad y conocimiento del ente, así como la confianza que la sociedad le brinde, resulta fundamental para la eficiencia de su labor, concordante con el principio de subsidiariedad enunciado. Asimismo, esta Unidad posee especial importancia en lo que respecta a la tutela del derecho al olvido cuando el interesado desconoce el otorgamiento de los datos derivado de nuestras acciones más cotidianas, así como el uso y almacenamiento de los mismos, a través de los nuevos dispositivos tecnológicos.

Por consiguiente, y en lo que respecta a nuestra materia, sería necesario que la URCDP sea mayormente promocionada, por ejemplo, en lo que hace a la tutela del los derechos de los usuarios y a la posibilidad de instaurar denuncias. Asimismo, sería altamente satisfactorio que esta Unidad busque alentar a los responsables para que se ajusten a la normativa interna referente a la protección de datos.

La primera esfera de tutela del derecho al olvido se encuentra en el completo cumplimiento de la normativa por parte de los obligados. En este punto, los responsables de las bases de datos, así como de los diversos dominios de las páginas webs y buscadores deberían

[188] ROTONDO, Felipe. *Red Iberoamericana de Protección de datos*, consultado en: *www.redipd.org*
[189] Unidad Reguladora y de Control de Datos Personales, Informe No. 1533, dictado el 3 de Junio de 2010.
[190] Unidad Reguladora y de Control de Datos Personales, Informe No. 2540, dictado el 20 de Agosto de 2010.

atender a la normativa existente, así como a las especificaciones que vendrán en atención al avance tecnológico, de forma de verter especial atención a la salvaguarda de los derechos involucrados. La política de privacidad, las condiciones de contratación y el consentimiento deben ser el centro de esta actividad, correspondiendo, al responsable del tratamiento de los datos, comprometerse estrechamente con la efectividad del derecho al olvido. Como dice el Papa Benedicto XVI: *"El mero hecho de que los medios de comunicación social multipliquen las posibilidades de interconexión y de circulación de ideas, no favorece la libertad ni globaliza el desarrollo y la democracia para todos. Para alcanzar estos objetivos se necesita que los medios de comunicación estén centrados en la promoción de la dignidad de las personas y de los pueblos…"*[191]

Hemos constatado que, en nuestro país, varios servicios no se adecuan a la normativa vigente. A modo de ejemplo, el artículo 6 del Decreto 414/009 referido a las formas de recabar el consentimiento, dispone que deberá facilitarse al titular un medio "(…) *sencillo, claro y gratuito para que manifieste su consentimiento o su negativa al tratamiento de sus datos. Se entenderá cumplido tal deber cuando se permita al titular la elección entre dos opciones claramente identificadas, que no se encuentren premarcadas a favor o en contra*". Además, agrega que vencido el plazo de diez días hábiles desde que el titular de los datos reciba la solicitud de consentimiento sin que se manifieste, su silencio equivaldrá a una negativa.

Si bien las normas del Decreto son específicas acerca del modo en que el titular de los datos debe otorgar su consentimiento para la recolección y tratamiento de la información que le concierne, encontramos que en redes sociales, como Facebook, al iniciar una cuenta, no se informa adecuadamente el tratamiento que se le dará a los datos ingresados en la red. Como éste, existen muchas otras páginas, de dominio internacional y aún nacional, cuyas condiciones no se adecuan con la normativa existente. Ello no solo ocurre en Internet, sino, con mayor intensidad, en lo que respecta a las bases de datos creadas por el uso de diversas tarjetas y promociones.

En este marco, la labor de los Entes a nivel internacional, y de la URCDP en el Uruguay, resulta fundamental, tanto en lo que respecta a la tutela y al amparo del derecho a la intimidad, protección de datos y del derecho al olvido, como a lo que hace al cumplimiento de la normativa aplicable en la materia, en su labor de prevención, lo que concluirá en la efectividad de la intervención y control administrativo propuesto, y que implicará la consecuente protección de los derechos individuales en pugna.

D. La Efectividad del Olvido: los Nuevos Finales puestos en Práctica

Analizamos en el Capítulo II de este trabajo, diversos ejemplos en los que eliminar los viejos recuerdos constituye un deseo de los sujetos, lo que, luego del estudio realizado, se traduce en un derecho: el derecho al olvido. Habiendo concluido que tenemos un derecho al olvido, corresponde cuestionarnos ahora, desde el punto de vista práctico: ¿Cómo lo hacemos efectivo?

Para ello, nos limitaremos al análisis de la realidad uruguaya, habiendo ya citado la normativa aplicable, el estado del reconocimiento de este derecho en nuestro país, así como los medios existentes para su tutela.

¿Cómo eliminar la información que Internet u otra base de datos posee de nosotros? ¿Cómo se tutela este derecho en la práctica?

[191] Carta Encíclica Caritas in Veritate del Sumo Pontífice Benedicto XVI, Roma, 29 de Junio de 2009.

Como vimos, la primera esfera de acción se encuentra en el cumplimiento de la normativa por parte del obligado. La regulación actual no le impone a éste el deber directo de eliminar los datos contenidos en su base o soporte cuando sea solicitado por el titular, sino en algunos supuestos. Para los no contemplados expresamente, -entre los que se incluyen la mayoría de los implicados en la realidad actual analizada-, corresponde cuestionarnos sobre su existencia en nuestro derecho; esto es, si el sujeto posee un derecho a ser olvidado, aún cuando éste no está reconocido explícitamente por la regulación.

Partiendo de la inclinación iusnaturalista de nuestra Constitución, entendemos al derecho al olvido reconocido implícitamente en las previsiones del artículo 72 de este cuerpo normativo, el cual incluye, en su enumeración de derechos, a todos aquellos que derivan de la personalidad humana o de la forma republicana de gobierno. Con base en el principio de dignidad humana, y teniendo en cuenta su vinculación con la intimidad y la nueva dimensión de su contenido, el derecho al olvido deriva de la propia naturaleza humana, y, por consiguiente debe ser respetado por todos los sujetos intervinientes. Ante su incumplimiento, corresponde que las garantías de los derechos humanos tengan completa efectividad práctica, de forma de tutelar los intereses de los titulares de la información que se desea eliminar.

No obstante, en lo que refiere al ordenamiento infraconstitucional, y como adelantábamos, la salvaguarda de este derecho es parcial. Es este un caso de vacío normativo, ante el cual debemos recurrir a las técnicas de la integración. En éstas, la aplicación de las normas de fundamento análogo, de los principios generales del derecho y de las doctrinas generalmente admitidas, se hace necesaria, partiendo de un análisis desde la Constitución Uruguaya, en su artículo 332.

En este punto, la regulación existente en la Ley 18.331, el desarrollo doctrinario, y, fundamentalmente, el principio de dignidad de la persona humana adquieren especial atención. Como señala Bidart Campos, los derechos humanos parten de un nivel por debajo del cual carecen de sentido: el reconocimiento de que en el ser humano hay una dignidad que debe ser respetada cualquiera sea el ordenamiento jurídico[192]. Por consiguiente, por medio de la integración amparamos, con el derecho al olvido, la realidad actual, no contemplada por nuestro ordenamiento, concluyendo en la obligación de los responsables de las bases de datos de eliminar los datos que poseen sin un interés legítimo establecido legalmente, sin consentimiento del titular, y que vulneren su intimidad, honor, imagen, seguridad o algún otro derecho inherente a su personalidad.

En un primer nivel, la actuación de la Unidad Reguladora, si bien podría controlar la conducta del obligado e imponerle sanciones al respecto, no podría exigirle directamente la eliminación de la información. En efecto, la Ley 18.331 le impone el deber de fiscalizar el tratamiento de los datos personales, pero no le da potestades que permitan exigirle al responsable la supresión de la información cuando ésta no resulte acorde a la normativa, lo que entonces, no está dentro de sus competencias, conforme al principio de especialidad en materia administrativa.

La vía jurisdiccional aparece, actualmente, en nuestro país, como el medio de tutela del derecho al olvido. A diferencia de lo que sucede con los otros poderes del Estado, y de lo que ocurría en la antigua Roma con el *non liquet*, el Juez no puede excusarse en el desarrollo de su actividad jurisdiccional y no fallar. Sin embargo, suele ocurrir, como ya estudiamos, que la

[192] BIDART CAMPOS, Germán. Teo*ría general de los derechos humanos*. Buenos Aires, Astrea, 1991, p. 73.

normativa actualmente vigente se erige como una barrera que impide la efectividad del derecho en cuestión. Así entonces, y ante la inexistencia de otros medios, el amparo aparece como la única vía procesal para la tutela del derecho al olvido. No obstante, las posibilidades de obtener una sentencia favorable en este ámbito son escasas.

En nuestro país, como adelantábamos, coexisten dos acciones de amparo: a) la constitucional, cuyo fundamento puede ser encontrado en el artículo 7 que consagra el derecho de todo habitante a ser protegido en el goce de su vida, honor, libertad, seguridad, trabajo y propiedad; en el artículo 72 de la Constitución; o en ambos[193]; y b) la legal, la cual está regulada por la Ley 16.011 ya citada.

Por otra parte, la acción de amparo como mecanismo de tutela se ubica, en los artículos 8 y 25 de la Convención Americana de Derechos Humanos, suscripta por Uruguay en 1985 (Ley 15.737). Decía Gros Espiell que: *"…incluso sólo como consecuencia de la aplicación directa en el Derecho Interno del Derecho Internacional vigente, es indiscutible que el "amparo" a que se refiere el artículo 25 del Pacto de San José, se integra en el Derecho nacional y se suma, formando una unidad, con lo dispuesto por la ley Nº 16.011 del 19 de diciembre de 1988"*[194].

En lo que refiere a las tutelas de la Convención, la Corte Interamericana de Derechos Humanos ha explicitado que no pueden vulnerarse ni siquiera en estados de emergencia[195], que el artículo 25.1 de la Convención obliga a los Estados a ofrecer a todas las personas sometidas a su jurisdicción un recurso judicial efectivo contra actos violatorios de sus derechos fundamentales, puntualizando que: "…no basta que los recursos existan formalmente, sino que los mismos deben dar resultados o respuestas a las violaciones de derechos humanos, para que éstos puedan ser considerados efectivos. Es decir, toda persona debe tener acceso a un recurso sencillo y rápido ante jueces o tribunales competentes que amparen sus derechos fundamentales. Dicha garantía constituye uno de los pilares básicos, no sólo de la Convención Americana, sino del propio Estado de Derecho en una sociedad democrática en el sentido de la Convención"[196].

La Ley 16.011, la cual es aplicada en su totalidad por nuestros tribunales, conforme al análisis realizado precedentemente, incluye varios requisitos para su procedencia. Así por ejemplo, establece un plazo de caducidad para el inicio de la pretensión de tan solo 30 días, así como incluye el elemento de la ilegitimidad manifiesta, entre otros que no están contemplados ni por el artículo 7 o 72 de la Constitución, ni por el artículo 25 de la Convención Americana.

Advertimos aquí, entonces, una importante barrera para la tutela del derecho al olvido, el cual se entiende reconocido, y cuya efectividad debería poder ser objeto de una acción de amparo, la cual no debería ser desestimada por cuestiones de índole formal.

En este punto, los jueces uruguayos y ante solicitudes de esta índole, deberían realizar una interpretación de la legislación conforme a la Constitución recurriendo al amparo constitucional, y, asimismo, conforme a la Convención Americana. La necesidad de un análisis

---

[193] Respecto al fundamento de la acción de amparo en el artículo 7 de la Constitución ver: OCHS OLAZABAL, Daniel. *La acción de amparo.* Montevideo, FCU, 1995, p, 7 y ss. Otros autores encuentran el fundamento en el artículo 72, en este sentido ver: REAL, Alberto Ramón. *La acción de amparo en la jurisprudencia argentina y ante el derecho uruguayo*, en: Revista de la Facultad de Derecho y Ciencias Sociales. Año XIV, Nº 1, 1963. Asimismo, otros expresan que la consagración está en los dos artículos precitados: RISSO FERRAND, Martín. *Derecho Constitucional I.* Ob. Cit., pp. 495 y ss.

[194] GROS ESPIELL, Héctor. *El derecho de amparo en el Uruguay*, en: FIX-ZAMUNDIO, Héctor (Dir.). *El Derecho de Amparo en el Mundo.* México, Porrúa, 2006, p. 634.

[195] Corte Interamericana de Derechos Humanos. Opinión Consultiva No. 9/87, del 6 de Octubre de 1987, solicitada por Uruguay, párrafo 38.

[196] Corte Interamericana de Derechos Humanos. Caso Maritza Urrutia v. Guatemala. Sentencia del 27 de noviembre de 2003, párrafo 117; y Caso Acosta Calderón v. Ecuador. Sentencia del 24 de Junio de 2005, párrafo 93.

de convencionalidad por parte de los integrantes del Poder Judicial fue introducido por la Corte Interamericana en el caso Almonacid Arellano y otros c. Chile, al decir que: "La Corte es consciente que los jueces y tribunales internos están sujetos al imperio de la ley y, por ello, están obligados a aplicar las disposiciones vigentes en el ordenamiento jurídico. Pero cuando un Estado ha ratificado un tratado internacional como la Convención Americana, sus jueces, como parte del aparato del Estado, también están sometidos a ella, lo que les obliga a velar porque los efectos de las disposiciones de la Convención no se vean mermadas por la aplicación de leyes contrarias a su objeto y fin, y que desde un inicio carecen de efectos jurídicos. En otras palabras, el Poder Judicial debe ejercer una especie de "control de convencionalidad" entre las normas jurídicas internas que aplican en los casos concretos y la Convención Americana sobre Derechos Humanos"[197].

El control de convencionalidad que propiciamos ya no refiere exclusivamente a la definición dada inicialmente por la doctrina[198], atinente al mecanismo de protección procesal que ejerce la Corte Interamericana, la que ante una confrontación normativa entre la Convención y el derecho interno, prefiere la aplicación de la primera. Sino que incluye los nuevos postulados que a su respecto ha realizado la Corte Interamericana en sus últimos fallos, esto es, a interpretar y aplicar la legislación interna conforme a la Convención. Asimismo, corresponde aplicar, en este punto, el principio *pro homine* y de directriz de preferencia, lo que implicaría recurrir al amparo constitucional. Por tanto, en la materia que nos ocupa, ello involucra un análisis del artículo 7 de la Constitución, de la Ley 16.011 y de la acción de amparo conforme al artículo 25 de la Convención Americana.

La labor del Poder Judicial debe estar orientada a cumplir con el mandato que el constituyente le ha otorgado, teniendo como fin último el cumplimiento del Estado de Derecho, siendo, en éste, la última garantía para efectivizar los derechos humanos. En este nuevo final, y en la práctica uruguaya, por tanto, el derecho al olvido, con reconocimiento implícito en la Constitución, debería ser efectivizado mediante el amparo de los órganos jurisdiccionales. Pues, si bien la regulación es insuficiente, debiendo ser atendida en los próximos años, las garantías constitucionales actuales permiten su tutela, la cual depende, en última instancia, del compromiso que los órganos jurisdiccionales evoquen a favor de una tutela jurisdiccional efectiva; esto es, posibilitando la puesta en práctica de los principios y medios de protección, y garantizando, por consiguiente, el derecho al olvido.

Los primeros pasos de este cambio de paradigma fueron dados ya por nuestra Suprema Corte de Justicia, que en Sentencia No. 365/2009, dictada el 19 de Octubre de 2009, señaló: *"La Corporación comparte la línea de pensamiento según la cual las convenciones internacionales de derechos humanos se integran a la Carta por la vía del art. 72, por tratarse de derechos inherentes a la dignidad humana que la comunidad internacional reconoce en tales pactos"*.

Esperamos que este sea el comienzo de un largo camino de reconocimientos y compromisos, en los que esta postura sea recogida por todos nuestros órganos jurisdiccionales. La labor de la jurisprudencia uruguaya en este sentido acompasaría y permitiría, además, la unificación de los criterios de protección entre los países latinoamericanos y el avance y

[197] Corte Interamericana de Derechos Humanos. Caso Almonacid Arellano y otros v. Chile. Sentencia del 26 de Setiembre de 2006, párrafo 124.
[198] REY CANTOR, Ernesto. *Control de Convencionalidad de las leyes y derechos humanos.* México, Porrúa, 2008, p. 46.

evolución hacia la configuración de lo que Sagüés denomina como un *"ius commune interamericano"*[199].

CONCLUSIONES

Avances tecnológicos, intimidad e Internet son una trilogía que parece no separarse en estos últimos años. La evolución tecnológica, sumada a la globalización, hizo que con la aparición de Internet, y particularmente de los buscadores y las redes sociales, la vigencia de muchos derechos, algunos de primera generación, reconocidos hace ya un largo tiempo atrás, se viera cuestionada.

En el presente trabajo analizamos una realidad en la que estamos inmersos, y en la que pocas veces nos hemos detenido a reflexionar, que ocurre tanto en los países Europeos, como en Latinoamérica, y, también acontece en nuestro país, Uruguay.

Esta realidad está específicamente orientada a la necesidad del reconocimiento del derecho al olvido, un derecho que, si bien ya había sido nombrado anteriormente, hoy en día, adquiere especial proyección e importancia.

Las materias trascendentes en la eliminación de datos ya no son solo penales o crediticias, y la supervisión y control del nuevo fenómeno parece haberse escapado, llegando, nuestra información, a infinidades de espacios, en cuestión de segundos, donde podría permanecer por décadas.

Los viejos recuerdos son los datos que conservamos en nuestra memoria, que han ocurrido en el pasado, o pertenecen al presente, muchos de los cuales no queremos compartir. Como analizamos, son varios los casos en los que se cuestiona la efectividad de los derechos humanos en pugna, al quedar, muchos sujetos, ligados a estos recuerdos, por estar contenidos en la web o en bases de datos desconocidas, dándoseles un uso no consentido ni imaginado. Además, con la conjunción de estos datos, las fotografías o las acciones, se podría arribar a obtener rasgos característicos de nuestra personalidad, lo que resulta riesgoso y determinante para nuestra intimidad.

