

## **Programa “OBSERVATORIO JURÍDICO”**

### **Entregable 3ª fase**

**Informe sobre tendencias 2013 con recomendaciones de generación de trabajo.**

**Equipo de trabajo: María José Viega,  
Marcelo Bauzá, Laura Nahabetian,  
Beatriz Rodríguez, Flavia Baladán,  
Jimena Hernández.**

## **A – Introducción**

El Grupo culmina su actividad anual presentando el siguiente reporte de tendencias y recomendaciones de trabajo.

Se trata de un documento que cierra un primer ciclo de actividades y propuestas que, en conexión a los restantes documentos del Programa entregados a lo largo de 2013, permite aquilatar las proyecciones del Observatorio Jurídico hacia el porvenir, en términos de “tendencias” y “recomendaciones”.

El desarrollo efectuado permite destacar:

- Tres tendencias que, por amplitud de rango, cabe clasificar como generales.
- Veinte tendencias de índole particular o sectorial, de las cuales se han seleccionado tres, recomendando su futuro seguimiento y profundización con mayor detenimiento.

La riqueza y variedad de los trabajos cumplidos ha permitido abordar una multiplicidad de asuntos atinentes a las áreas y cometidos sobre los que la Agencia tiene especialidad y competencia, mostrando cuál es el estado y perspectivas esperables de estos temas en el futuro inmediato.

En un mundo dinámico y dinamizado por las TIC, estar al corriente de tendencias así como seleccionar algunas para una mayor focalización, parecen ser factores destacados al servicio de elegir caminos y opciones a recorrer. Es aspiración del Grupo que, los trabajos y análisis practicados, ayuden en el trazado de las políticas y lineamientos estratégicos futuros de la Agencia.

## **B - Tendencias generales**

**1. PROMOCIÓN del desarrollo inclusivo y participativo, de modo armónico con las crecientes demandas de transparencia y rendición de cuentas.**

Si hubiere que marcar un grado de importancia, la expresada constituye una tendencia de primer orden, que forma parte del marco fundamental en la materia, poniendo el acento en dos factores a igual título de relevancia.

Su adopción, cuidado y respeto son de rigor, por considerarse líneas maestras adoptadas por aquellos países que han resuelto poner en práctica unas políticas firmes y prevalentes en el área del gobierno electrónico y la sociedad de la información.

No es un dato menor que el “E-GovSurvey 2012” destaque este singular binomio (desarrollo inclusivo y participativo, transparencia y rendición de cuentas) advirtiendo y alentando la sinergia que se genera en torno al mismo, de cuyo resultado simbiótico emerge el pilar que legitima las citadas políticas: *“La función cada vez más importante del gobierno electrónico en la promoción del desarrollo inclusivo y participativo ha ido de la mano con las crecientes demandas de transparencia y rendición de cuentas en todas las regiones del mundo. El gobierno electrónico ha cambiado en gran medida las expectativas de lo que los gobiernos pueden y deben hacer, al valerse de modernas tecnologías de la información y las comunicaciones para fortalecer los servicios públicos y el desarrollo equitativo centrado en las personas.”*<sup>1</sup>

La cuestión del desarrollo sostenible no es ajena, tampoco, a esta consideración de fundamentos cruciales apreciables en la base de toda política de gobierno electrónico, para poner en práctica de un modo eficaz (inclusión, participación, transparencia, rendición de cuentas). Sobre el punto, el citado informe destaca esta relación y consecuente tendencia: *“... se ha dado una creciente convicción de que los esfuerzos para lograr un acercamiento holístico de la gobernanza del desarrollo sostenible requieren un planeamiento nacional estratégico para asegurar eficacia, transparencia, capacidad de respuesta, participación e inclusión en la prestación de los servicios públicos.”*<sup>2</sup>

---

<sup>1</sup> “Estudio de las Naciones Unidas sobre el Gobierno Electrónico, 2012. Gobierno electrónico para el pueblo” (versión en español). Consultable en: [http://www.unpan.org/egovkb/global\\_reports/08report.htm](http://www.unpan.org/egovkb/global_reports/08report.htm) pág. iii (Prefacio).

<sup>2</sup> “Estudio de las Naciones Unidas...” pág. 2.

El mismo acento, aunque ya no tanto en los dos polos de la ecuación sino en el primero de ellos (inclusión y participación), surge de documentos regionales de primer orden, reafirmando la precitada tendencia: *“Lineamiento: considerar el gobierno electrónico como una obligación de los gobiernos para con sus ciudadanos. Prioridad: alcanzar un gobierno electrónico transaccional y participativo”*.<sup>3</sup>

## **2. REDUCCIÓN de la brecha digital y aumento del acceso a los servicios públicos en poblacionales vulnerables y comunidades alejadas.**

En este punto la línea directriz es clara y contundente, marcando una tendencia que ha pasado a ser eje fundante y vertebral del gobierno electrónico.

Se ha dicho al respecto lo siguiente: *“La transformación de la brecha digital en beneficios digitales para el desarrollo del pueblo requiere un enfoque directo y específico en los grupos vulnerables por parte del gobierno electrónico. Tal enfoque no acepta la formulación de políticas de gobierno electrónico unilaterales ni fragmentadas”*.<sup>4</sup>

El fenómeno reviste múltiples contornos y oportunidades a aprovechar. Se señala, por ejemplo. *“Las nuevas habilidades y el nuevo capital social que han de crearse están mucho más relacionados con la influencia creciente de los medios de comunicación social en línea. Los medios de comunicación social incluyen y captan grupos sociales más diversos en la fijación de las políticas. Los conocimientos técnicos específicos más bajos que se necesitan para ingresar información en estos medios puede ser una ventaja para los grupos vulnerables”*.<sup>5</sup>

Finalmente se ha advertido acerca del criterio adecuado que debe

---

<sup>3</sup> Plan de Acción ELAC 2015. Consultable en <http://www.eclac.cl/cgi-bin/getprod.asp?xml=/elac2015/noticias/paginas/9/44209/P44209.xml&xsl=/elac2015/tpl/p18f.xsl&base=/elac2015/tpl/top-bottom.xsl>

<sup>4</sup> “Estudio de las Naciones Unidas...” pág. 120.

<sup>5</sup> “Estudio de las Naciones Unidas...” pág. 121.

imperar en la materia, a fin de no dejarse llevar por indicadores absolutamente insuficientes cuando se trata de cuantificar al abatimiento real de la manida brecha. Muestra de esta necesaria visión es la siguiente transcripción: *“La brecha digital ya no se limita a contar líneas telefónicas o suscripciones a teléfonos móviles por cada 100 habitantes. Consiste en quién posee la habilidad y medios para acceder a la información y utilizarla luego para crear nuevos contenidos e interactuar con otras personas para satisfacer mejor sus necesidades y aspiraciones. Para reducir este tipo de brecha es necesario que las economías sólidas y los sistemas de gobernanza vigorosos pongan acento directo en los grupos vulnerables, incluidas las específicas desventajas que ellos enfrentan y las contribuciones únicas que ellos pueden hacer para reducir la brecha digital. El gobierno electrónico debe tener en cuenta el arnés de capacidades de las personas a fin de abordar esta cuestión eficazmente en miras de apuntalar el desarrollo sostenible para el pueblo”.*<sup>6</sup>

### **3. PROFUNDIZACIÓN de la e-administración y la i-administración.**

De acuerdo con el conocido estudio de Capgemini encargado por la Comisión Europea<sup>7</sup>, existen cuatro niveles (stages) de e-Administración, según sea la disponibilidad online de los servicios otorgados:

Stage 0: no online service (“Sin implementar”)

Stage 1: information (“Presencia”)

Stage 2: one-way interaction (“Interacción unidireccional”)

Stage 3: two-way interaction (“Interacción bidireccional”)

Stage 4: (Full) transaction (“Transacción completa”).