Estas controversias merecen un nuevo final.

Los viejos recuerdos son los datos que existieron y existen actualmente de nosotros, incorporados a la gran plataforma universal; los nuevos finales simbolizan la efectividad del derecho al olvido, el derecho que posee todo sujeto a que dicha información sea eliminada y suprimida cuando así lo estime conveniente, debiéndose armonizar, en su reconocimiento y aplicación, con los demás intereses en pugna.

Los viejos recuerdos son la recepción parcial del derecho al olvido, únicamente orientado a las bases de datos penales y crediticias, así como la insuficiencia en la aplicación práctica de los mecanismos previstos para su tutela por parte de los órganos jurisdiccionales; los nuevos finales representan la conciencia y el compromiso con la problemática actual, la consagración expresa de este derecho, así como su protección, tanto por vías normativas, como administrativas y jurisdiccionales; las que específicamente atiendan a esta nueva realidad y sean puestas en práctica, en concordancia con la constitucionalidad y la convencionalidad.

Estos recuerdos serán, en los próximos años, olvidados y, sin duda, se convertirán en viejos recuerdos, con nuevos finales.

---

[199] SAGÜES, Néstor Pedro. *El "control de convencionalidad" como instrumento para la elaboración de un ius commune interamericano*, en: Biblioteca Jurídica virtual del Instituto de Investigaciones Jurídicas de la UNAM, consultado en: *www.jurídicas.unam.mx*.

Bibliografía Consultada

ALEXY, Robert. *Teoría de los Derechos Fundamentales*. Madrid, Centro de Estudios Constitucionales, 1993.

ARRIETA, Raúl; ORTIZ, Claudio y otros. *Chile y la protección de datos personales. ¿Están en crisis nuestros derechos fundamentales?* Chile, Universidad Diego Portales, 2009.

BIDART CAMPOS, Germán. *Teoría general de los derechos humanos.* Buenos Aires, Astrea, 1991.

BIDART CAMPOS, Germán. *Tratado elemental de derecho constitucional.* Buenos Aires, Ediar, 1994.

CABANELLAS DE LAS CUEVAS (Dir.), Guillermo. *Derecho de Internet.* Buenos Aires, Heliastra, 2004.

CORREA, Carlos; NAZAR, Félix; CZAR, Susana; BATTO, Hilda. *Derecho Informático*. Buenos Aires, Depalma, 1987.

DE SLAVIN, Diana. *Mercosur: La protección de los datos personales*. Buenos Aires, Depalma, 1999.

DIAZ REVORIO, Francisco. *Los derechos humanos ante los nuevos avances científicos y tecnológicos.* Valencia, Tirant Lo Blanch, 2009.

DROMI, José Roberto y MENEM, Eduardo. *La Constitución Reformada: Comentada, Interpretada y Concordada.* Buenos Aires, Ediciones ciudad Argentina, 1994.

DRUCAROFF AGUIAR, Alejandro. *Información crediticia, derecho al olvido e interés general.* Artículo Publicado en Revista La Ley Online, consultado en: *www.laleyonline.com.uy.*

DURÁN MARTÍNEZ, Augusto. *Derecho a la protección de datos personales y al acceso a la información pública.* Montevideo, Editorial Amalio M. Fernández. 1ª Ed., 2009.

EGUIGUREN PRAELI, Francisco. *La libertad de Expresión e Información y el Derecho a la Intimidad Personal.* Lima, Palestra, 2004.

FERRAJOLI, Luigi. *Los fundamentos de los derechos fundamentales.* Madrid, Editorial Trotta, 2005.

FIX-ZAMUNDIO, Héctor (Dir.). *El Derecho de Amparo en el Mundo*. México, Porrúa, 2006.

GARECA PERALES, Pedro. *El hábeas data en la Constitución de Bolivia.* En: Anuario de Derecho Constitucional Latinoamericano, Año 11º, Tomo II, Konrad Adenauer Stiftung, 2005.

GROS ESPIELL, Héctor. *Estudios sobre derechos humanos.* Instituto Interamericano de Derechos Humanos, Editorial Jurídica Venezolana, 1985.

GUTWIRTH, Serge; POULLET, Yves; LENEES, Ronald y otros. *Computers, Privacy and Data Protection: an Element of Choice*. Nueva York, Springer, 2011.

HERRÁN ORTIZ, Ana Isabel. *El derecho a la intimidad en la Nueva Ley Orgánica de Protección de Datos Personales.* Madrid, Dykinson, 2002.

LAMAS, Mario Daniel. *Estudio sobre el nombre, la imagen, la intimidad, la identidad, el honor y la reputación como derechos personales y como derechos patrimoniales.* Montevideo, CIKATO, 2004.

NOGUEIRA ALCALÁ, Humberto. *Autodeterminación informativa y hábeas data en Chile e información comparativa*, en: Anuario de Derecho Constitucional Latinoamericano, 11º Año, Tomo II. Konrad Adenauer Stiftung, 2005.

OCHS OLAZABAL, Daniel. *La acción de Amparo*. Montevideo, FCU, 2001.

PALAZZI, Pablo. *Informes Comerciales.* Buenos Aires, Astrea, 2007.

PALAZZI, Pablo. *La Transmisión Internacional de Datos Personales y la Protección de la Privacidad.* Buenos Aires, Ad-Hoc, 2002.

REY CANTOR, Ernesto. *Control de Convencionalidad de las leyes y derechos humanos.* México, Porrúa, 2008.

RISSO FERRAND, Martín. *Algunas garantías básicas de los derechos humanos*. Montevideo, FCU, 2008.

RISSO FERRAND, Martín. *Algunas Reflexiones sobre los derechos al honor, a la intimidad, a la propia imagen y la libertad de prensa,* en: Anuario de Derecho Constitucional Latinoamericano, Konrad Adenauer Stiftung, 2002.

RISSO FERRAND, Martín. *Derecho Constitucional I.* Montevideo, FCU, 2005.

ROIG, Antoni. *Derechos Fundamentales y Tecnologías de la Información y de las comunicaciones (TICs).* Barcelona, Bosch Editor, 2010.

RUFFINI GANDOLFI, María Leticia. *Divulgación de hechos privados y responsabilidad de los medios masivos de comunicación*, en: Estudios Jurídicos Nº 6. Facultad de Derecho Universidad Católica del Uruguay, 2006.

SAGÜES, Néstor Pedro. *El "control de convencionalidad" como instrumento para la elaboración de un ius commune interamericano*, en: Biblioteca Jurídica virtual del Instituto de Investigaciones Jurídicas de la UNAM, consultado en: www.jurídicas.unam.mx.

SCHWOB, Marc. *Como conservar e desenvolver sua memoria*. Rio de Janeiro, Ediouro Publicaciones, 2005.

Privacy-by-design ou Privacy-by-Law

Pr. **Jean-Jacques Lavenue**[200,201]
Clémence Codron[1,2], doctorante
M. **Nicolas Desrumaux**[1,2], Docteur en Droit public
M. **Gaylord B. Hamerel**[1,2], doctorant

> *« Et pourtant ce tyran, seul, il n'est pas besoin de le combattre, ni même de s'en défendre ; il est défait de lui-même, pourvu que le pays ne consente point à la servitude. Il ne s'agit pas de lui rien arracher, mais seulement de ne lui rien donner. »*[202]

Prolégomènes : Privacy et labellisation

La « *privacy-by-design* » repose sur un concept fondamental aux contours incertains. La « *Privacy* » n'est pas la vie privée stricto sensu, et recouvre encore moins la notion de données personnelles telle que nous la connaissons en droit français, et plus largement, à l'échelle du droit applicable dans l'Union européenne. La notion de *privacy* pose un problème technique pour les juristes français. C'est un export linguistique d'un concept dont le développement est beaucoup plus étroit qu'un emprunt aux systèmes de Common Law. La *privacy* prise dans la logique industrielle trouve ses fondements dans un concept existant dans l'ordre juridique des Etats-Unis.

Sans affirmer ou prétendre que le droit communautaire, ou plus étroitement le droit français, laissent augurer une autonomie d'un concept de vie privée plus marqué et presque autonome, il est important de relever que la *privacy* nord-américaine ne correspond qu'à un nuage de dispositions éparpillées dans les législations de l'Etat fédéral et des Etats fédérés. Sa substance est moins unifiée que les notions de vie privée et de données personnelles, telles que la loi du 6 janvier 1978, le détermine.

Trouver les déterminants de la *privacy* revient à chercher l'application et l'interprétation de principes généraux à travers la jurisprudence, en concurrence avec d'autres principes, parfois plus ancrés dans la législation. La source reconnue de la notion de *privacy* émane du Bill of Rights (principalement les dix premiers Amendements, ainsi que le Quatorzième de la Constitution des Etats-Unis) ; son principe n'est pas explicitement défini. Ainsi, l'évocation d'une atteinte à un principe de *privacy* ne constitue pas une contestation de légalité des actes, mais renvoie régulièrement au contrôle de constitutionnalité des dispositions légales ou des conventions. Le Quatrième Amendement (le droit des personnes de voir garantis de l'intégrité de leur personne, de leur domicile, de leurs documents et biens) est la source principale de jurisprudence émanant sur la question. Les différents cas tranchés en la matière ont permis de dégager des solutions incertaines aux intrusions dans la vie privée, autorisées ou limitées par la législation fédérale.

Ce sont alors les contours de la propriété privée qui sont pris en compte pour l'essentiel, et le statut de la donnée personnelle dans son prolongement. La question régulièrement tranchée n'est donc pas celle de la garantie de l'intégrité des données personnelles, mais bien de vérifier si leur divulgation a été autorisée.

[200] Univ Lille Nord de France, F-59000 Lille, France.
201 UDSL, CERAPS, UMR 8026 F-59000 Lille, France.
202 LA BOÉTIE, *Discours de la servitude volontaire*, 1576, trad. Charles Teste (1836), p. 14.

La jurisprudence « United States vs Katz » a montré qu'une limite d'interprétation opposable à la protection induite par le Quatrième Amendement est la diffusion publique, en toute connaissance de cause, le Quatrième Amendement est censé protéger les personnes, et non les lieux, quels qu'ils soient. Les dérivés de cette position ont progressivement fixé la nécessité d'une information simplifiée sur les tenants technologiques liés à cette exposition potentielle à un transfert des informations. C'est bien le partage de l'information qui est encadré, et non la possibilité d'empêcher sa consultation. L'affaire « United States vs Hambrick » a confirmé qu'à défaut d'avoir prohibé contractuellement la diffusion d'informations personnelles par un tiers, l'utilisateur ne peut plus s'opposer à la dissémination des informations en question aux tiers, et *de facto* faire fonctionner les mécanismes de *privacy*.

Qu'il soit question de droit du travail, de protection des brevets, du commerce, ou des obligations de sécurité publique, la notion de *privacy* est remise en jeu au gré des contentieux, majoritairement fondé sur des questions de responsabilité contractuelle. Cette pratique constitue une mécanique propre aux systèmes de Common Law, où la contractualisation des rapports prime sur la nécessité d'un régime légal formaliste, ou d'une protection renforcée initiée par le législateur. Le gardien reconnaissable à l'échelle fédérale pour la protection des principes de protection de la *privacy* est la Federal Trade Commission [FTC].

L'amalgame entre vie privée, données personnelles et *privacy* est courant dans le domaine des technologies de l'information. Le vocable à dimension variable est représentatif d'une somme d'hésitations en matière de technologies de l'information quant au modèle de gestion des données, aux outils confiés à l'utilisateur, et plus généralement au rôle de l'utilisateur.

Si la technologie et les outils qui en découlent se veulent neutres, leur rôle et leurs usages portent la marque de fabrique de leurs créateurs. L'ensemble des moyens mis en œuvre dans la conception d'une solution logique, ou matérielle, représentent une somme de connaissances articulées en fonction de la destination (de finalité ?) de l'outil et de son environnement, qu'il soit humain, ou normatif.

L'existence de standards ne correspond pas en soi des normes techniques et industrielles telles qu'elles s'entendent à l'échelle économique. Hors du champ strict de la norme juridique, la normalisation constitue à la fois l'état de l'art, l'étalon ou la référence technique d'un secteur ou d'un type de produits ou de services, au profit de leur commercialisation. La dimension de la normalisation fait de plus en plus partie du lot commun lié à l'intelligence économique et à la compétitivité[203], lorsque la « normalisation informelle » rend l'Etat aveugle face à des organisations nord-américaines hors tutelle des Etats et des organisations de normalisations telles que l'ISO ou l'AFNOR. Elles permettent d'établir des standards de fait excluant la garantie de participation équilibrée telle que voulue dans les institutions recevant une participation des Etats.

La consécration d'une norme technique en France passe obligatoirement par sa reconnaissance dans un texte réglementaire. L'article 17 du décret du 16 juin 2009[204] relatif à la normalisation organise le processus de reconnaissance vertical des normes à l'échelle nationale et du rôle centralisateur de l'AFNOR (association créée en 1926, financée à hauteur de 20 % de son budget par l'Etat français) en ces termes :

« *Les normes sont d'application volontaire.*

Toutefois, les normes peuvent être rendues d'application obligatoire par arrêté signé du ministre chargé de l'industrie et du ou des ministres intéressés.

203 cf Rapport Carayon au premier ministre de 2006, *« A armes égales »*, pp. 47-55, disponible sur le site de la Documentation française (Accueil > Rapports publics > A armes égales : rapport au Premier ministre). URL : http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics//064000728/0000.pdf (page vérifiée le 30 juin 2012).
204 Décret n°2009-697 du 16 juin 2009, JORF n°0138 du 17 juin 2009 page 9860. Le décret peut être consulté sur le site Légifrance (NOR: ECEI0909907D ; version valide au 02 février 2012).

Les normes rendues d'application obligatoire sont consultables gratuitement sur le site internet de l'Association française de normalisation. »

Plus que de simples recommandations techniques, les normes industrielles constituent un ensemble de référentiels marquant un enjeu industriel et commercial pour la structuration du marché autour de spécifications *a minima*, visant à assurer l'effectivité d'un modèle consensuel favorisant les usages et les bonnes pratiques entre la recherche, les industriels et le produit de leurs travaux. C'est avant tout un exercice consensuel d'agrégation des connaissances sur un sujet, voué à définir le périmètre d'accès à une technologie ou une méthodologie. Elle peut revêtir une dimension strictement nationale et plusieurs échelles d'importance à l'international.

La normalisation internationale est apparue simultanément après la Première Guerre mondiale, dans la foulée de la reprise économique et de l'entrée dans la seconde phase de l'ère industrielle propice à l'expansionnisme du secteur secondaire. Plus qu'une simple méthode d'unification, elle représente un enjeu pour les Etats (soit de manière directe, soit par le biais d'instituts de normalisation privés liés plus ou moins directement à l'Etat) et les organisations internationales *ad hoc* (dits organismes de normalisation, ou Standard Development Organisation [SDO]) s'étant emparées des compétences d'établissement et de protection des normes.

A l'échelle européenne, le Comité européen de normalisation [CEN] recouvre l'ensemble des organismes de normalisation des Etats membres, et dispose théoriquement de l'appui de l'outil normatif des directives communautaires pour imposer l'application des normes, européennes, et internationales (a fortiori produites au sein des comités ISO) dans chaque Etat membre de l'Union.

Il en résulte que le modèle dominant en matière de normalisation repose sur l'existence d'ONG ou d'associations aux missions reconnues par les pouvoirs publics des pays faisant interface entre les intérêts scientifiques, industriels des entreprises, et le devoir régalien pour les Etats d'assurer à la fois l'efficacité de leur industrie et d'aménager leur échelle de protectionnisme économique et technologique.

Il existe toutefois des ordres de normalisation alternatifs aux processus mis en place (de plus ou moins loin) par les Etats, à l'initiative d'entreprises ou de groupes d'intérêts industriels disposant des moyens nécessaires au soutien de programmes et de consortiums de normalisation parallèles. Dans le domaine des technologies de l'information et du réseau internet, des références de normalisation comme le W3C (World Wide Web Consortium) et le IEEE (Institut des ingénieurs en électricité et électronique) échappent à l'implication des Etats, y compris des Etats-Unis. Ces normalisations informelles bénéficient pourtant, par leur ancrage dans l'industrie et la présence d'entreprises clef du marché, du pouvoir d'imposer des standards de fait, sans interventions extérieures au giron des contributeurs industriels.

Parfois répercutées tardivement dans d'autres ordre normatifs (en particulier en raison de l'inévitable période de latence liée aux négociations et au canal de diffusion, discussion, production d'une norme internationale concertée) tels qu'au sein des ISO, ces normes s'imposent souvent d'elles-mêmes par leur diffusion préalable, et leur intégration dans un canal de collaboration avec les institutions officielles.

Le mouvement d'intégration progressive des organismes parallèles dans un processus d'échange institutionnalisé constitue une nouveauté. Le rapprochement en novembre 2010 de l'ISO vers le W3C, comme organisme de soumission, marque une étape notable de remise en cause du modèle initial de normalisation dans une ambiance de méfiance réciproque. Si ce geste est marquant, c'est aussi parce qu'il repose sur un constat simple, rendant le W3C incontournable en matière de normalisation des outils du web.

Il reste que le W3C est un consortium purement industriel au sein duquel la représentation n'est pas assurée en fonction de critères de nationalité mais d'intérêts économiques et industriels pour la question.

Il reste que la promotion de la « *privacy-by-design* » s'apparente très largement à l'embryon d'un modèle de normalisation de fait, qu'on pourrait qualifier de « molle ». L'implication d'acteurs hétérogènes, dépourvus d'une légitimité ou d'un mandat relevant de la souveraineté des Etats finançant leurs fonctions, ou de représentants des intérêts économiques d'acteurs industriels, ne suffit pas à repérer les contours d'un consortium structuré, ou d'un normalisateur de fait tel que connu jusqu'ici.