Sin desmerecer las bondades, tránsitos y dificultades consiguientes para arribar y permanecer eficazmente en cada una de estas instancias, se ha podido

---

<sup>6</sup> “Estudio de las Naciones Unidas...” pág. 121.

<sup>7</sup> El mencionado Estudio está publicado en:

[http://ec.europa.eu/information\\_society/eeurope/i2010/docs/benchmarking/egov\\_benchmark\\_2007.pdf](http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/egov_benchmark_2007.pdf)

observar la aparición de un escalón superior, en los siguientes términos: *“El nivel 5 supone un “ir más allá” en la e-Administración; consiste en la proactividad, la personalización, en aprovechar el canal establecido para aumentar el valor añadido de los servicios, poniendo automáticamente la información a disposición de la ciudadanía conforme a las necesidades e intereses de cada cual”*.<sup>8</sup>

Se trata, en suma, de la llamada “administración inteligente” (i-administración), caracterizada básicamente como la “administración que aprende” a través de facilitar mecanismos potenciadores del conocimiento a los administrados (individuos, grupos, etc.), que le permiten retroalimentar con ganancia sus cometidos y labores.

Ello importa un grado de desarrollo de la administración electrónica superior al conocido, con el consiguiente cambio cultural, *“haciendo confluir o converger: CALIDAD, CONOCIMIENTO y TIC. Una Administración que personaliza y atiende individualizadamente a cada ciudadano, según sus necesidades, demandas y requerimientos concretos... que es capaz de prever y anticiparse a las demandas de los ciudadanos y poner a disposición de éstos las respuestas a sus requerimientos, en el momento, en la forma, en la cantidad y en la calidad que necesita por el canal que solicite.”*<sup>9</sup>

---

<sup>8</sup> “Cuestiones básicas de la e-administración”, Universidad del País Vasco. Consultable en:

[http://www.pas-personal.ehu.es/p263shformct/es/contenidos/informacion/pasform\\_capsulas\\_formativas/es\\_form/adjuntos/e-administraci%C3%B3n.pdf](http://www.pas-personal.ehu.es/p263shformct/es/contenidos/informacion/pasform_capsulas_formativas/es_form/adjuntos/e-administraci%C3%B3n.pdf)

<sup>9</sup> José BENEDITO AGRAMUNT - “La e-Administración, Una administración para el Siglo XXI”. Consultable en [www.socinfo.info/seminarios/java/valencia.pdf](http://www.socinfo.info/seminarios/java/valencia.pdf)

## **C - Tendencias sectoriales**

### **1. Aplicación de las TIC a grandes temas del desarrollo humano**

Se verifica hoy día un amplio consenso vinculado con el impacto que tienen las Tecnologías de la Información y la Comunicación en las diferentes áreas de desarrollo de las sociedades. Las TIC emergen tal si fueran instrumentos novedosos, generándose una amplia gama de utilidades para éstas, siendo una de sus principales condiciones la de funcionar como eficaces herramientas para el desarrollo.

Esta correlación e incluso, identificación entre TIC y desarrollo, se verifica central en las agendas políticas de los últimos diez años. Habitualmente, se considera que existe una conexión positiva entre ambos factores, de modo que la inversión en TIC es vista como una dimensión importante en la consecución exitosa de proyectos con desenvolvimiento futuro.

Sin embargo, aún hace falta un importante camino que recorrer para incluir genuinamente a dichas tecnologías en las agendas de desarrollo, dado que los países del Sur no acostumbran priorizar la inversión en estas áreas.

Por tanto, a los efectos de la obtención del objetivo del desarrollo sostenible, ha de crearse un ecosistema propicio a fin de tratar el tema de los contenidos, la conectividad y la accesibilidad a partir de un enfoque holístico e integrado.

Además, el alto costo del *hardware* y de la conectividad de las telecomunicaciones y las tecnologías representa un obstáculo superlativo. En el mismo sentido, este desafío puede superarse estimulando la fabricación local de tecnologías, así como la incorporación de disposiciones normativas que avancen en el sentido de la prestación de todos los servicios públicos en clave electrónica con la finalidad de otorgar garantías de su transparencia, eficiencia, accesibilidad y fiabilidad.

En este sentido, temas tales como educación, energía, infraestructura,

medicina, entre otros, se verifican de una centralidad tal, que la incorporación de métodos y mecanismos electrónicos será lo que facilite el tan necesario desarrollo sostenible.

## **2. Web *n.0***

En sus inicios la web era un lugar virtual donde colocar información contenida en códigos de difícil manipulación y actualización, no existiendo interacción.

Esto evolucionó sustancialmente con la aparición de la web 2.0 donde se ampliaron las interacciones, estandarizándose los lenguajes para facilitar la reutilización de los códigos.

El advenimiento de la web semántica, ha sido un hito sustancial donde la inteligencia humana conjuntamente con la artificial, sumado al lenguaje adecuado, permiten la comunicación entre ellas.

A esta web 3.0 se le deben sumar las cualidades de ubicuidad, red móvil, usabilidad, accesibilidad, web indexable y actualizable, y así es que se llega a la denominada web 4.0 o web cerebral.

Hasta ese momento la referencia era a un entorno web emocionalmente neutro; sin embargo el advenimiento de la web 5.0 implica la incorporación de emociones a partir de dispositivos y herramientas que reconocen el tipo de sensaciones que genera un video o las reacciones que provoca un texto.

Dispositivos portátiles, ligeros, con implantaciones neuronales, memoria y velocidad de aprendizaje, de alta resolución, con capacidad para el desarrollo de una interacción total donde lo que siente el usuario está presente, es lo que se denomina web sensorial y emotiva.

Aparentemente no hay límites en esta evolución que paulatinamente incorpora más y más elementos a la web, planteándose a priori un futuro ilimitado con sus consideraciones de diferente índole, imprescindibles de ser analizadas en sus diversas perspectivas.



### **3. E - salud - Telesalud**

La denominada salud electrónica o e-salud implica el empleo de las tecnologías de la información, especialmente Internet, para mejorar o facilitar la salud y los cuidados médicos. El sector sanitario ha sido siempre muy activo en la incorporación de tecnologías para el cuidado del paciente, y en las últimas décadas se ha visto ampliamente influenciada por las Tecnologías de la Información. Los cambios tecnológicos influyen también en cambios organizativos y nuevas concepciones de los servicios sanitarios.

La telesalud es sin duda la máxima expresión de la aplicación de las tecnologías de la información, incrementado por el uso de Internet, a la salud de las personas, implicando la aplicación de estas tecnologías para la transmisión de información del cuidado de la salud con el objetivo de brindar servicios clínicos, administrativos y educativos.

Esta nueva realidad debe ser observada y no puede ser ajena al Derecho, en virtud de que muchas veces los problemas de aplicación e interpretación de las normas se ocasionan como consecuencia de la inseguridad jurídica, producto de la ausencia de regulación de ciertos fenómenos tecnológicos. Sin lugar a dudas el generar un marco legal adecuado debe ser una de las preocupaciones al implementar servicios de salud en la modalidad de telesalud. Asimismo resulta determinante estimar la necesidad y la conveniencia de menores o mayores niveles de regulación y la identificación de aquellos puntos donde la normativa tradicional en la materia necesita ser actualizada.

### **4. Cloud computing**

Uno de los temas más resonantes en la actualidad es el cloud computing o la denominada computación en la nube. Redes sociales como por ejemplo

Facebook, así como cuentas de correo electrónico basadas en la web, como gmail, recurren a la nube. El servicio de computación en la nube supone la entrada de un tercero que no es sino el proveedor de servicios en la nube. Esto plantea un nuevo escenario que, aun siendo muy conveniente desde el plano comercial, puede dar lugar a importantes planteamientos desde el punto de vista jurídico, sobre todo, si pensamos en la utilización de estos servicios por parte de las entidades estatales. Desde el Observatorio Jurídico, ello nos lleva necesariamente a reflexionar acerca de los desafíos que pueden plantearse, teniendo en cuenta que gran parte de la legislación nacional no se elaboró pensando en la computación en la nube.