I. - Un modèle proliférant présenté comme incontournable

Dans sa dimension transnationale l'emprise de l'approche normative nord américaine bénéficie d'un phénomène de promotion du concept non juridique de *privacy-by-design*. Promu comme un modèle à vocation universelle, ce concept peut aussi être appréhendé comme un exemple du phénomène de tautisme, développé par Lucien Sfez. Issu d'une approche à dominante mercatique, le modèle de la *privacy-by-design* bénéficie d'une promotion qui échappe à la législature étatique.

- **À propos d'une démarche paradoxale plus soucieuse de merchandisage que d'efficacité dans la protection juridique des individus**

Présenté comme une sorte de panacée universelle susceptible, dans l'intérêt général, d'assurer la protection de la vie privée et des données personnelles, le concept de « privacy-by-design » apparaît à l'analyse comme le produit d'une approche particulière et d'une sorte d' auto-promotion qui renverse l'approche européenne de la protection de la vie privée par un retournement du mécanisme de la responsabilité au profit du secteur industriel.

Il est possible d'en donner un exemple. Il pourra découler ainsi de la logique présidant au mécanisme mis en place, qu'à partir du moment où le particulier n'aura pas utilisé (ou su utiliser) le mécanisme technologique mis à sa disposition pour exercer la protection de sa vie privée ou de ses données, l'entreprise industrielle pourra voir sa responsabilité dégagée des atteintes commises à la vie privée. Les moyens de sa propre protection ayant été fournis a priori à l'usager, les données sensibles pourraient être alors, récupérables du fait de l' « imprudence » ou de l'absence de diligence des individus. Ce qui naturellement n'est pas le cas lorsque la loi impose au secteur marchand de ne pas porter atteinte à la « privacy ».

Le nouveau concept de *privacy-by-design* est l'expression d'une philosophie spécifique, et l'affirmation par ses promoteurs d'une sorte de « reconnaissance générale » alléguée ne doit pas dispenser l'observateur de l'analyse du discours. Selon la référence classique du « qui parle ? » et « d'où parle-t-il ? ».

Le juriste européen à l'occasion de cette démarche a alors l'impression de se trouver face à un phénomène qui illustre le phénomène de « tautisme »[205] décrit par Lucien SFEZ[206]. La communication, remplaçant la loi, vient présenter comme vérité et référence normative, ce qui n'est qu'une opération de réduction du périmètre de l'action normative de l'État au profit du secteur privé, de la protection des citoyens remplacés par des clients pour la protection de leur propre « privacy ». Le discours sur la technologie vecteur du bien commun remplace alors le discours sur la loi protectrice des libertés et de la vie privée. Le concept de *privacy-by-design* procède à un « arraisonnement » du droit au moyen d'un discours

205 Confusion qui s'installe entre le fait réel et sa représentation médiatique. Le tautisme *« utilise la tautologie comme seule vérification : si je répète, je prouve »* in SFEZ (L.), *Critique de la communication*, Le Seuil, 1988/1992, p.110.
206 Ibid.

biaisé sur la privacy comme moyen et non comme finalité. Reposant sur la définition d'une sorte de mise en place de bonnes pratiques industrielles, la *privacy-by-design*, apparaît comme un cheval de Troie susceptible de donner des coudées franches au secteur marchand.

1. a. La production du concept de « privacy-by-design ».

Ainsi que le rappelait, en 2009, le Contrôleur européen de la protection des données Peter Hustinx, « *le concept de privacy-by-design » est étroitement lié à celui de ''technologies renforçant la protection de la vie privée''(PET, Privacy Enhancing Technologies). Ce terme a été utilisé pour la première fois dans le rapport 'Technologies renforçant la protection de la vie privée : le chemin vers l'anonymat » publié en 1995* »[207].

Les auteurs en étaient John J. Borking[208], Commissaire à la protection de la vie privée des Pays Bas, et Ann Cavoukian, docteur en psychologie, Assistant Commissioner à la Privacy de l'Ontario. Sur la page qu'elle consacre à la *privacy-by-design*, la Commissaire de l'Ontario confirme que « *La protection de la vie privée est un concept mis au point par la commissaire à l'information et à la protection de la vie privée de l'Ontario Ann Cavoukian, PhD., afin de composer avec les effets croissants et systémiques des technologies de l'information et des communication et des réseaux de grande envergure* »[209]. L'assertion est réitérée dans les nombreuses pages internet promouvant le concept et son maître d'œuvre[210].

Pour autant que l'on s'attache à définir ce que serait l'approche plus spécifique d'Ann Cavoukian par rapport à celle de John J. Borking, la distinction paraît se situer sur la place que les deux commissaires ont accordé au droit dans l'organisation du mécanisme de protection. Autant chez l'un la prise en compte de la dimension juridique du projet paraît en soi importante[211] , autant, chez l'autre, celle-ci ne semble au mieux être prise en compte qu'en tant qu' élément d'appui d'une dimension commerciale, voire marketing, du produit labellisé « PbD ». Le droit y paraîtrait même, comme hypothèse de départ, disqualifié pour non-efficience. Ainsi qu'Ann Cavoukian le souligne sur son site : «*La protection intégrée de la vie privée est fondé sur le principe selon lequel la protection de la vie privée ne pourra être assurée par le simple respect des lois et cadres règlementaires et doit, idéalement, être intégrée dans les activités de l'organisation* »[212]. Toute l'ambiguïté de la démarche et l'origine de ce qui nous paraît être en réalité un processus de contournement de la loi par les marchands du temple (la « main invisible » de Hayek ?) et de retournement de la responsabilité des acteurs nous paraît résider dans cette affirmation. Cela ressort également d'un autre document d'Ann Cavoukian, lorsqu'elle écrit : «*Le respect de la vie privée a toujours été une norme sociale, mais depuis quelques années, il a évolué.* ***Il ne s'agit plus désormais de respecter simplement la loi, mais également de se démarquer sur le marché****, de mériter la confiance des consommateurs et de favoriser le libre choix dans notre société de l'information.*

« De plus en plus, on considère que l'innovation, la créativité et la compétence doivent être envisagées selon une approche conceptuelle globale, interdisciplinaire, intégratrice et inspirante, ***dans le but d'éliminer les***

207 HUSTINX (P.), *Respect de la vie privée dès la conception (privacy-by-design): le séminaire définitif*, Madrid, 2 nov. 2009, p. 1. Disponible sur le Site du Contrôleur européen à la protection des données : http://www.edps.europa.eu > Publications > Discours et articles > 2009. URL : http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2009/09-11-02_Madrid_privacybydesign_FR.pdf (page vérifiée le 30 juin 2012).
208 BORKING (J. J.), *Privacy Enhancing Technologies*, Based on a Joint Study in Netherlands and Ontario, 1995 ; BORKING (J. J.) et RAAB (Ch. D.), *Laws, PETs and other Technologies for Privacy Protection*, JILT, 2001, vol. 1 (refered article) disponible sur le site de l'Université de Warwick (http://www2.waewick.ac.uk > Faculties > Law > Electronic Law Journals > JILT > Borking ; page vérifiée le 30 juin 2012).
209 http://ipc-new.dev.agriya.com/about/history/ (Site http://Privacybydesign.ca > About PbD > History ; page vérifiée le 30 juin 2012).
210 http://ipc-new.dev.agriya.com/ (idem)
211 http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_1/borking/#a1 (fil d'Ariane : v. note 7).
212 La version anglaise paraît plus claire encore : *« privacy-by-design advances the view that the future of privacy cannot be assured solely by compliance with legislation and regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation. »* ; Site http://privacybydesign.ca, page « History » (About PbD > History).

contraintes*…L'intégration de la protection de la vie privée dans une technologie, un processus ou un système doit se faire de façon à préserver la pleine fonctionnalité et, dans toute la mesure du possible, à optimiser toutes les exigences.*

« On considère souvent la protection de la vie privée comme un objectif à somme nulle qu'on ne peut privilégier qu'au détriment d'autres intérêts légitimes, d'objectifs de conception ou de capacités techniques. Or la protection intégrée de la vie privée rejette cette approche ; elle ***permet de poursuivre des objectifs légitimes touchant des aspects autres que la protection de la vie privée,*** *selon une démarche novatrice à somme positive* »[213]. Est-ce faire preuve d'une excessive paranoïa que de penser que ce type de phraséologie est susceptible de lectures antithétiques ou ,au moins d'ambigüité ?[214]

2. b. Un concept anti-juridique soutenu dans un rapport de force par le secteur marchand.

Cette approche est présentée par les prosélytes du *privacy-by-design* comme une évidence. Avec un oeil critique, nous y voyons un simple effet de tautisme. C'est, d'une certaine manière, ce qui ressort du discours de Peter Hustinx lorsque, assimilant PETs[215] et *privacy-by-design*, il déclare : «*il faut se rendre à l'évidence que le concept…a été pleinement accepté. D'une certaine façon, il est considéré comme une marque de commerce forte, et différentes tentatives ont eu lieu pour bénéficier de sa réputation et y inclure d'autres technologies, qui ne sont pas nécessairement des technologies '' renforçant la protection de la vie privée » mais des technologies ''imposant la vie privée'' ou ''permettant la vie privée''*[216]. Or, précisément, le fait d'intégrer dans « *les objectifs de la protection intégrée de la vie privée… le contrôle sur les renseignements qui nous concernent et permettre aux organisations de se donner un avantage concurrentiel appréciable »*[217], mesure ce qui nous apparaît comme une confusion dans les finalités, un mélange des genres. II est également révélateur d'une conception traduisant une volonté de changement de rapport de forces au sein du triptyque technique-droit-citoyen encadré par l'État, susceptible d'amener à l'établissement d'un rapport commerce-bonnes pratiques-usagers/clients défini par le pouvoir Marchand[218]. Cette démarche familière à l'univers conceptuel anglo-saxon se heurte encore assez largement, à l'heure actuelle, aux ordonnancements juridiques des États de l'ensemble Européen.

Affirmer que la *privacy-by-design « est considérée comme une nouvelle norme mondiale en matière de protection de la vie privée »* n'implique en rien que lui soit reconnue a priori la moindre valeur juridique. Tautisme ou Méthode Coué, l'approche proactive, en l'état (juridique) actuel des choses, est un produit, un possible standard de packaging ou de marketing ce n'est en aucun cas une nouvelle norme juridique mondiale. Le choix de l'adjectif, ou son absence dans les déclarations d'Ann Cavoukian, a son importance. Il ne s'agit bien en l'espèce que d'une participation à une sorte entreprise de déjuridicisation de la protection de la vie privée et des données personnelles utilisant les moyens de la communication**.**

Que l'on y soit ou non favorable, le mécanisme mis en place par la *privacy-by-design*, sauf à correspondre à un discours fort général et velléitaire, supposera d'une certaine manière la prise en charge de la protection de la vie privée par l'industrie à travers une sorte de dialogue pragmatique entre entrepreneurs et usagers. C'est ce qui ressort de l'énumération des sept principes fondamentaux, lorsqu' on lit :

---

213 http://www.ipc.on.ca/images/Resources/pbd-implement-7found-principles-f.pdf (http://www.ipc.on.ca > Resources > Pratiques exemplaires et lignes directrices, page vérifiée le 30 juin 2012). Nous grassons.
214 « Aie confiance, Crois en moi, Que je puisse, Veiller sur toi…Fais un somme, Sans méfiance, Je suis là, Aie confiance... » siffle le serpent Kaâ à Moogly dans le Livre de la jungle…
215 Privacy Enhancing Technologies. Voy. John J. Borking et Charles D. Raab, préc. dans leur article *Laws,Pets, and other Technologies for Privacy Protection*, préc.
216 V. supra note 8.
217 CAVOUKIAN (A.), *La protection intégrée de la vie privée. Les sept principes fondamentaux*, disponible sur : http://ipc.on.ca/images/Resources/pbd_7foundationalprinciples-f.pdf (préc. note 14).
218 La « Politique de confidentialité », restant aussi à définir par l'entreprise, constituera également un sujet d'interrogation pour le citoyen / usager / client.

*« 1. Prendre des mesures **proactives** et non réactives; des mesures **préventives** et non correctives. La protection intégrée de la vie privée (PIVP) se caractérise par des mesures proactives et non réactives. Elle consiste à prévoir et à prévenir les incidents d'atteinte à la vie privée avant qu'ils ne se produisent. En effet, la PIVP n'attend pas que des risques pour la vie privée se concrétisent, et elle ne propose aucune solution pour résoudre les cas d'atteinte*

à la vie privée qui se sont déjà produits. Elle vise plutôt à les prévenir. Bref, la protection intégrée de la vie privée vient avant et non après de tels incidents.

*2. Assurer la protection **implicite** de la vie privée.On peut être sûr d'une chose : la protection intégrée de la vie privée est implicite. Elle vise à procurer le maximum de vie privée en veillant à ce que les renseignements personnels soient systématiquement protégés au sein des systèmes informatiques ou dans le cadre des pratiques internes. Donc, la vie privée d'un particulier est protégée même si ce dernier ne pose aucun geste, car la protection de la vie privée est intégrée dans le système, implicitement.*

*3. **Intégrer** la protection de la vie privée dans la conception des systèmes et des pratiques. La protection intégrée de la vie privée, comme son nom le suggère, est intégrée dans la conception et l'architecture des systèmes informatiques et des pratiques des organismes; elle n'y est pas greffée après coup. La protection de la vie privée devient donc un élément essentiel des fonctionnalités de base. Elle fait partie intégrante du système, sans porter atteinte à ses fonctions.*

*4. Assurer une fonctionnalité **intégrale** selon un paradigme à somme positive et non à somme nulle . La protection intégrée de la vie privée vise à tenir compte de tous les intérêts et objectifs légitimes en cause selon un paradigme à somme positive et non selon une approche périmée à somme nulle, qui nécessite des compromis inutiles. La protection intégrée de la vie privée évite ces fausses dichotomies, par exemple celle qui oppose la protection de la vie privée à la sécurité, en démontrant qu'il est **vraiment** possible de réaliser ces deux objectifs à la fois.*

*5. Assurer la sécurité de bout en bout, pendant **toute la période de conservation des Renseignements.** La protection intégrée de la vie privée, lorsqu'elle est intégrée dans le système avant que l'on ne commence à recueillir les renseignements qu'il contiendra, persiste de façon sécurisée pendant toute la période de conservation de ces renseignements; ainsi, des mesures de sécurité essentielles à la protection de la vie privée sont mises en œuvre du début jusqu'à la fin. Cela permet d'assurer la conservation sécurisée des données, puis leur destruction sécurisée à la fin de leur période de conservation. Ainsi, la protection intégrée de la vie privée assure une gestion intégrale, sécurisée et debout en bout des renseignements pendant toute leur période de conservation.*

*6. Assurer la **visibilité** et la **transparence.** Grâce à la protection intégrée de la vie privée, tous les intervenants seront assurés que sans égard aux pratiques ou aux technologies employées, le système fonctionne conformément aux promesses et aux objectifs établis, sous réserve d'une vérification indépendante. Les éléments et le fonctionnement du système demeurent visibles et transparents, tant pour les utilisateurs que pour les fournisseurs. La vérification permet d'établir un climat de confiance.*

*7. **Respecter** la vie privée des utilisateurs. Avant tout, la protection intégrée de la vie privée oblige les concepteurs et utilisateurs à privilégier les intérêts des particuliers en prévoyant notamment des mesures strictes et implicites de protection de la vie privée, des exigences appropriées quant aux avis et des fonctions habilitantes et conviviales, axées sur l'utilisateur. »*[219]

L'énumération de ces principes fondamentaux de la *privacy-by-design*, la description qui est faite de leur contenu, confirment le franchissement d'une étape dans un processus de disparition de la protection de la vie par la loi (*Privacy by Law*) au profit de « procédés techniques » ou de « bonnes pratiques ». On peut imaginer alors qu'il sera plus facile d'affirmer, par la suite, le caractère obsolète d'un système juridique dont

219 CAVOUKIAN (A.), *La protection intégrée de la vie privée. Les sept principes fondamentaux*, préc. note 14. Nous grassons.

on n'aura cessé de souligner l'imperfection, l'inefficacité et les entraves qu'il apporte aux activités économiques. Il y a de la ruse dans ce mode de raisonnement et de construction où plane l'ombre de Friedrich Hayek. La question qui devra alors être posée sera celle de l'égalité de l'information et du dialogue dans la relation entre les concepteurs des produits et les clients/usagers soucieux de la protection de leur vie privée mais dont les données personnelles restent un enjeux du commerce international. Il suffit à cet égard de se référer aux enquêtes portant sur la lecture par les consommateurs des politiques de confidentialité des sites pour en avoir une idée[220].

Et à cet égard écrire que « ***dans la mesure du possible***, *il faut restreindre la capacité d'identifier et d'observer les renseignements personnels ainsi que d'établir des liens entre eux* »[221] ou de « *Pratiques équitables en matière de Renseignement (PEMR)* » n'est ni suffisant ni satisfaisant. Ainsi que l'écrivait Henri Lacordaire : « *Entre le fort et le faible, entre le riche et le pauvre, entre le maître et le serviteur, c'est la liberté qui opprime et la loi qui affranchit* »[222]. Malgré son ample diffusion, la *Privacy-by-Design* ne saurait en aucun cas faire l'économie de la *Privacy by Law*.

B) La diffusion du concept de *Privacy-by-design*

Dans une optique marchande anglo-américaine, le respect dû à la rentabilité du processus occupe une grande place. L'on accepterait bien qu'une doctrine existe pour étayer cette approche, mais le discours développé, tautiste, ne saurait être confondu avec une posture doctrinale argumentée. Il y a une volonté de faire de l'*efficience de la privacy* le principal indicateur d'évaluation des projets et des programmes innovants. Les ambassadeurs de la *privacy-by-design* (a) promeuvent leur propre droit (anglo-saxon) sans s'inscrire dans une démarche synthétique, comparatiste ou fédérative. Contrairement à ce qu'ils pourraient laisser croire, le cadre de leur militantisme ne s'inscrit ni dans le darwinisme juridique[223], ni dans la recherche d'un système optimal promouvant l'Etat de droit[224]. Ils évaluent la *privacy-by-design* avec une lumière favorable, pour en conforter et légitimer les principes, en supposant la causalité là où une simple corrélation peine à s'imposer. Las, ce faisant, ils présupposent que la légitimité d'accompagnement de l'activité économique par les grands fonctionnaires l'emporte sur leur légitimité de contrôle ou leur légitimité de proximité[225]. De sorte qu'ils évoluent sur le marché des services juridiques en faisant corps avec l'influence économique, sans préoccupation pour l'assise démocratique des règles juridiques, et en controuvant les mérites de la pensée économique ; loin d'un marché pur dans lequel triomphe le meilleur système, ils imposent un système préfabriqué aux vertus supposés. Leurs relais académiques (b), négligeant l'exigence scientifique de rechercher les tenants et aboutissants de la *privacy-by-design*, se sont contentés de réceptionner l'idée. Leur

220 Voy. les réflexions d'Emmanuelle Lamandé : *Entre industriels avides et utilisateurs résigés, la « privacy-by-design » a encore du chemin à faire*, publié sur le site http://www.globalsecuritymag.fr > Dossiers > Investigations. URL : http://www.globalsecuritymag.fr/Entre-Industriels-avides-et,20111204,27273.html (page vérifiée le 30 juin 2012).
221 CAVOUKIAN (A.), *La protection intégrée de la vie privée. Les sept principes fondamentaux*, préc. Nous grassons.
222 Quarante-cinquième conférence de Notre-Dame. Disponible sur le site http://www.citationspolitiques.com (http://www.citationspolitiques.com/theme.php3?id_mot=66, page vérifiée le 30 juin 2012).
223 Bien qu'à l'instar des auteurs de *Legal Studies*, ils se revendiquent de Friedrich A. Hayek.
224 En ce sens, DELMAS-MARTY (M.), *La refondation des pouvoirs*, Seuil, janv. 2007, spéc. pp. 264 et s., et *Vers une communauté de valeurs ?*, Seuil, fév. 2011, pp. 331 et s., où l'auteure discute les conditions d'émergence de l'Etat de droit à l'échelle globale.
225 ROSANVALLON (P.), *La légitimité démocratique*, Seuil, 2008, 368 p., spéc. pp. 234-238, où l'auteur discute la possibilité de représenter des intérêts futurs auprès des institutions démocratiques élues, et où il souligne le rôle de la société civile dans la construction d'une légitimité réflexive. Pour autant, il se garde bien de franchir le Rubicon d'une légitimité scientiste, qui donnerait au discours techno-scientifique une implantation dans tout système démocratique.

validation académique, si elle renforce le concept selon le programme escompté[226], n'en consiste pas moins à revêtir d'un vernis juridique des pratiques ajuridiques.

3. a. Les ambassadeurs et les missionnaires, de prosélytiques agents de diffusion

La *privacy-by-design* a fait florès grâce à l'activisme du Commissaire Cavoukian, dont la stratégie rhétorique n'est pas exempte de contradiction. L'*Information and Privacy Commissioner of Ontario* s'est ainsi dotée de plusieurs outils de propagande : les plus visibles sont les ambassadeurs, le plus subreptice la revue IDIS (*Identity in the Information Society*).

Présentés comme experts en matière de protection de la vie privée, les ambassadeurs de la *privacy-by-design* constituent un ensemble hétéroclite de figures issues de la société civile comme de la communauté politique : directeurs et/ou chefs de département d'entreprises[227], dont les cabinets d'avocats[228], consultants de *think tanks*[229], businessmen engagés dans la *charity* internationale[230], figures politiques[231], administrateurs de la haute fonction publique[232], universitaires et académiciens[233], … mais aussi des pairs et de proches collaborateurs de Ann Cavoukian[234]. Nettement majoritaires, les membres de la société civile sont issus de firmes très variées, et même parfois concurrentes. Or, cette très grande hétérogénéité d'intérêts et de compétences n'affaiblit en rien la diffusion de la *privacy-by-design* ; au contraire, elle permet de réunir des compagnies désireuses de s'imposer, à moindres coûts, comme autorités d'incontournables sources de normalisation. Agissant en amont de toute certification officielle, ces sociétés privées emploient le concept de *privacy-by-design* comme vecteur d'une *pré-normalisation*, espérant que ses principes gagneront leurs lettres de noblesses comme normes industrielles *de facto*[235]. Non seulement ces ambassadeurs s'inscrivent dans une démarche idéologique expansionniste peu soucieuse de dialogues juridiques interculturels[236], mais de surcroît ils offrent à leurs firmes l'économie d'un processus de normalisation officiel, supposant du temps et des investissements, tels que les normes AFNOR ou ISO. Quant à la minorité des ambassadeurs inscrits dans

226 Voy. http://privacybydesign.ca/about/ambassadors/ (Site : http ::/ /privacybydesign.ca > About PbD > Ambassadors).
227 In extenso, Joseph H. Alhadeff (Oracle), Stephan Brands (Microsoft), Anneke Covell (American Express), Malcolm Crompton (Information Integrity Solution Services), Michelle Dennedy (Sun Microsystems), Khaled El Emam (Privacy Analytics), John Ellingson (Skeptical Systems), Mark Fabro (Lofty Perch), Michael Fertik (Reputation.com), Uwe Findler (PAREXEL International Corporation), Natalie Fonseca (SageScape), Victor J. Garcia et Scott Taylor (Hewlett Packard), Eduard Goodman (IDT911), Michael Ho (Bering Media), David A. Hoffman (Intel Corporation), Jane Horvath (Google), Pat Jeselon (Pat Jeselon & Associated Consulting), Stephen Johns 'Flybits/Ryerson Ubiquitous Computing Group), Nandini Jolly (CryptoMill Technologies), Jeff Jonas et Harriet Pearson (IBM), Krista Jones (MaRS Discovery District), Larry Keating (No Panic Computing), Chris Kelly (Facebook), Chris King (eMeter Strategic Consulting), Karl Martin (Bionym), Gene McLean (McLean Security Advisory & Associates Inc), Terry McQuay (Nimity), Fazila Nurani (PrivaTech Consulting), Claudiu Popa (Informatica Corporation), Doron Rotman (KPMG), Chris Shepherd (ICCT Corp), Yosi Shneck (Société israélienne de distribution d'd'électricité), Arthur Smith (GS1 Canada), Max Snijder (European Biometric Group).
228 Ainsi, Joan Antokol (Park Legal), Carlos Chalico et Christine R. Ravago (Ernst & Young's), Nicola Fabiano (Studio Legale Fabiano), Cristos Velasco San Martin (ProDatMex), Michael Winters (Hydro One Networks).
229 *Ex pluribus*, Martin Abrams ou Jules Polonetsky (Future of Privacy Forum).
230 Ainsi : Noah Lang (Reputation.com), Robert Johnston National (Association for Information Destruction, Inc.).
231 Entre autres, Sa Majesté le Prince Fahad bin Faisal Al Saud (Arabie Saoudite), Jacques Bus (Commission européenne), Alexander Dix (Datenshcutzbeauftrager), The Honourables Pamela Jones Harbour et Mozelle W. Thompson (Commissaires au Commerce, US), Stephen Lau (ancien Commissaire à la vie privée et à la protection des données de Hong Kong), David Nicholl (Ministry of Government Services, Infrastructure Technology Services), Peter Schaar (Landesbeauftrager für Datenschutz und Informationsfreiheit), Marie Schroff (Commissaire à la Vie privée de Nouvelle-Zélande).
232 Thomas Marinelli P. Eng (Ontario Lottery & Gaming Corporation), Norine Primeau-Menzies (Ontario Telemedicine Network).
233 L. Jean Camp (Professeur d'Informatique associé, Université d'Indiana), Daniel Guagnin (Sociologue au Centre for Technology and Society, Technische Universität Berlin), Dimitrios Hatzinakos (Université de Toronto), Masao Horibe (Hitotsubashi University Tokyo), Ana Brian Nougreres (Faculté de Droit d'Uruguay), Konstantinos N. Plataniotis (Knowledge Media Design Institute), Marilyn Prosch (Université d'Etat d'Arizona), Hossein Rahnama (Université Ryerson, Canada), Kai Rannenberg (Institut Goethe de Francfort, Allemagne), Jean-Pierre Seifert (Technische Universität Berlin), Omer Tene (Ecole de Management de la Faculté de Droit, Rishon le Zion, Israël).
234 Ainsi, Anita Fineberg, juriste ayant travaillé durant 7 ans pour elle, ou Robin Gould-Soil, son homologue auprès du *Office of the Privacy Commissioner of Canada*, Yoram Hacohen (Autorité israélienne sur le Droit, l'Information et la Technologie), Peter Hustinx (CEPD), Jeff Kirk, que Mme Cavoukian a formé comme étudiant en Master, Rebecca Wynn (NCI Information System), une interlocutrice régulière d'Ann Cavoukian.
235 Sur la réponse apportée par le droit américain et la FTC, voir la seconde partie de la présente contribution.
236 Sur le contenu, la portée et les difficulté du dialogue interculturel dans la discipline juridique, voy. EBERHARD (Ch.), *Dialogue interculturel, in* ADRIANTSIMABZOVINA (J.), GAUDIN (H.), MARGUÉNAUD (J.-P.), RIALS (S.) et SUDRE (F.), « Dictionnaire des droits de l'homme », PUF, oct. 2008, pp. 280-283.

la sphère publique, il est regrettable que leurs contributions soient revêtues du sceau de leurs chapelles d'origine, dont ils revêtent la légitime autorité, bien qu'agissant en *missi dominici* de l'IPCO. Entre confusion des genres et intérêts incompatibles[237], leur position semble volontairement ambiguë et, partant, écorne leurs obligations éthiques.

Les ambassadeurs ont diffusé leur oracle dans une revue du groupe Springer, aux atours scientifiques savamment choisis : la revue *Identity in the Information Society* (IDIS). Antenne du réseau *European Network on the Future of Identity in the Information Society* (FIDIS), la revue se prétend internationale et interdisciplinaire et visant à promouvoir l'étude de l'identité dans la société de l'information. Elle se donne pour axe central « *the developing relationships between identity, security and privacy in an information-intensive society that in the name of security, better marketing or more efficient delivery of goods and services relentlessly tracks physical persons, their financial transactions, and their healt* ». Conseillers du comité éditorial, Ann Cavoukian et Serge Gutwirth y ont cosigné[238] et parrainé[239] divers articles apologétiques de la *privacy-by-design* dans le numéro 3 de l'année 2010. Or, selon ses éditeurs, James Backhouse, Bert-Jaap Koops, *et* Vashek Matyas, cette revue n'est-elle pas sensée embrasser simultanément « *law, technology, and information systems alongside other social, political and management issues* » ? Non seulement leur traitement complaisant de la *privacy-by-design* enfreint la rigueur et la méthodologie juridiques, mais de surcroît il déconsidère les revues qui, pour être vraiment interdisciplinaires, ne feignent pas de tenir pour du droit ce qui n'en est manifestement pas.

Ces outils de propagande bénéficient également de mesures d'appui disparates et sporadiques, qui se déploient au sein de la communauté scientifique. D'authentiques chercheurs se font, à leur tour, ambassadeurs de la *privacy-by-design*, reprenant en écho ses bienfaits et tentant maladroitement d'en systématiser les aspects juridiques, politiques et sociaux. Hélas, faute de méthode, le chercheur peut se faire pamphlétaire. L'un des plus symptomatiques est Yves Poullet. Celui-ci pose une bonne question :

> « *It was essential that the European debate enlarge the basic protection of data to include the infrastructures and terminals. How can the data be properly protected if the technical solutions do not take into account present-day constraints and transpose them efficiently into regulation?* »[240].

Mais au lieu d'explorer le panel des mécanismes technologiques à disposition, le Pr. Poullet saute immédiatement à la conclusion : « *This approach called 'privacy-by-design' is based on some early thinking in the area first framed in French law in 1978* ». Or, une telle assertion est critiquable à trois points de vue : tout d'abord, il n'est pas avéré que la *privacy-by-design* soit la réponse appropriée au projet d'élargissement de la protection européenne des données. Ensuite, le Pr. Poullet n'explicite pas l'ambivalence planant autour du terme de régulation[241], donnant à penser au chercheur continental qu'un règlement communautaire sera adopté, au chercheur anglo-américain que le secteur privé se dotera de « bonnes pratiques ». Enfin, il semble que l'auteur confonde ici *privacy-by-design* et PET, en prêtant à la première les caractéristiques des secondes.

---

237 SFEZ (L.), *Technique et Idéologie. Un enjeu de pouvoir*, Seuil, 2002, p. 26.
238 Voyez McQUAY (T.) & CAVOUKIAN (A.), *A pragmatic approach to privacy risk optimization: privacy-by-design for business practices*, IDIS n° 3, juill. 2010, pp. 379-396 ; CAVOUKIAN (A.), FISHER (A.), KILLEN (A.) & HOFFMANN (D. A.), *Remote home health care technologies: how to ensure privacy? Build it in:* privacy-by-design, IDIS n° 3, mai 2010, pp. 363-378 ; CAVOUKIAN (A.), TAYLOR (S.) & ABRAMS (M. E.), privacy-by-design: *essential for organizational accountability and strong business practices*, IDIS n° 3, juin 2010, pp. 405-413.
239 HUSTINX (P.), privacy-by-design: *delivering the promises*, IDIS n° 3, mai 2010, pp. 253–255 ; SCHAAR (P.), *privacy-by-design*, IDIS n° 3, avr. 2010, pp. 267-274 ; DAVID (J. S.) & PROSCH (M.), *Extending the value chain to incorporate privacy-by-design principles*, IDIS n° 3, mai 2010, pp. 267–274.
240 POULLET (Y.), *Data protection legislation: What is at stake for our society and democracy?*, computer law & security review vol. 25, 2009, pp. 211–226 ; Voy. également LE MÉTAYER (D.), *privacy-by-design: a matter of choice*, *in* GUTWIRTH (S.), POULLET (Y.) et De HERT (P.), « Data Protection in a Profiled World, 2010, Part 6, pp. 323-334, spéc. p. 323.
241 Qui, dans la langue de Shakespeare, signifie plusieurs choses, allant du règlement (doté d'un effet normatif, *hard law*) au dialogue sociétal ou à la coopération (qui n'est pourvu, au mieux, que d'un effet incitatif, moindre qu'une *soft law*).

De juridico-politique, le propos devient partisan *expressis verbis*. L'on pourrait multiplier les exemples[242].

Étonnante sous la plume d'un universitaire, cette approche juridico-politique se retrouve plus aisément dans l'œuvre législative des institutions de l'Union européenne. L'intérêt pour la *privacy-by-design* est venue de la Commission européenne à travers les technologies renforçant la vie privée *(Privacy Enhancing Technologies)*[243]. Elle a ensuite rayonné auprès des autorités européennes chargées de la protection des données (G29), avant de gagner le débat parlementaire des eurodéputés. L'on peut tout de même s'étonner que l'autorité européenne chargée simultanément de l'*intérêt communautaire*, de la *gouvernance* et de la *concurrence*, mue par une idéologie économique libérale néo-classique[244], demande aux autorités nationales de contrôle de développer les PETs et d'encourager la *privacy-by-design*... Dans son approche, il semble qu'elle ait trouvé fort commode qu'un concept de *privacy-by-design* vienne englober l'ensemble de ces technologies bénéfiques pour la vie privée... au point de confondre les dogmes de l'une et les mérites des autres. S'entremêlent ainsi une politique technologique et une politique juridique, sans beaucoup de clarté. Bien qu'il soit « *difficile de distinguer l'usage de solutions techniques pour régler des problèmes juridiques (…) et l'usage de ces techniques dans le contexte d'une politique juridique déterminée* »[245], le principal problème n'est pas tant celui de la redistribution des rôles et de la décentralisation des actions[246] que celui de l'externalisation de toute responsabilité, au risque de sa désincarnation[247].

L'approche défendue par la Commission présente bien des faiblesses. Relevons, avec le CRID, que « *[l]es conditions techniques de la protection ont une importance croissante et sont un gage d'effectivité du dispositif juridique au point que l'on peut observer un certain déplacement du centre de gravité du droit de la protection des données vers les règles de sécurité comme en témoignent (…) les dispositions de la directive ''vie privée et communications électroniques''* »[248] mais aussi de la proposition de règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données)[249]. Un tel glissement serait anodin s'il n'était commis par l'institution détentrice du monopole d'initiative de la législation de l'Union européenne et susceptible, à ce titre, d'influencer profondément les normes européennes.