Para profundizar el estudio de este tema, el Observatorio Jurídico ha tomado como referencia documentos que han elaborado diversas organizaciones, destacándose entre ellos la Evaluación de Riesgo – NIST, las Recomendaciones de la CNIL sobre Cloud computing, y la WP196 Recomendación 5/2012.<sup>10 11 12</sup>

## 5. Gobernanza

La gobernanza de Internet, según la World Summit on the Information Society “es el desarrollo y la aplicación por los gobiernos, el sector privado y la sociedad civil, en sus respectivos papeles, de principios, normas, reglas, procedimientos de adopción de decisiones y programas comunes que

---

<sup>10</sup> Informe NIST sobre Cloud Computing: [https://downloads.cloudsecurityalliance.org/initiatives/guidance/NIST-Draft-SP-800-144\\_cloud-computing.pdf](https://downloads.cloudsecurityalliance.org/initiatives/guidance/NIST-Draft-SP-800-144_cloud-computing.pdf)

<sup>11</sup> Grupo de Trabajo del Artículo 29, opinión WP 196 disponible en [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion\\_recommendation/files/2012/wp196\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion_recommendation/files/2012/wp196_en.pdf)

<sup>12</sup> Recomendaciones sobre Cloud Computing de la CNIL <http://www.cnil.fr/linstitution/actualite/article/article/cloud-computing-cnils-recommandations-for-companies-using-these-new-services/>

configuran la evolución y el uso de Internet”.<sup>13</sup>

Los especialistas en telecomunicaciones consideran a la gobernanza de Internet a través del prisma del desarrollo de la infraestructura técnica. Los especialistas en informática se centran en el desarrollo de diferentes normas y aplicaciones, tales como XML o Java. Los especialistas en comunicación hacen hincapié en la facilitación de la comunicación. Por su parte, los activistas de derechos humanos consideran la gobernanza de Internet desde la perspectiva de la libertad de expresión, la privacidad y otros derechos humanos.

Dependiendo de las áreas se verifican diferentes enfoques. Así, los especialistas en temas jurídicos se concentran en la agenda de derechos y en la competencia y solución de controversias. Los políticos se centran en los temas que se vinculan con sus electorados. Los diplomáticos se ocupan principalmente de los procesos de protección de los intereses nacionales.

En conclusión es posible afirmar que las aristas son múltiples, los centros de interés variados pero el elemento común lejos de ser la tecnología, lo es la persona y sus derechos, desde las diferentes perspectivas y centralidades.

## **6. Neutralidad en la red**

La neutralidad en la red no es un tema nuevo, y ha sido objeto de debate desde hace algunos años. Generalmente la neutralidad de la red se refiere al principio de que todas las comunicaciones electrónicas que pasan a través de una red deben ser tratadas por igual, independientemente de su origen, contenido o destino.

El tema ha resurgido en el correr de este año en virtud de las críticas realizadas a la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen medidas en relación con el mercado único europeo de las comunicaciones electrónicas y para crear un continente conectado,

<sup>13</sup> Resolución de ONU N° 56/183 (21 December 2001) adoptó la definición de World Summit on the Information Society (WSIS) <http://www.itu.int/wsis/basic/about.html>

modificando las Directivas 2002/20/CE, 2002/21/CE y los Reglamentos (CE) nº 1211/2009 y (UE) nº 531/2012, de 11 de setiembre de 2013.<sup>14</sup> Se considera que uno de los aspectos más controvertidos de la propuesta de Reglamento es la neutralidad de la red. En principio, la Unión Europea había decidido tomar medidas para salvaguardar la neutralidad de la red tras la publicación de un estudio realizado por el Organismo de Reguladores Europeos de Comunicaciones Electrónicas (ORECE) en 2011, que encontró que en la recepción de servicios en línea muchos consumidores europeos se enfrentaban a prácticas de bloqueo o estrangulamiento de contenido. La propuesta de Reglamento tiene por objeto poner fin a esas prácticas y dar a cada consumidor europeo el llamado "derecho de abrir Internet". Se prevé que los usuarios finales tengan la facultad de celebrar acuerdos sobre los volúmenes de datos y velocidades con los proveedores de servicios de Internet.