Un peu plus vigilant, le Parlement européen a fait évoluer sa lecture du concept de « vie privée dès la conception ». D'une approbation inconditionnelle[250], il s'est ensuite rallié à une position plus nuancée : partant d'un a priori positif[251], il adjoint immédiatement des exigences de transparence, de sécurité juridique

242 Ainsi, le Dr. Parry Aftab (*When your brands matters*, *in* « Privacy-by-Design : the Gold Standards », Toronto, 2010) envisage la *privacy-by-design* comme un label de promotion de ses ambitions de consultance en droit de l'internet et de ses activités entrepreneuriales (WiredTrust.com), ou encore Nicola Fabiano, thuriféraire de la *privacy-by-design* sur son blog.
243 Latent dans la communication de 2003 (COM (2003) 205 final, point 8, *Rapport de la Commission sur la mise en œuvre de la directive 95/46/CE*), cet engouement devient explicite depuis 2007 (COM (2007) 228 final, 2 mai 2007, *Communication au Parlement européen et au Conseil sur la promotion des technologies de promotion de la protection des données (PETs)*). Ces communications sont disponibles sur le site de la Commission (http://ec.europa.eu).
244 S'agissant de la philosophie politique défendue par la Commission européenne, nous nous appuyons sur les travaux de BRACQ (S.), publiés dans la Revue trimestrielle de Droit européen, et de IDOT (L.), dans la revue Europe.
245 BLANDIN-OBERNESSER (A.), *Quelles solutions techniques pour résoudre les problèmes juridiques posés par la technique ?*, *in* LE MÉTAYER (D.) (éd.), « Les technologies de l'information au service des droits : opportunités, défis, limites », Cahiers du CRID, n° 32, Bruylant, 2010, p. 56.
246 *Ibid.*, p. 57.
247 V. *infra*.
248 BLANDIN-OBERNESSER (A.), *Quelles solutions techniques pour résoudre les problèmes juridiques posés par la technique ?*, *op. cit.*,. 48.
249 Commission européenne, 25 janv. 2012, COM (2012) 11 final, 135 p., doc. 2012/0011 (COD), disponible sur la page « Protection des données » du site de la Commission européenne, DG Justice, Droits fondamentaux et citoyenneté (http://ec.europa.eu/justice/data-protection/index_fr.htm).
250 Résolution du Parlement européen du 10 mars 2009 *sur les prochaines évolutions de la gestion des frontières dans l'Union européenne et expériences comparables dans des pays tiers*, doc. A6-0061/2009, 2008/2181(INI), pt. 16 : « *estime que la prise en compte du respect de la vie privée lors de la conception (privacy-by-design) doit figurer à la base de toute initiative lorsqu'elle risque de mettre en danger les données personnelles et d'entamer la confiance du public dans les entités qui les détiennent;* ».
251 Résolution du Parlement européen du 6 juill. 2011 *sur une approche globale de la protection des données à caractère personnel dans l'Union européenne*, doc. 2011/2025(INI) pt 35 : « estime que les concepts de «prise en compte du respect de la vie privée dès la conception» et du «respect de la vie privée par défaut» participent au renforcement de la protection des données et souscrit à leur application concrète et à

et de respect des droits et libertés fondamentaux à la « vie-privée-dès-la-conception »[252]. Ce faisant, il soumet le concept litigieux à l'empire du droit. L'on peut toutefois regretter que, même avec les précautions requises, le Parlement de Strasbourg approuve ainsi la contribution de la *privacy-by-design* à l'accroissement de la protection des données personnelles, sans en débusquer les vicissitudes. Le même regret affectera le CEPD (Peter Hustinx, par ailleurs l'un des ambassadeurs de la *privacy-by-design*) : rattaché au Parlement européen, le CEPD valide le concept d'Ann Cavoukian et lui donne une portée quasi-juridique. Certes, il reconnaît la coparentalité du concept[253], mais, conjointement avec d'autres commissaires chargés de la protection des données et de la vie privée[254], il accepte trop rapidement la poursuite d'autres aspects du processus sans les questionner !

Bref, pour retrouver la qualité scientifique qui fait tant défaut aux apôtres de la *privacy-by-design*, sans doute faut-il se tourner vers les publications scientifiques autour des PETs (*Privacy Enhancing Technologies*). Moins naïfs, les spécialistes et ingénieurs qui évoquent la *privacy-by-design* ont le mérite d'en restituer la paternité à son auteur Marc Langheinrich[255], véritable initiateur du débat autour de la *privacy-by-design*. Ainsi en informatique ambiante[256], en étude des interfaces homme-machine[257], comme en management[258], ils développent une approche de la *privacy-by-design* épurée des préceptes de l'ICPO.

4. b. Les juristes et les prescripteurs : de la communication au droit mou.

La position suiviste de juristes complaisants génère une labellisation juridique de normes sans portée. L'on pourrait aborder leur inclination pour la *privacy-by-design* comme un effet de mode, induit par l'éphémère attrait que suscite un anglicisme flou, donc censément malléable[259]. L'on pourrait voir dans cet emploi une stratégie d'auto-promotion, visant à assurer la notoriété numérique du juriste dans ses activités présentes et futures[260]. L'on pourrait enfin supposer qu'ils sont animés par une finalité louable, savoir la mise en conformité avec les prospectives esquissées par les autorités de régulation européenne[261], ou l'extension de la « juridicité » des droits à la vie privée à la *terra incognita* de la recherche scientifique et de la construction de démonstrateurs technologiques. Cette tendance serait dérisoire si elle ne contribuait

---

leur renforcement ainsi qu'à la nécessité de promouvoir le recours aux technologies renforçant la protection de la vie privée ; (...) ». Cet engouement lui a été principalement inspiré par sa commission du Marché intérieur et de la protection des consommateurs, dans son avis du 14 avril 2011, sur rapport de l'eurodéputé Matteo Salvini (doc. A7-0244/2011, réf. PE460.636v02-00).

252 *Ibid.*, qui se poursuit ainsi : « (…) souligne que toute mise en œuvre du concept de «prise en compte du respect de la vie privée dès la conception» doit reposer sur des critères et des définitions pertinents et concrets afin de protéger le droit des utilisateurs à la vie privée et à la protection des données, et d'assurer la sécurité juridique, la transparence, des conditions de concurrence équitables et la libre circulation; estime que la prise en compte du respect de la vie privée dès la conception devrait reposer sur le principe de la limitation des données, à savoir que tous les produits, services et systèmes devraient être conçus de manière à ne collecter, n'utiliser et ne transmettre que des données personnelles absolument nécessaires pour leur fonctionnement; ».

253 Le CEPD fait ainsi justice à Langheinrich. V. *privacy-by-design: delivering the promises*, préc.

254 Voy. la résolution sur la *privacy-by-design* adoptée à l'occasion de la 32e conférence annuelle des commissaires à la protection des données et de la vie privée, Jerusalem, 27-29 oct. 2010, 2 p.

255 LANGHEINRICH (M.), *privacy-by-design—Principles of Privacy-Aware Ubiquitous Systems, in « Ubicomp 2001: Ubiquitous Computing »*, LNCS: Springer, 2001, vol. 2201/2001, pp. 273–291.

256 LIU (A. X.) & BAILEY (L. A.), *PAP: A privacy and authentication protocol for passive RFID tags*, Computer Communications, vol. 32, 2009, pp. 1194-1199 ; AHAMED (S. I.), LI (H.), TALUKDER (N.), MONJUR (M.), HASAN (C. S.), *Design and implementation of S-MARKS: A secure middleware for pervasive computing applications*, The Journal of Systems and Software, vol. 82, 2009, pp. 1657-1677 ; DRITSAS (S.), GRITZALIS (D.), LAMBRINOUDAKIS (C.), *Protecting privacy and anonymity in pervasive computing: trends and perspectives*, Telematics and Informatics, vol. 23, 2006, pp. 196-210.

257 ABSCAL (J.) & NICOLLE (C.), *Moving towards inclusive design guidelines for socially and ethically aware HCI*, Interacting with Computers, vol. 17, avr. 2005, pp. 484-505.

258 SUBIRANA (B) & BAIN (M.), *Architecting and Managing Virtual Learning Networks: A Business Process orientated Approach to Legal Compliance*, European Management Journal, vol. 21, n° 5, 2003, pp. 598-613.

259 Mireille Delmas-Marty a déjà développé une approche similaire en matière pénale (DELMAS-MARTY (M.), *Le flou du droit*, PUF, 1986, coll. Quadrige, spéc. pp. 245 et s.).

260 L'auto-promotion professionnelle encourageant l'auto-validation conceptuelle et vice-versa. Par exemple FOREST (D.), *Les trois lois du double virtuel*, Expertises des systèmes d'information, n° 361, août 2011, p. 294, singeant Isaac Asimov en proposant trois « lois » de protection et d'orientation de la personnalité à l'ère numérique.

261 Ainsi, l'avocat Guillaume Desgens-Pavanau déplore que la proposition de loi Détraigne-Escoffier ne tienne pas compte des recommandations du groupe de l'article 29, soutenant l'inscription d'une *privacy-by-design* dans une réflexion à moyen terme (DESGENS-PAVARAU (G.), *À propos de la proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique*, Communication Commerce électronique n° 7, juill. 2011, Alerte 7.

pourtant au cautionnement du discours techno-scientifique ainsi tenu[262]. Par leur perméabilité au jargon anglo-américain, ils instaurent une *cosmétique* de la vie privée et fondent une pseudo-caution académique, au lieu d'explorer dans tous ses aspects le dialogue asymétrique entre sciences de l'ingénieur et sciences juridiques.

Loin de constituer une faute scientifique discréditant immédiatement leur commettant, cette complaisance est un élément de la stratégie de diffusion de la *privacy-by-design*. En effet, celle-ci nourrit l'ambition de concilier des champs scientifiques hétérogènes autour du droit à la vie privée, et réconcilier ainsi les scientifiques de toutes origines et de toutes spécialités. Cette inclination œcuménique – impérialiste ? – est clairement revendiquée comme précepte de la *privacy-by-design*[263], et génère en réalité nombre d'incompréhensions et de désaccords. Faisant mine de « juridiciser » ce qui relève en définitive d'une démarche d'accompagnement, ils omettent la véritable garantie *a posteriori* de la vie privée : celle qui relève du contrôle de l'autorité publique en charge de l'intérêt général[264]. Ils ne relèvent aucune contradiction entre la promotion de la *privacy-by-design* et le principe de neutralité technologique de la réglementation[265]. De sorte que, par cette coupable négligence et sous couvert de donner une caution juridique à un procédé de protection partielle et partiale, ils participent *nollens vollens* à la diffusion systématique d'un vernis juridique sur des pratiques mercantiles. Alex Türk, ancien président de la CNIL, l'illustre bien. Analysant la *privacy-by-design* comme un mécanisme technologique au secours de la technologie – et non comme un concept technologique au service du droit – il en souligne les potentialités innovantes[266] mais valide au passage la *privacy-by-design* comme « principe » et « cadre »[267], alors qu'elle recoupe davantage un ensemble de préceptes. Surtout, il ne propose ni définition[268] ni appréciation des risques inhérents à la diffusion de ce concept dans les sciences juridiques. En creux, l'ancien président de l'autorité française de protection des données donne à la *privacy-by-design* un surcroît de crédit au nom d'une efficacité... qui reste à démontrer.

Les discours tenus par ces juristes-relais de la *privacy-by-design* présentent certaines aspérités. La première aspérité a trait à la préférence pour un *« contrôle par réactivité »* plutôt qu'à une « ingérence par anticipation » : ils tiennent pour acquis que le Droit soit intrinsèquement placé dans une position seconde au regard du développement technologique, qu'il ne saurait entraver a priori en aucune manière. Ils tiennent pour libérale toute société dans laquelle le Droit n'empêche ni n'autorise a priori, mais n'intervient que pour

---

262 BENSAUDE-VINCENT (B.), *Les vertiges de la technoscience. Façonner le monde atome par atome*, éd. La Découverte, avr. 2009, coll. Sciences et Sociétés, 228 p.

263 *« There is a need for both privacy and business professionals to consider privacy in a holistic manner »* nous annoncent Pat Jeselson et alii, *in* « A Foundational Framework for a *Privacy-by-Design* Privacy Impact Assessment », nov. 2011, p. 5. Or, le concept de « holisme » est ici profondément ambigü : il désigne une méthode d'approche des faits en science économique et en sociologie (BOUDON (R.) & BOURRICAUD (F.), *Dictionnaire critique de la sociologie*, PUF, 7e éd., juin 2011, 714 p.), mais semble employé par Ann Cavoukian dans une acception exclusivement fédérative.

264 Parmi une littérature abondante, citons RUSSO (C.), *Article 8§1*, *in* PETTITI (L.-E.), DECAUX (E.) & IMBERT (P.-H.), *La Convention européenne des droits de l'homme. Commentaire article par article*, Paris, Economica, 2e éd., 1999, pp. 305 et s. ; SUDRE (F.), *Droit européen et international des droits de l'homme*, Paris, PUF, 2010, 925 p.

265 BLANDIN-OBERNESSER (A.), *Le principe de neutralité technologique*, *in* « Le droit de l'Union européenne en principes. Liber Amicorum en l'honneur de Jean Raux », Rennes, Apogée, 2006, pp. 243-259.

266 *« Ce concept pourrait également sous-tendre de nouvelles approches qualifiées de ''biométries révocables'' qui permettraient de supprimer le risque de repérage, par corrélation, d'un individu qui s'enrôle sur plusieurs dispositifs fournis par un même fabricant. (…) En matière de vidéo-surveillance, le même principe permettrait de concevoir de nouveaux systèmes permettant de flouter automatiquement (ou masquer) les visages ou les corps de personnes filmées selon le besoin. (….) On voit là comment cette technique d'intégration de protection des données dès l'origine offre un cadre intéressant à une conciliation entre les exigences de sécurité collective et de respect de la vie privée et de l'identité des personnes. »* (TÜRK (A.), *La vie privée en péril. Des citoyens sous contrôle*, Odile Jacob, avril 2011, p. 153). L'on notera l'emploi sage du conditionnel présent.

267 *Ibid*.

268 L'auteur mentionne certes la position du G29, mais elle ne constitue pas une définition. Déployant une approche fonctionnelle de la *privacy-by-design*, le G29 *« recommande que les nouvelles technologiques soient conçues avec un paramétrage par défaut favorable au respect de la vie privée, et ce de manière contraignante. Dans son esprit, cela signifie que que la collecte des données devrait être limitée, que les personnes concernées devraient bénéficier d'un bon niveau d'information et disposer de pouvoirs de contrôle plus importants, que les données collectées devraient bénéficier d'un haut niveau de sécurité. »* (*La vie privée en péril. Des citoyens sous contrôle*, *op. cit.*, pp. 152-153).

évaluer et corriger a posteriori[269]. Ce faisant, ils omettent volontiers que chaque règle connaît une trajectoire sociale propre et que chaque liberté, y compris celle de mener des recherches, possède une historicité et une fonction sociales. Partant, leurs interactions ne sauraient se résoudre dans la recherche du seul ordre d'intervention, mais doivent s'analyser comme un processus complexe[270], une internormativité continue[271] et à plusieurs niveaux. Enfin, une telle analyse confond assez nettement la garantie légale comme norme sociale de garantie des tiers et l'interventionnisme de l'Etat comme personne agissante.

La seconde aspérité rejoint ce dernier aspect en développant un discours de tardiveté et d'impuissance de l'Etat devant un outil parfaitement universalisable et, partant, supposé dépasser le cadre de la collectivité nationale pour embrasser l'ensemble des communautés humaines. Contre la dissémination universelle des résultats, nos chercheurs tiennent pour excessivement présents les agents de la puissance publique – malgré la disparition des corps d'expertise de l'Etat – et analyse leur action en terme d'obstruction. Ils ne retiennent du droit qu'un ensemble de verrous qu'il s'agit de lever et un composé de jalons qu'il faut franchir, au bénéfice de tous, et tiennent pour congrue leur propre place dans les processus de découverte... Le calcul de rationalité économique vient d'ailleurs à bout de leurs arguments d'efficience pour écarter la lettre et l'esprit de la loi, prônant une déréglementation et un désengagement public tous azimuts. Or, il fut assez nettement démontré que chacun de ces postulats est faux : la mesure de l'entrave ne dépend pas d'une séparation entre sphère publique ou sphère privée des fonctions (laquelle tend à s'estomper[272]), l'universalité de la découverte scientifique n'est pas acquise dès le début de la recherche[273], et aucune efficience économique n'est retirée d'un désengagement public.

Une troisième aspérité a trait, pour conclure, au satisfecit donné dans le contrôle de l'utilisateur final, qu'il soit spécialiste ou simple citoyen, « normalement averti ». Ainsi, la possibilité de s'opposer à un détournement des données personnelles ou à un mésusage du produit de la recherche leur apparaît, au nom de l'individualisme libéral, comme la garantie optimale du respect de la vie privée. Pour nécessaire qu'elle semble, cette garantie ne paraît guère suffisante. En effet, les personnes concernées par les données et les utilisateurs sont supposés être pleinement informés des risques, totalement réactifs aux errements et entièrement maîtres de la destinée de leurs données, via l'outil technologique. Aux fondements de ce précepte, le dogme de l'infaillibilité technologique suppose un second dogme : celui d'une infaillible réactivité humaine. Dans cette pensée magique, le détournement de traitement sera immanquablement corrigé par un tiers ou bien les risques liés à ce détournement seront immanquablement assumés par des tiers, en dernier lieu l'utilisateur final. Ainsi « *C'est là que réside la principale faiblesse du système qui suppose que les utilisateurs soient avertis, compétents, voire désireux de protéger leurs données, sachant que la propension au dévoilement de la vie privée est forte (…). Le risque est donc de voir émerger une protection au seul bénéfice des initiés, une protection à deux vitesses. Il est aussi de faire passer la protection, du champ de l'obligation à la charge des responsables, à celui d'une option au bénéfice des individus, éventuellement au détriment des dispositions consacrées*

269 Rappelant la distinction entre *régime d'autorisation* et *régime de déclaration* inscrite au cœur des libertés publiques, leur prose aplanit toute la complexité dans la relation entre Droit et technologie. Or, cette simplification est déjà le fruit d'un travail de modélisation de fonctionnement d'une société. Dans ce modèle le processus de découverte scientifique existe et précède la définition légale des notions, en tant que condition d'une authentique liberté.

270 Comme le remarque Danièle Bourcier, *« [c]'est sans doute la particularité des sciences humaines par rapport aux autres sciences d'obliger à réintroduire l'historicité et la spécificité des systèmes sociaux par rapport à l'ensemble de systèmes »* (BOURCIER (D.), *Sciences juridiques et complexité. Un nouveau modèle d'analyse*, *in* « Technologie, Droit et Justice », *Droit et Cultures* n° 61, 2011/1, p. 52).

271 DELMAS-MARTY (M.), *Le relatif et l'universel*, Seuil, 2004.

272 Les réflexions de Jean-Charles Froment développées en matière de vidéo-surveillance peuvent être transposées, *mutatis mutandis* (FROMENT (J.-Ch.), *Le placement sous surveillance électronique comme expression d'un nouveau mode de surveillance sociopolitique : quels nouveaux risques pour les libertés ?*, *in* MAYER (M.), HAVERKAMP (R.) & LÉVY (R.), « Will Electronic Monitoring Have a Future in Europe ? », éd. Iuscrim, Freibourg, 2003, pp. 237 et s.

273 DELMAS-MARTY (M.), *Le relatif et l'universel*, *op. cit.* ; FROMENT (J.-Ch.), *Sécurité, justice et technologies. De quelques enseignements du développement des technologies de contrôle à partir des exemples du placement sous surveillance électronique et de la vidéosurveillance*, Droit et Cultures n° 61, 2011/1, pp. 219-222.

aux droits des personnes concernées par les traitements : droit d'accès, droit d'opposition »[274] mais aussi droit de rectification ou droit de suppression. *« Se profile également une tendance à faire de la personne une co-responsable du traitement lorsque les moyens techniques de réaliser elle-même les obligations qui s'imposent normalement aux responsables de traitements lui sont confiés »*[275]. Allons plus loin : lorsque les moyens techniques existent, l'utilisateur devient seul et unique responsable du mésusage de ses données personnelles, soit *ab initio* par l'onction de la *privacy-by-design*, soit *in fine* par le jeu contractuel. En définitive, le contrôle ultime de l'utilisateur final est présupposé dans la *privacy-by-design*, tandis que le transfert de responsabilités, bien certain, est irréversible.

Loin de constituer une mise en débat scientifique, les discussions mentionnant la *privacy-by-design* apparaissent assez largement comme un lieu de diffusion, voire de propagande, d'un concept dénué de substrat juridique. Les cénacles où ces discussions sont menées ne sauraient conférer à celle-ci la juridicité qui lui fait défaut, sauf à verser dans l'argument d'autorité. Au contraire, ces lieux apparaissent comme autant d'incubateurs où les « ambassadeurs » de la *privacy-by-design* exercent une magistrature d'influence plutôt qu'un magister scientifique. De sorte que nous pouvons observer les ces politiques et académiciens contribuent à enténébrer le débat. Relevons, avec Lucien Sfez[276], qu'ils produisent un discours de rationalisation et de progrès visant la légitimation d'un ordre désiré, plutôt que d'analyser la légitimité et la rationalité intrinsèques des méthodes de la *privacy-by-design*.

II – Une réalité contestable annonciatrice de glissements paradigmatiques ?

Si l'affirmation classique du temps du droit à rebours du temps technologique est devenue un refrain répété *ad nauseam* pour fustiger les cadres législatifs et réglementaires, il demeure que des limites existent, des principes s'imposent. Beaucoup de ceux-ci sont suffisamment compréhensibles pour être intégrés dans une technologie au prix d'un double effort : celui de vouloir les comprendre et celui de les intégrer.

L'amalgame entre vie privée, données personnelles et *Privacy* est courant dans le domaine des technologies de l'information. L'emploi de ce vocable est représentatif d'une somme d'hésitations en matière de technologies de l'information quant au modèle de gestion des données, aux outils confiés à l'utilisateur, et plus généralement au rôle de l'utilisateur.

Alors que la question de base repose sur la possibilité de concevoir des protections de la vie privée pouvant s'appuyer à la fois sur une approche technologique et une approche organisationnelle mises au service du respect des règles applicables, les logiques développées dans les différents « modèles » de promotion de la protection des données personnelles ne reposent pas sur une approche de droits des utilisateurs[277]. Celles-ci devraient pouvoir servir à déterminer ce qui est permis par le Droit, et de fixer les obligations pour ce qui est contraint par le Droit afin de les intégrer dans le processus de développement d'un système d'informations (B). L'action de l'administration américaine et *a fortiori* de la *Federal Trade Commission* [FTC] nous servira de prétexte pour esquisser une approche critique de la compréhension et de l'applicabilité de la *privacy-by-design* sur le territoire de la notion de *Privacy* (A).

274 BLANDIN-OBERNESSER (A.), *Quelles solutions techniques pour résoudre les problèmes juridiques posés par la technique ?*, *op. cit.*, p. 50.
275 *Ibid.*
276 SFEZ (L.), *Critique de la Communication*, préc. ; dans le même sens, *Technique et Idéologie. Un enjeu de pouvoir*, *op. cit.*, pp. 86 et s.
277 Comprenons par là autant de politiques d'accès aux données.

A. Approche critique de la compréhension et de l'applicabilité de la privacy-by-design sur le territoire américain

Au jeu de trouver une des limites de la *privacy-by-design,* il apparaîtrait sans aucun doute qu'en matière de compréhension des procédures et des outils offerts aux usagers résident de grandes carences de vulgarisation. Qu'il soit question de technologies pouvant aider à la sécurisation et à la confidentialité des données, ou des risques encourus par certains actes, l'aléa des usages pose les limites même de l'utilité de ces procédés. Prise sous cet angle, la dimension d'*empowerment* vers l'utilisateur promue par la *privacy-by-design* paraît pour le moins optimiste puisque dépendante totalement de la compréhension de l'environnement sociétal dans lequel devraient prévaloir les principes du Droit.

Le rôle des organes de régulation reste donc primordial dans le choix des méthodes qu'ils promeuvent afin d'assurer la préservation des droits fondamentaux des utilisateurs, que chaque développeur doit en tant que citoyen pouvoir intégrer dans son raisonnement logique.

a. Évolutions de l'encadrement de la *Privacy* aux États-Unis

L'agence fédérale chargée de la régulation du commerce et de la concurrence, a pris l'initiative de promouvoir depuis fin 2010 un *Framework* (cadre de travail) applicable aux activités commerciales susceptibles de collecter, traiter ou valoriser des données personnelles. Loin de se limiter à des précautions techniques ou la promotion d'outils, l'agence propose dans son rapport « *Protecting Consumer Privacy in an Era of Rapid Change* »[278] un ensemble de principes dits « substantiels », parmi lesquels la sécurité des données, des limites de collecte raisonnables, la précision des données, etc.

D'autre part, nous y découvrons la préconisation d'un « *Comprehensive Information Privacy Program* » [CIPP]. Sous ce vocable, on trouve la promotion de l'intégration d'un personnel dédié dans les entreprises, responsable de la formation aux questions liées à la *Privacy*, ainsi qu'aux responsabilités qui en découle pour les utilisateurs. Il est aussi question de prendre en charge l'évaluation et le contrôle des risques en matière de *Privacy* dans les entreprises engrangeant une grande quantité de données d'utilisateurs, sensibles ou non, au travers de ses services. On reconnaît peu ou prou notre Correspondant Informatique et Libertés [CIL] national dans quelques prérogatives, mais il manque encore un texte fondateur comme la loi de 1978 en France pour façonner les limites d'utilisation et de collecte des données.

1. Du côté des utilisateurs

À l'échelle de l'utilisateur, l'ensemble des recommandations promues dans le rapport de la FTC est accompagné par des propositions d'outils de protection de la *Privacy*. Ceux-ci reposent sur une classification fonctionnelle très peu opératoire, voire factice. Aucun outil de gestion et de protection n'est promu en particulier, mais on peut remarquer que les solutions envisagées sont de l'ordre de la compensation de l'intervention du régulateur par le biais d'un outil technique, et de mesures de protection imposées par le législateur de manière plus générale. On retiendra sur la base du *Framework* de la FTC que les PET constituent une catégorie d'outils techniques censés permettre à l'utilisateur de maîtriser sa vie privée[279].

En effet, si l'on suit la catégorisation la plus commune des PET, les technologies dites de « substitution » doivent assurer la protection complète de la vie privée en limitant, voire empêchant toute diffusion de données personnelles. Ces outils de protection des environnements de travail, d'anonymisation

278 *Protecting Consumer Privacy in an Era of Rapid Change. A Proposed Framework for Business and Policymakers*. Disponible sur le site de la FTC (http://www.ftc.gov). URL : http://ftc.gov/os/2010/12/101201privacyreport.pdf
279 *Ibid.* p. 22 et s.

ou de chiffrement des communications peuvent être considérées comme « supplétifs » aux méthodes de protection (comprenez prescriptions légales ou, référentiels validés par les organismes de régulation) que pourraient assurer les Etats, ou plus généralement, les services commerciaux susceptibles d'assurer ce genre de protection.

Les « *Fair Information Practice Principles* » [FIPPs] posent quant à eux les principes d'une collecte respectueuse des règles en matière de données personnelles. Les PET dites « complémentaires » sont les outils de choix, et eux-mêmes des produits devant assurer le respect du cadre réglementaire en offrant un contrôle à la fois à l'utilisateur et aux gestionnaires du système d'informations.

Il est à noter au sujet des techniques dites « supplétives » que certaines d'entre elles peuvent revêtir en fonction de leur usage le rôle de moyen de détournement de méthodes de filtrage mis en place par les entreprises pour protéger et contrôler leur système d'informations, et être utilisés de la même manière par les Etats désirant imposer des règles de surveillance aux frontières de leurs réseaux. On trouve par exemple des outils tels que des proxy « SOCKS v5 » encapsulés dans un tunnel chiffré en SSH, permettant par l'usage de moyens de chiffrement avancés d'outrepasser les règles de sécurité d'un réseau filtrant les contenus ou les accès vers l'Internet. De fait, la nature des activités couvertes par ce type d'outils peut tout à fait être confondue avec un désir de contrevenir au droit, et confondre ainsi la préservation de la collecte excessive, de la propagation, ou du contrôle de ses données avec la dissimulation d'activités répréhensibles.

Le choix proposé reste large, et prend en compte de manière extensive la capacité de l'utilisateur à savoir choisir, user et gérer ces outils à son avantage. Confier la mainmise complète de l'individu sur ses données, ressemble soit à une confiance trop aveugle dans la maîtrise technique des outils par les utilisateurs, ou l'hypothèse que seuls ceux qui en sont aptes le pourront, et laisseront la plus grande masse réduite à rester hors du champ de la maîtrise de ses données, et les laisser entre les mains des exploitants de services.

5. 2. Du côté de la collecte et du backend pour les entreprises

La question de l'intégration du contrôle de la confidentialité et de la conformité des systèmes de traitement de données bute sur un problème technique complexe à résoudre. Beaucoup de restrictions et de limitations fixées par les législations existantes en matière de vie privée et de données personnelles sont de l'ordre des données subjectives (voire d'informations pouvant être déduites, comme la confession, les opinions…[280]). Le désir de produire un système efficace censé assurer le contrôle des données insérées, ou contenues dans un bloc d'informations de manière autonome ou automatisée n'est pas opérationnel.

La complémentarité avec des technologies palliatives à la complexité et à l'étendue de ce que recouvre la vie privée reste le seul recours, qui additionné à un contrôle effectif de l'humain, demeurent les seules réponses crédibles. De fait, il est préconisé par la FTC des pratiques comme la sécurisation des données, le respect de politiques de conservation et d'accès des utilisateurs à leurs données, assurer un souci constant de précision dans les champs de données recueillies, ainsi qu'une limitation de la collecte aux données strictement nécessaires[281].

À l'échelle de l'administration fédérale, il est recommandé de procéder à des « *Privacy Impact Assesment* »[282] [PIA] constituant des études d'impact et de risques en matière de données personnelles. Dans cette première prise de position de la FTC au regard de la *privacy-by-design*, on remarque que les

280 Directive 95/46 précitée, Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF du 7 janvier 1978, p. 227.
281 Voy. *Protecting Consumer Privacy in an Era of Rapid Change...* précité (p. 39 et s.).
282 Sur le même site, voy. : http://www.ftc.gov/os/2004/03/piapublic.pdf (page vérifiée le 30 juin 2012)

préconisations restent pour le moins peu contraignantes, et pour tout dire, laissent planer de sérieux doutes sur leur effectivité réelle. L'histoire a eu raison de ce rapport de la commission au travers d'une des entreprises américaines des plus emblématiques en matière de valorisation des données personnelles comme produit publicitaire : Google.

À l'image de la France et de l'Allemagne, le développement du système d'imagerie cartographique « *Street View* » a posé problèmes au régulateur américain, qui a émis une série de réserves et de demandes visant à assurer une collecte proportionnée de données face aux objectifs commerciaux de la solution[283], et en réclamant l'adoption de bonnes pratiques, dont l'intégration de personnels responsables de la *Privacy* à l'échelle du développement et de la gestion des projets entre autres conseils de former leur personnel au respect de la vie privée.

La remise en question de la politique de Google par la FTC s'est renouvelée à l'occasion du lancement de « *Google Buzz* »[284], dont l'intégration d'office dans le service Gmail a soulevé l'opprobre de la commission fédérale, matérialisée par le dépôt d'une plainte administrative. Le mépris des accords de *Safe Harbor*[285] caractérisé par l'absence d'information des utilisateurs de l'emploi des données (pour lesquelles ce dernier n'a pas consenti à les partager avec un autre service de la marque) a motivé la FTC à contraindre Google d'adopter une charte globale de protection de la vie privée des clients de leurs services. Cette réponse *a posteriori* constitue une correction marginale d'un phénomène remarquable, du fait de la taille de l'entreprise et l'étendue de ses services, mais elle n'apporte pas de réelle garantie générale de conformité face à la croissance de ce marché.

Appliqués à des services similaires hors Etats-Unis (en particulier « Street View » en Allemagne et en France), ces appels à la raison suscitent une responsabilisation des entreprises. Pour autant, ils ne sauraient contraindre de la même manière que les mécanismes de mise en responsabilité des entreprises manipulant des données personnel ou privé.

b. Mouvement des lignes à l'échelle fédérale

Les développements précédents peuvent laisser croire que la FTC, et parfois par extension le *Department Of Commerce* [DOC], sont les principaux garants de la vie privée aux États-Unis. Il est indéniable que l'autorité fédérale de la concurrence représente un acteur de poids sur la question, en particulier pour le respect des accords de *Safe Harbor*, mais son rôle se limite pourtant en matière de vie privée à des préconisations et des actes de corégulation, dépendant beaucoup de la volonté des industriels. Cela laisse planer une attente d'autorégulation des entreprises, perçue comme l'innovation, à la compétitivité économique, et bien sûr, conforme au principe de liberté d'entreprendre.

La FTC est génétiquement programmée par la section 18 du *FTC Act*[286] à ne pouvoir agir qu'en matière de concurrence et de pratiques déloyales touchant les activités commerciales que sous couvert de procédures lourdes et incertaines poussant l'institution à préférer des solutions accommodantes et conventionnelles. L'opportunité de recourir à la *privacy-by-design* comme justification logique apparaît donc toute trouvée pour compenser ce qui peut représenter des pieds de plomb grevant sa capacité d'action.

Bien que les solutions adoptées pour les cas opposant la FTC à Google s'approchent quelque peu des préconisations de la *privacy-by-design*, la réponse fédérale qui se dessine pourrait pourtant marquer un tournant vers la rigueur et la prescription de nouvelles obligations légales.

283 En supprimant et en ne collectant plus par exemple les identifiants des points d'accès WiFi croisés par le véhicule de capture
284 Voy. http://www.ftc.gov/opa/2011/03/google.shtm (page vérifiée le 30 juin 2012).
285 *Safe Harbor Workbook* : http://export.gov/safeharbor/eu/eg_main_018474.asp (page vérifiée le 30 juin 2012).
286 Sur le site de la FTC: http://www.ftc.gov/ogc/brfovrvw.shtm (Accueil > General Counsel > Legal Authority).

1. L'annonce d'une prise de conscience fédérale

Le 23 février 2012, une proposition de la maison blanche intitulée « *Consumer Data Privacy in a Networked World : A framework for protecting privacy and promoting innovation in the global digital economy* »[287] vient trancher, à la fois sur le plan fonctionnel et logique avec la proposition faite au Congrès de légiférer pour la construction d'une « *Consumer Privacy Bill of Rights* », soit une véritable charte des droits fondamentaux de la *Privacy* vouée à pallier aux manques reconnus du système actuel supporté en partie par la FTC. Deux points sont soulevés comme manques fondamentaux devant être corrigés : d'une part l'absence de principes fondamentaux de protection de la vie privée s'imposant au monde économique, et le manque d'engagement des acteurs économiques et industriels dans le règlement des atteintes à la vie privée.

Dans la forme actuelle de cette proposition, la FTC reste le pivot central de la protection de la vie privée, et de son exploitation commerciale. Cité en exemple, l'article 27 de la Directive 95/46/CE[288] est vu de l'autre côté de l'Atlantique comme un cadre permettant d'imposer la loi dans les codes de conduite à l'échelle européenne. Sans endosser des atours rigoristes, la position de la proposition admet les limites de la simple autorégulation et insiste sur l'accompagnement et la validation encadrée des chartes.

Bien que le texte ne représente qu'un embryon de ce que pourrait être, ou ne jamais être cette prise de position politique pour le renforcement de la protection des données des individus, qui combinée avec l'initiative du « *Do Not Track* »[289] (modulo sa réelle réception par l'industrie sous l'impulsion de la FTC qui depuis 2010 s'escrime à voir les grands noms de l'industrie suivre le mouvement) marque l'insuffisance des initiatives d'autorégulation, et l'importance d'imposer à la fois des principes fondamentaux et des pratiques vertueuses par la loi pour dépasser le simple acte de volonté.