Sin embargo la propuesta de Reglamento también prevé la posibilidad para los proveedores de comunicaciones electrónicas al público deben ofrecer servicios de conectividad de primera calidad. En este sentido, los usuarios finales tendrán libertad para convenir con los ISP - o con los proveedores de contenidos, aplicaciones y servicios - la prestación de servicios especializados con una mejor calidad de servicio. A fin de permitir la prestación de los servicios especializados a los usuarios finales, la propuesta de Reglamento permite a los ISP y proveedores de contenidos, concertar acuerdos entre sí para transmitir los volúmenes de datos relacionados con el tráfico o los servicios especializados con una definida calidad del servicio o capacidad dedicada.

## **7. Ciberseguridad**

El término Ciberseguridad se define como los procedimientos aplicados para la gestión y protección del uso, procesamiento, almacenamiento y

---

<sup>14</sup> Resolución del Parlamento Europeo sobre la internet abierta y la neutralidad de la red en Europa disponible en <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+MOTION+B7-2011-0572+0+DOC+XML+V0//ES>

transmisión de datos e información; a través de las Tecnologías de Información y Comunicación (TIC) al momento de navegar en el ciberespacio. La Ciberseguridad es vital para los internautas ya que la confidencialidad de sus sistemas puede ser vulnerable a los ataques de virus informáticos.

Este año la ciberseguridad ha sido noticia reiteradamente en diferentes países del mundo. Como sucede con algunos de los otros fenómenos descritos en este documento, la ciberdelincuencia también se ha extendido mucho en los últimos años debido a la expansión de Internet. Entre las principales noticias en la materia se destaca la creación del Centro Europeo del Cibercrimen EC3 dentro del seno de Europol<sup>15</sup>. También se destaca que algunos países han regulado el tema estableciendo marcos normativos de referencia.

## **8. Ciberdefensa**

La determinación conceptual específica de ciberguerra, ha sido y sigue siendo de una importante complejidad, sin perjuicio que no se trata de una actividad novedosa ya que puede remontarse a finales del siglo pasado.

Sin embargo, es posible afirmar que se trata de un concepto estratégico de los gobiernos que requiere la comprensión de variables tales como las vulnerabilidades en la infraestructura crítica de un Estado, las garantías y derechos de los ciudadanos en el mundo online, la renovación de la administración de justicia en el entorno digital y, la evolución de la inseguridad de la información en el contexto tecnológico y operacional.

En función de lo antedicho y su vínculo con la ciberguerra es central que se posicione el pensamiento estratégico vinculado con la defensa no solo en su consideración tradicional sino en aquella de índole global mediante las tácticas, técnicas y procedimientos que otorguen seguridades a los ciudadanos. Por lo tanto es imprescindible avanzar a partir de una aproximación holística de todos

---

<sup>15</sup> Se puede visitar el sitio del Centro Europeo del Cibercrimen EC3 en <https://www.europol.europa.eu/ec3>

los actores que deben implicarse en la defensa del bienestar, intereses y valores de estados libres y democráticos.

## **9. Ciberguerra**

La referencia a ciberguerra debe considerarse efectuada al desplazamiento del conflicto -tradicionalmente bélico- al ciberespacio, mediante la utilización de las tecnologías de la información que sustituyen a los tradicionales campos de batalla. La ciberguerra es rentable y anónima permitiendo ataques a gran escala en la medida que no se verifican barreras de índole física que impidan que se propaguen los ataques.