Il convient tout de même de remarquer que les droits attribués par cette proposition de *Bill of Rights* conduisent à promouvoir pour les données, ou les agrégations de données : la capacité de contrôle individuel de ses données, la transparence, le respect du contexte des données confiées, la sécurité, l'accessibilité et l'exactitude des données, le respect d'une collecte ciblée, le droit à une réponse responsable des opérateurs face à leurs engagements.

Il transpire de ces recommandations qu'il faille inscrire la doctrine développée dans le *Framework* de la FTC comme base, en relevant chaque fois les limites relatives à la compréhension des outils par les utilisateurs et la réelle transparence des acteurs dans la promotion de ces différents outils devant mettre en confiance et sensibiliser les utilisateurs face à leurs intérêts de préserver leurs données personnelles[290].

2. Le glissement de l'autorégulation à la corégulation encadrée, sans privacy-by-design

Le contrôle individuel apparaît au travers de ce projet comme une approche limitée, et insuffisante devant justifier d'imposer aux entreprises clarté et transparence vis-à-vis des modes d'expression du consentement, et d'information aux utilisateurs. C'est donc bel et bien une recherche de contrainte d'adhésion des entreprises américaines au *Consumer Privacy Bill of Rights* qui est espérée, plus que l'attente d'une prise de conscience générale de tous les enjeux de la vie privée par chaque utilisateur des services.

287 Sur le site de la Maison Blanche : http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (page vérifiée le 30 juin 2012).
288 Dir. 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* (JORF n° L 281 du 23 nov. 1995 pp. 31 – 50). Disponible sur le site Eur-Lex du portail Europa (http://eur-lex.europa.eu). Voy. : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:fr:HTML (page vérifiée le 30 juin 2012).
289 Voy. http://www.ftc.gov/opa/2010/12/privacyreport.shtm (page vérifiée le 30 juin 2012).
290 Voy. à titre comparatif, la politique de protection des données mises en place par la commission européenne: http://ec.europa.eu/justice/data-protection/index_en.htm (Domaines politiques > Justice et droits des citoyens > Protection des données).

La volonté de renforcer des outils juridiques confiés à la FTC dans une voie capacitante[291] en matière de contrôle apparaît d'autant plus clairement, et non plus le maintien d'une simple co-régulation. Ce rapprochement est aussi en cours à l'échelle européenne et française.

Ainsi, l'initiative de réforme de la directive 95/46/CE initiée par la proposition de Règlement[292] relatif à « la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données » a lancé la remise à plat de principes ancrés depuis plus de 17 ans dans les ordres juridiques européens. Bien que critiqué sur quelques aspects par les Etats membres, dont à l'échelle française par le Sénat et l'Assemblée Nationale[293], le projet se présente dans le sens d'une réduction des obligations de déclaration des entreprises, assortie d'un renforcement des sanctions à l'égard des responsables du traitement.

Ensuite par la voix de la Présidente de la CNIL, Madame Falque-Pierrotin, qui via une tribune du 31 mai 2012[294] a exprimé l'engagement de l'autorité française vers la corégulation : *« Certes, nos pouvoirs de contrôle et de sanction sont puissants et nous n'hésitons pas à y avoir recours en cas de besoin. Pour autant, ces instruments coercitifs ne peuvent suffire à mettre ce nouvel univers en état de droit. Face à la complexité de l'écosystème numérique, l'enjeu du régulateur est de construire des relais. La CNIL entend donc s'appuyer davantage sur les acteurs privés et publics afin qu'ils prennent leur part de la charge de la régulation. ».*

La *privacy-by-design* n'apparaît toutefois pas directement dans le discours général tenu par la CNIL en matière de co-régulation, et il paraît très périlleux de chercher des points de jonction entre le développement de cette nouvelle doctrine de coopération avec les acteurs privés et publics sur le plan des recommandations de cette dernière[295].

La nouvelle matrice se profilant du côté des Etats-Unis en matière de protection des données personnelles est à ce stade encore mouvante. Il est pourtant possible, à titre d'indice, de relever qu'aucune référence directe à la *privacy-by-design* ne décore la proposition, pas plus que des chartes en vigueur et publiées se conformant explicitement au bloc de principes promus par la *privacy-by-design.*

L'analyse des risques inhérents à l'exploitation d'une technologie informationnelle doit répondre de la même manière aux règles de sécurité juridique dès la construction de l'outil qu'aux contraintes de normativité technique, et ne pas se contenter d'être un facteur de gestion des puits de données où l'espoir de la compréhension et de maîtrise de l'utilisateur final ne peut être au mieux que présumée. La cape de la *privacy-by-design* ne peut et ne doit, en aucun cas, évoluer en marge du droit, ni supplanter ou suppléer aux règles relatives à la protection de la vie privée; le droit reste un outil de mise en confiance puissant s'il dispose des atours nécessaires à son respect et à son intégration. Non pas comme limite à la technique, mais comme garantie d'un développement vertueux : c'est le choix qui semble se profiler d'un côté et de l'autre de l'Atlantique, où l'on préfèrera la *privacy by law* à la *privacy-by-design*.

B. *Privacy-by-design* ou *Privacy by Law*

Si on se cantonne à l'analyse d'Ann Cavoukian, il paraît délicat de procéder à une analyse croisée de deux notions envisagées comme antagonistes. Selon elle, la *privacy by Law* doit être reléguée au second plan

291 Nous empruntons l'expression à l'économiste Amartya SEN, in *Commodities and Capabilities,* Oxford India Paperbacks, 1987
292 Proposition de Règlement du Parlement européen et du Conseil précitée.

293 En particulier sur la centralisation de l'autorité de contrôle à l'échelle européenne, risquant de supprimer les spécificités de la protection des données personnelles en France, CNIL comprise

294 (page vérifiée le 30 juin 2012).

295 Voy. *Supra* le projet de Règlement général sur la protection des données.

pour lui préférer la *privacy-by-design*. Quant à ses détracteurs, ils soutiennent que la *privacy-by-design* est devenue un « concept-gadget », un slogan superflu... Malgré sa diffusion et malgré la promotion de modes de responsabilisation entrepreneuriale par les instances de régulation, la *privacy-by-design* reste difficile à saisir dans l'esprit d'un juriste. L'entreprise est d'autant plus complexe que la notion même de *privacy* (vie privée) ne cesse d'être reconnue par la doctrine et la pratique internationales.

La notion de vie privée, typiquement franco-européenne, a connu un développement exponentiel. Depuis la loi sur la liberté de la presse[296] de 1881 en France, et son article 31[297] faisant référence expressément à la vie privée, ce concept n'a de cesse d'investir des pans entiers du droit français, et plus globalement du droit européen. Quant à la *privacy* - défendue pour la première fois en 1890 par Samuel D. Warren et Louis D. Brandeis dans un article intitulé « *the right to privacy*[298] » - elle a connu un succès normatif sans précédent allant jusqu'à inspirer les droits européens post Seconde Guerre mondiale[299]. Selon ces auteurs, « *le droit existant offre un principe qui peut être invoqué pour protéger la vie privée de l'individu contre l'intrusion soit d'une presse trop entreprenante, (…), soit du possesseur de tout autre procédé moderne d'enregistrement ou de reproduction de scènes ou de sons. En effet, la protection fournie n'est pas restreinte par les autorités aux cas où un certain média ou une forme particulière d'expression a été adopté, ni aux produits de l'intellect. (...) La circonstance qu'une pensée ou une émotion ait été enregistrée dans une forme permanente rend son identification plus facile et, dès lors, peut être importante du point de vue de la preuve mais elle ne change rien du point de vue du droit au fond* »[300]. Ainsi la *privacy*, le droit au respect de la vie privée et la protection offerte par ce droit le serait pour tout individu peu important la technologie utilisée afin de violer ce droit, et peu important le territoire sur lequel l'individu se trouve.

C'est cette même idée que l'on retrouve dans la Convention européenne de sauvegarde des droits de l'Homme, en son article 8, « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* », ou encore dans l'article 12 de la Déclaration Universelle des Droits de l'Homme, « *Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes* ». Pour autant que l'on se situe au niveau français, européen, canadien ou encore international, la *privacy* et le droit au respect de la vie privée renvoient, dans le domaine des nouvelles technologies à d'autres notions, qui elles aussi méritent d'être définies.

6. a) Données personnelles, renseignements personnels et *privacy*

A l'origine, le droit à la protection des données personnelles est apparu, au niveau européen, comme une déclinaison du droit au respect de la vie privée. On a assisté, par la suite, à une véritable autonomisation du droit à la protection des données personnelles. Par exemple, la Charte européenne des droits fondamentaux du 7 décembre 2000 reconnaît à côté du droit au respect de la vie privée et familiale, garanti par son article 7, un droit à la protection des données à caractère personnel, qui fait l'objet de son article 8 : «

296 Loi du 29 juillet 1881 sur la liberté de la presse, JORF du 30 juillet 1881, p. 4201
297 Article 31 de la loi du 29 juillet 1881 : « Sera punie de la même peine, la diffamation commise par les mêmes moyens, à raison de leurs fonctions ou de leur qualité, envers un ou plusieurs membres du ministère, un ou plusieurs membres de l'une ou de l'autre Chambre, un fonctionnaire public, un dépositaire ou agent de l'autorité publique, un ministre de l'un des cultes salariés par l'Etat, un citoyen chargé d'un service ou d'un mandat public temporaire ou permanent, un juré ou un témoin, à raison de sa déposition. La diffamation contre les mêmes personnes concernant la vie privée relève de l'article 32 ci-après ».
298 WARREN (S. D.) et BRANDEIS (L. D.), *The Right to Privacy* , in Harvard Law Review, Vol. IV, 1890, p.193-220. Pour une traduction en français, réalisée par Françoise Michaut : http://www.cliothemis.com/Traduction-de-Louis-D-Brandeis#nb2
299 Bibliographie sommaire concernant l'essor de la privacy : ARIES (Ph.) et DUBY (G.) (dir.), *Histoire de la vie privée*, Paris, Seuil, 1985; BÉLIVEAU (P.), *Les garanties juridiques dans les chartes des droits*, Montréal, Thémis, 1991, p. 343-348 ; BIOY (X.), *le libre développement de la personnalité en droit constitutionnel (Allemagne, Espagne, France, Italie, Suisse)*, Revue internationale de droit comparé, 1, 2003, p. 123-147 ; RUSSO (C.), *Article 8§1*, préc. pp. 305-306 ;...
300 Op. cit.

1. Toute personne a droit à la protection des données à caractère personnel la concernant. 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante. ». Ce droit démembré de la vie privée doit être transposé par les États membres pour accéder à sa pleine effectivité. « *L'objet des législations nationales relatives au traitement des données à caractère personnel est d'assurer le respect des droits et libertés fondamentaux, notamment du droit à la vie privée reconnu également dans l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et dans les principes généraux du droit communautaire; que, pour cette raison, le rapprochement de ces législations ne doit pas conduire à affaiblir la protection qu'elles assurent mais doit, au contraire, avoir pour objectif de garantir un niveau élevé de protection dans la Communauté*[301] ».

Que l'on se situe dans la sphère internationale, au Canada, en Europe ou en France la protection de la vie privée, des données à caractère personnel ou des renseignements personnels est appréciée. La seule définition de la « donnée personnelle » illustre le degré de précision requis par ces systèmes normatifs. Les données personnelles sont entendues en droit français, comme en droit européen[302] comme « *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne*[303] ». Le système de protection de la vie privée en matière de nouvelles technologies, et plus précisément en matière de données personnelles est assuré à ce niveau par la loi de 1978[304] et la directive européenne précitée, ainsi que l'article 9 du Code civil. Au Canada, le terme « renseignement personnel » s'entend, selon le paragraphe 2 de la Loi sur la Protection des Renseignements Personnels et les Documents Électroniques, de « *tout renseignement concernant un individu identifiable, à l'exclusion du nom et du titre d'un employé d'une organisation et des adresse et numéro de téléphone de son lieu de travail* »[305]. Le paragraphe 4 prévoit que la Loi sur la Protection des Renseignements Personnels et les Documents Électroniques s'applique à toute organisation à l'égard des renseignements personnels « *qu'elle recueille, utilise ou communique dans le cadre d'activités commerciales* » ou « *qui concernent un de ses employés et qu'elle recueille, utilise ou communique dans le cadre d'une entreprise fédérale* ». Selon les juges canadiens, la définition du renseignement personnel donne lieu à une interprétation large : un renseignement concernant un individu identifiable lorsqu'il y a une possibilité sérieuse qu'un individu puisse être identifié au moyen du renseignement, que ce renseignement soit pris seul ou en combinaison avec d'autres renseignements disponibles[306].

Pourquoi vouloir reléguer le droit au second plan des préoccupations de la *privacy-by-design* dès lors que le droit international et européen organise un système juridique clair relatif à la protection des données ? La protection de la vie privée dans le domaine des nouvelles technologies et plus globalement le droit des

301 Considérant n°10 de la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, J.O. n° L 281 du 23 novembre 1995, p. 0031 - 0050
302 Il semble utile de préciser ici que la loi du 6 janvier 1978 est le texte fondateur et primordial de la protection des données à caractère personnel. La Directive européenne 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données (JOCE du 23 11 1995 n°L281/31) reprend les grands principes de cette loi et va plus loin en renforçant notamment le droit des individus
303 Article 2 de la loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF n°182 du 7 août 2004, p. 14063, texte n°2.
304 Loi 78-17 (Informatique et Libertés) précitée.
305 Paragraphe 2 de la loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000 ch. 5.
306 *Gordon contre Canada (Ministre de la santé)*, 2008 CF 258 (CanLII), disponible en anglais, à l'adresse suivante : http://www.canlii.org/en/ca/fct/doc/2008/2008fc258/2008fc258.html

données à caractère personnel est fondée sur l'assurance du respect des libertés et des droits fondamentaux. L'analyse de la vision de la *privacy-by-design* souhaitée par Ann Cavoukian détourne le rôle du droit en le plaçant au second plan, et en rendant les citoyens non plus détenteurs réels de ces derniers, mais comme acteurs en charge de leur propre liberté. Cette vision de la *privacy* ne lasse pas d'interroger sur son caractère utopique.

D'une part, il semble utile de rappeler ici que dans l'opinion publique les nouvelles technologies ne semblent *a priori* poser aucun problème. Bien que certains soient conscients d'une captation des données personnelles par ces dernières, ils restent « *naïfs* »[307] quant à l'utilisation possible de ces données et s'enlisent derrière le poncif du « rien à cacher car rien à se reprocher ». Comment rendre ces derniers acteurs de leur propre liberté dès lors que les dangers pour leur vie privée ne sont pas même perçus ?

D'autre part, *a posteriori*, le rôle du juge dans l'affirmation du droit au respect de la vie privée, et de la protection offerte par ce dernier dans le domaine des nouvelles technologies est fondamental. Rappelons ici le positionnement de la Cour de Justice de l'Union européenne qui a reconnu depuis la fin des années 1960, « *le droit au respect de la vie privée comme un principe général du droit communautaire, car fondé sur la tradition constitutionnelle commune aux États de la CEE, dont elle assure le respect* »[308, 309]. C'est bien à cette étape - lors d'une possible action en justice - que la prégnance du retournement du mécanisme de la responsabilité au profit du secteur industriel, évoquée plus haut, apparaît. Comment pourrait-on garantir le respect du droit à la vie privée si le secteur industriel pouvait se cacher derrière la (bonne pratique de) mise en œuvre effective de tel ou tel procédé technique prenant en compte la vie privée intégrée dès la conception d'une nouvelle technologie ? Le risque d'une modification insidieuse du régime de la responsabilité incombant désormais à l'utilisateur final est présent mais ce n'est pas le seul problème : *quid* de la charge de la preuve, qui pourrait être en ce cas une sorte de *probatio diabolica* impossible à rapporter par ce dernier.

Enfin, il semble utile de rappeler ici qu'au niveau international, les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel ont été adoptées en tant que recommandation du Conseil de l'OCDE, le 23 septembre 1980[310]. Cette Recommandation, traduisant un consensus international, définit des principes directeurs pour la collecte et le traitement d'informations de caractère personnel[311]. Ces principes ont été formulés de manière suffisamment générale pour s'adapter à l'évolution technologique. Ils englobent tous types de supports pour le traitement informatique de données concernant des individus (de l'ordinateur local aux réseaux aux ramifications mondiales), toutes sortes de traitements de données personnelles (de la gestion du personnel à la compilation de profils de consommateurs) et toutes catégories de données (des données de trafic aux données de contenu, des plus banales aux plus sensibles)[312].

---

307 Expression utilisée par Monsieur Alex Türk pour désigner des « citoyens sous contrôles » dans son livre intitulé, *La vie privée en péril, des citoyens sous contrôle*, ed. Odile Jacob, 2011

308 Affaire 29/69 du 12 novembre 1969 *Erich Stauder contre Ville d'Ulm*. Et par la suite : affaire 11/70 du 17 décembre 1970 *Internationale Handelsgesellschaft*, ou encore affaire 4/73 du 14 mai 1974 *Nold*.

309 Il est nécessaire de rappeler ici le rôle de l'article 9 du Code civil Français : *« chacun a le droit au respect de sa vie privée »*.

310 Disponible sur le site de l'OCDE à l'adresse suivante : http://www.oecd.org/document/18/0,2340,fr_2649_34255_1815225_1_1_1_1,00.html

311 L'OCDE a été la première organisation internationale à promouvoir, dès 1980, une politique internationale pour la protection de la vie privée eu égard au traitement informatique de données. Vers la fin des années 70, l'OCDE a identifié les traits communs des démarches adoptées par les divers pays dans ce domaine et défini certains intérêts ou valeurs de base couramment considérés comme des composants élémentaires des droits des personnes à l'égard du traitement de leurs informations personnelles.Les principes identifiés dans les Lignes Directrices traduisent les droits et obligations des individus vis à vis des traitements informatiques de données les concernant, et les droits et obligations des responsables des traitements. Elles s'appliquent aux données de caractère personnel dans les secteurs public et privé qui, compte tenu de leur mode de traitement, de leur nature ou du contexte dans lequel elles sont utilisées, comportent un danger pour la vie privée et les libertés individuelles, et sont applicables à l'échelle nationale et internationale.

312 Pour rappel, ces Lignes Directrices comportent les principes fondamentaux suivants, applicables au plan national :
- Principe de la limitation en matière de collecte : Il conviendrait d'assigner des limites à la collecte des données de caractère personnel

La mise en œuvre de ces principes au plan intérieur doit être établie en suivant des procédures juridiques, administratives et autres ou des institutions pour protéger la vie privée et les données personnelles, en particulier en « adoptant une législation nationale appropriée ; [en] favorisant et soutenant des systèmes d'auto-réglementation, qu'ils revêtent la forme de codes de déontologie ou d'autres formes ; [en] permettant aux personnes physiques de disposer de moyens raisonnables pour exercer leurs droits ; [en] instituant des sanctions et des recours appropriés en cas d'inobservation des mesures mettant en oeuvre les principes, [et en] veillant à ce que les personnes concernées ne fassent l'objet d'aucune discrimination inéquitable.

Ces principes, technologiquement neutres, sont toujours largement utilisés, dans le secteur public et privé, et figurent dans un grand nombre d'instruments nationaux et internationaux. Ces derniers continuent d'ailleurs à influencer la protection de la vie privée dans les tentatives de législations récentes. Pour preuve, faisant écho à la lettre d'indignation des procureurs de trente-six états américains face à la nouvelle politique de confidentialité de Google[313], la Maison Blanche a présenté, en février 2012, un projet de loi pour la protection de la vie privée des consommateurs dans un monde désormais connecté[314]. Cette proposition s'inspire directement des principes issus des lignes directrices de l'OCDE précitée ; ces derniers étant repris dans leurs grandes lignes dans le projet de loi américain[315]. L'exemple américain témoigne d'une ambition internationale de « *promouvoir et de stimuler une croissance économique et une prospérité durables* ***par des environnements politiques et réglementaires*** *qui favorisent l'innovation, l'investissement et la concurrence dans le secteur des technologies de l'information et de la communication* »[316], selon la déclaration de Séoul sur *le futur de l'économie Internet* en juin 2008, proclamée sous l'égide de l'OCDE, et réaffirmée lors de la réunion à haut niveau de cette même organisation sur l'économie Internet en juin 2011.

---

et toute donnée de ce type devrait être obtenue par des moyens licites et loyaux et, le cas échéant, après en avoir informé la personne concernée ou avec son consentement.
- Principe de la qualité des données : Les données de caractère personnel devraient être pertinentes par rapport aux finalités en vue desquelles elles doivent être utilisées et, dans la mesure où ces finalités l'exigent, elles devraient être exactes, complètes et tenues à jour.

- Principe de la spécification des finalités : Les finalités en vue desquelles les données de caractère personnel sont collectées devraient être déterminées au plus tard au moment de la collecte des données et lesdites données ne devraient être utilisées par la suite que pour atteindre ces finalités ou d'autres qui ne soient pas incompatibles avec les précédentes et qui seraient déterminées dès lors qu'elles seraient modifiées.
- Principe de la limitation de l'utilisation : Les données de caractère personnel ne devraient pas être divulguées, ni fournies, ni utilisées à des fins autres que celles spécifiées conformément (au principe de spécification des finalités), si ce n'est :
a) avec le consentement de la personne concernée ; ou
b) lorsqu'une règle de droit le permet.
- Principe des garanties de sécurité : Il conviendrait de protéger les données de caractère personnel, grâce à des garanties de sécurité raisonnables, contre des risques tels que la perte des données ou leur accès, destruction, utilisation, ou divulgation non autorisés.
- Principe de la transparence : Il conviendrait d'assurer, d'une façon générale, la transparence des progrès, pratiques et politiques, ayant trait aux données de caractère personnel. Il devrait être possible de se procurer aisément les moyens de déterminer l'existence et la nature des données de caractère personnel, et les finalités principales de leur utilisation, de même que l'identité du maître du fichier et le siège habituel de ses activités.
- Principe de la participation individuelle : Toute personne physique devrait avoir le droit :
a) d'obtenir du maître d'un fichier, ou par d'autres voies, confirmation du fait que le maître du fichier détient ou non des données la concernant ;
b) de se faire communiquer les données la concernant ; dans un délai raisonnable ; moyennant, éventuellement, une redevance modérée ; selon des modalités raisonnables ; et sous une forme qui lui soit aisément intelligible ;
c) d'être informée des raisons pour lesquelles une demande quelle aurait présentée conformément aux alinéas (a) et (b) est rejetée et de pouvoir contester un tel rejet ; et
d) de contester les données la concernant et, si la contestation est fondée, de les faire effacer, rectifier, compléter ou corriger.
- Principe de la responsabilité : Tout maître de fichier devrait être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus.
313 Document disponible à l'adresse suivante : http://epic.org/privacy/google/20120222-Google-Privacy-Policy-Final.pdf
314 *Consumer Data Privacy In a Networked World : A framework for protection privacy and promoting innovation in the global digital economy*, February 2012, The White House, Washington.
315 Les principes contenus dans le projet de loi américain : « individual control », « transparency », « respect for context », « security », « access and accurancy », « focused collection », « accountability »
316 Nous grassons.

Bien que le système légal de protection des données personnelles puisse sembler imparfait au vu de la spécificité des nouvelles technologies, et du fait d'un environnement immatériel transnational, les règles juridiques actuelles fournissent une réponse claire et ont vocation à s'appliquer. La *privacy-by-design* ne peut supplanter les règles relatives à la protection de la vie privée édictées par l'Etat. Ce dernier, garant des droits et libertés de ses citoyens, doit adopter toute loi propice à interdire le traçage ou la typologie numériques illégales.

7. b) L'interdiction de tracer, de typer... par la loi

L'idée d'une protection de la vie privée dès la conception des nouvelles technologies n'est pas propre à Ann Cavoukian. L'article 17 de la directive relative à la protection des données fait obligation au responsable du traitement de mettre en œuvre les mesures techniques et d'organisation appropriées pour assurer un niveau de sécurité approprié au regard de la nature des données et des risques présentés par leur traitement. Un rapport de la Commission européenne du 15 mai 2003 sur la mise en œuvre de cette directive[317], et une communication de la Commission au Parlement européen et au Conseil visant à promouvoir la protection des données par les technologies renforçant la protection de la vie privée[318] viennent tous deux encadrer le concept de « *Privacy enhancing technology* ». La communication précitée est claire sur le sujet : « *Une étape supplémentaire sur la voie de l'objectif que poursuit le cadre juridique, à savoir limiter le traitement des données à caractère personnel et recourir autant que possible, à des données anonymes ou à des pseudonymes, pourrait être favorisée par des dispositifs appelés «technologies renforçant la protection de la vie privée», qui contribueraient à garantir que les infractions aux règles de protection des données et les violations des droits des individus soient des actes non seulement interdits et passibles de sanctions, mais aussi techniquement plus compliqués*[319] ». Pour autant, à l'opposé d'Ann Cavoukian, le droit est au cœur de cette analyse. « *Les technologies renforçant la protection de la vie privée doivent être mises en œuvre conformément à un cadre réglementaire, qui comporte des règles applicables de protection des données offrant à tous les individus plusieurs niveaux négociables de protection de la vie privée. Le recours à ces technologies ne signifie pas que les opérateurs peuvent être exemptés de certaines de leurs obligations légales (par exemple, celle de permettre aux particuliers d'accéder à leurs données)*[320] ». Plus récemment cette exigence de prise en compte de standards clairs, s'appuyant sur le droit, pour la *privacy-by-design* a été reformulée par le Parlement européen[321].

Une telle exigence est induite également par une autre idée : le droit à la vie privée demeure un droit subjectif, représentant un « intérêt juridiquement protégé »[322], qui ne devient effectif qu'à la condition d'être activement revendiqué par ses détenteurs[323]. Appliquant cette définition aux droits fondamentaux, Jellinek distingue deux types de droits de l'homme: les droits-libertés ou « *droits de statut négatif* », qui ne requièrent

317 Rapport de la Commission des communautés européennes du 15 mai 2003, *Premier rapport sur la mise en œuvre de la directive relative à la protection des données (95/46/CE)*, COM (2003), 265 final.
318 Communication de la commission au parlement européen et au conseil, *Promouvoir la protection des données par les technologies renforçant la protection de la vie privée*, du 2 mai 2007, COM (2007), 228 final.
319 *Op. cit.* p. 4.
320 *Op. cit.* p. 6
321 Résolution du Parlement européen du 6 juillet 2011 sur une approche globale de la protection des données à caractère personnel dans l'Union européenne. Le point n° 35 de cette résolution est très clair sur ce point. Le parlement européen « *estime que les concepts de «prise en compte du respect de la vie privée dès la conception» et du «respect de la vie privée par défaut »* participent au renforcement de la protection des données et souscrit à leur application concrète et à leur renforcement ainsi qu'à la nécessité de promouvoir le recours aux technologies renforçant la protection de la vie privée; souligne que toute mise en œuvre du concept de « *prise en compte du respect de la vie privée dès la conception» doit reposer sur des critères et des définitions pertinents et concrets afin de protéger le droit des utilisateurs à la vie privée et à la protection des données, et d'assurer la sécurité juridique, la transparence, des conditions de concurrence équitables et la libre circulation; estime que la prise en compte du respect de la vie privée dès la conception devrait reposer sur le principe de la limitation des données, à savoir que tous les produits, services et systèmes devraient être conçus de manière à ne collecter, n'utiliser et ne transmettre que des données personnelles absolument nécessaires pour leur fonctionnement.* »
322 Définition du droit subjectif donnée par Ihering.
323 Le droit subjectif deviendrait alors, selon Jellinek, « un intérêt protégé par la reconnaissance de la faculté humaine de vouloir ». JELLINEK (G.), *La déclaration des droits de l'Homme*, 1904.

pour s'exercer qu'une protection de l'Etat, et les droits-créances ou « *droits de statut positif* »qui impliquent à la fois une revendication active des sujets de droit et une intervention de l'État agissant au titre de débiteur. Appliquée à la prise en compte de la vie privée dès la conception, l'analyse couplée de Ihering et Jellinek des droits fondamentaux et de la vie privée démontre que l'acteur principal dans la garantie des droits est bel et bien l'État dans son rôle de législateur, mais aussi dans son rôle de garant des droits fondamentaux. Afin de mieux appréhender cette analyse et sa conséquence principale (le rôle prépondérant de l'État), il est nécessaire de revenir sur la définition même du droit subjectif.

Dans le langage juridique, le droit subjectif est une prérogative attribuée à un individu dans son intérêt lui permettant de jouir d'une chose, d'une valeur ou d'exiger d'autrui une prestation. Autrement dit, il est une faculté individuelle que certaines règles de droit relevant du droit objectif reconnaissent à une personne, lui conférant un bienfait, et dont le titulaire maîtrise l'usage. Le droit objectif, quant à lui, est l'ensemble des règles qui tendent à la régulation des comportements humains, à la vie en société, et qui bénéficient de la contrainte étatique, qui sont sanctionnées par la puissance publique. On le comprend bien ici, la vie privée, étant un droit subjectif, son titulaire pourra décider librement de le mettre ou non en œuvre ; mais, en cas de violation de ce dernier, il sera sanctionné par un droit objectif, impliquant l'intervention de la puissance publique, de l'État.

En qualité d'acteur principal en ce domaine, ce dernier doit être le moteur d'une convergence des systèmes juridiques en matière de protection de la vie privée, ou du moins, a un rôle à jouer dans la définition de standards internationaux dans le domaine de la protection des données personnelles. On l'a vu plus haut, les notions de renseignements personnels, propre au droit canadien, et celle de données personnelles, propre à l'analyse franco-européenne sont proches. La loi canadienne, relativement récente, semble même inspirée du droit européen, ou du moins tente de s'en rapprocher. C'est d'ailleurs ce que l'on peut comprendre sur le site internet du secrétariat du Conseil du Trésor du Canada : « *la vie privée est un concept important au 21e siècle, et ce, pour différentes raisons. L'une d'elle est économique. Avec la Communauté européenne (CE) qui ne cesse de croître, le Canada doit adopter des normes sur la vie privée afin de pouvoir établir des relations commerciales avec les pays membre de la Communauté européenne* »[324]. Aussi, les standards internationaux, nécessaires à la convergence des systèmes juridiques en la matière, existent déjà via l'édiction et la diffusion des Lignes directrices de l'OCDE concernant la protection de la vie privée et les flux transfrontières de données issues des technologies de l'information et de la communication. Ces standards correspondent à un double objectif : promouvoir l'innovation et la croissance économique liées aux technologies de l'information et de la communication tout en donnant sa juste place au Droit[325]. Les principes issues des lignes directrices de l'OCDE paraissent clairs quant à leurs buts légaux. D'une part, l'accent est mis sur l'importance de l'interdiction de tracer, de typer les citoyens, via notamment les principes de qualité des données et de spécification des finalités. D'autre part, l'OCDE insiste sur la place de l'Etat en tant que détenteur des pouvoirs de régulation et de sanction. Le récent projet de loi américain sur la protection de la vie privée dans un monde connecté[326] en est d'ailleurs le reflet - la conclusion de ce projet de loi déclare que les Etats-Unis s'engagent en tant que démocratie à protéger la vie privée. L'affaire Megaupload, quant à elle, en est une parfaite illustration. Il est néanmoins nécessaire d'atténuer le propos lorsque l'on confronte ces

324 http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/course1/mod1/mod1-4-fra.asp

325 Le communiqué sur les principes applicables à la politique de l'Internet, issue de la réunion à haut niveau de l'OCDE du 28-29 juin 2011 reflète d'ailleurs parfaitement cette idée : *« Pour encourager l'investissement et l'innovation dans sur le marché Internet, il faut que les droits définis par la loi, notamment ceux des internautes, soient clairement définis et protégés par un processus robuste et équitable, compte tenu de la nécessité pour les gouvernements de faire respecter le droit applicable. Il importe à cet égard que les gouvernements travaillent avec l'industrie et la société civile pour promouvoir le respect du Droit et la protection des droits fondamentaux. »*

326 *Consumer Data Privacy In a Networked World*, préc.

principes à la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Ce texte est l'aboutissement d'un processus initié en 2009, notamment par la Commission. Son objectif est « *de doter l'Union d'un cadre juridique plus solide et plus cohérent en matière de protection des données, assorti d'une application rigoureuse des règles, afin de permettre à l'économie numérique de se développer sur tout le marché intérieur et aux personnes physiques de maîtriser l'utilisation qui est faite des données les concernant, et de renforcer la sécurité juridique et pratique pour les opérateurs économiques et les pouvoirs publics* ». L'harmonisation proposée par la Commission européenne pose quelques problèmes. Le règlement européen, d'application directe, ne permettra pas aux États membres d'adopter des dispositions plus favorables[327], or comme le rappelle un rapport du Sénat Français[328], « *s'agissant d'un domaine dans lequel l'atteinte portée aux droits fondamentaux d'une personne peut être considérable, l'harmonisation proposée ne doit s'effectuer que dans le sens d'une meilleure protection des personnes. Elle ne saurait, pour cette raison, priver les États membres de la possibilité d'adopter des dispositions nationales plus protectrices* »[329]. Les récentes tentatives de législations (européenne et américaine) ont le mérite de démontrer, même si elles semblent contradictoires dans leurs effets potentiels, que l'effectivité de la *privacy by Law* est conditionnée par le rôle prépondérant de l'Etat, dans son pouvoir de régulation, mais aussi de sanction. Quant à elle, la *privacy-by-design* n'est pas un objet juridique. Si on devait l'analyser comme tel, cette notion pourrait être au mieux une obligation de résultat pesant sur le secteur industriel ; ou au minimum, une obligation de sécurité de moyen, au pire une obligation de sécurité de résultat. Là encore, le droit viendra assurer le respect de la vie privée et sanctionner sa violation *à posteriori* au niveau national[330], européen[331], et / ou international[332]. Toutefois, si le juge est considéré comme le gardien des libertés, l'État, lui, doit agir comme le garant de ces dernières. Rappelons ici, l'article 16 de la Déclaration des Droits de l'Homme et du Citoyen de 1789 : « *toute Société dans laquelle la garantie des Droits n'est pas assurée, ni la séparation des Pouvoirs déterminée, n'a point de Constitution* ».

La *privacy-by-design* voudrait rendre le citoyen « *naïf* »[333] acteur de sa propre liberté, voire le transformer, à son tour, en « idiot utile ». Or ceci n'est possible que sous la double condition du respect de standards et de normes internationales de protection de la vie privée mais aussi d'une sensibilisation forte aux problèmes liés aux nouvelles technologies. Le citoyen ne doit pas être au service de l'informatique, « *l'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* »[334]. C'est dire combien, à l'opposé de toute *privacy-by-design*, il importe de revenir aux fondamentaux.

Lille, le 26 juin 2012
Université Lille-Nord-de-France

327 On pense ici notamment aux articles 19 et 20 du règlement européen qui, confrontés à l'article 8 de la Charte européenne des Droits Fondamentaux, attestent d'un affaiblissement de la protection en matière de données à caractère personnel.
328 Rapport fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) sur la proposition de résolution européenne de M. Simon SUTOUR, présentée au nom de la commission des lois, en application de l'article 73 quinquies du Règlement, sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (E 7055), 29 février 2012
329 *Op. cit.*
330 On pense ici, en France, à l'article 9 du Code civil : « Chacun a le droit au respect de sa vie privée », mais aussi et surtout à la loi informatique et libertés
331 Directive précitée
332 La Convention européenne des droits de l'Homme et plus précisément, son article 8.
333 Op. Cit.
334 Article 1er de la loi informatique et libertés de 1978.