Se trata de un hacking cuya motivación es de orden político y su objetivo es el sabotaje y el espionaje. El objetivo es la producción de alteraciones en la información y sistemas de quien se determina como enemigo conjuntamente con la protección de la información y sistemas propios.

La Resolución del Consejo de Seguridad de Naciones Unidas sobre ciberguerra estableció que se trata del “Uso de computadores o medios digitales por un gobierno, sea con conocimiento explícito de o aprobación de ese gobierno contra otro estado, o propiedad privada dentro de otro estado incluyendo: accesos intencionales, interceptación de datos o daño a infraestructura digital e infraestructura controlada digitalmente”.

Desde el punto de vista geoestratégico es posible visualizar a futuro que la ciberguerra en la actualidad no es más que la escaramuza primaria de futuros conflictos. Por lo mismo, es central tener conciencia de la gravedad de la situación y analizar las capacidades de reacción y discusión políticas seria y negociada.

Entre las amenazas más importantes a la seguridad mundial se encuentra en tercer lugar después de la guerra mundial convencional y las armas de destrucción masiva, sobre todo en la consideración que varios países han declarado tener lo que se denomina ciberarmada.

## **10. Impresora 3D – Propiedad intelectual**

Se entiende la impresión 3D como “la tecnología que propicia la fabricación casera o profesional de prácticamente cualquier objeto que se desee partiendo de un diseño digital. La impresora imprime el diseño, transformando los bits en objetos físicos”<sup>16</sup>. La impresión 3D tiene amplia repercusión en el ámbito de la Propiedad Intelectual donde debe continuarse el respeto de los derechos de los autores, resurgiendo también el tópico de las copias privadas, y otros temas como la cantidad de copias que se pueden realizar, la posibilidad de efectuar modificaciones del diseño original, entre otros. Por otro lado, también se observan problemas con la Propiedad Intelectual en lo atinente a la comercialización del producto tanto del aparato reproductor en sí como sobre las obras que genera éste.

## **11. BYOD (Bring your own device)**

El BYOD (Bring your own device por sus siglas en inglés) es una tendencia creciente en las empresas de todo el mundo que consiste en una política que permite, alienta, y en ocasiones incluso impone, a los empleados, que utilicen para su trabajo (dentro o fuera de la empresa), sus propios dispositivos móviles (ordenadores portátiles, smartphones, notebooks, tablets, etc), pudiendo acceder con ellos a recursos privilegiados de la empresa, tales como el correo electrónico, los servidores de archivos, las bases de datos, entre otros, así como a las aplicaciones y a los datos personales de dicha empresa.<sup>17</sup>

Ante la expansión del BYOD se identifican una serie de preocupaciones que merecen un estudio mayor. Nos referimos a la identificación de la propiedad de los dispositivos y de la información que se encuentra en ellos, la seguridad

---

<sup>16</sup> <http://www.impresoras3d.com/aspectos-legales-de-la-impresion-3d-abanlex>

<sup>17</sup> <http://leyprotecciondedatos.files.wordpress.com/2013/01/quc3a9-es-el-byod.pdf>

de la información corporativa, la gestión de los registros de información, los problemas relacionados con el E-discovery, así como el cumplimiento de las normas laborales, entre otros<sup>18</sup>.

Las primeras soluciones que se vislumbran en derecho comparado para superar estos problemas tienen relación con políticas de uso de los dispositivos por parte de las distintas Entidades.

## 12. Internet de las cosas

Cuando se habla de “Internet de las cosas” se dice que consiste en que las cosas tengan conexión a Internet en cualquier momento y lugar. Dicho de otra forma, se puede entender como la integración de sensores y dispositivos en objetos cotidianos que quedan conectados a Internet a través de redes fijas o inalámbricas.<sup>19</sup>

La evolución de este tema ha conllevado muchas repercusiones jurídicas que es necesario conocer, en virtud de que se trata de un fenómeno de alcance mundial del cual Uruguay no se encuentra al margen. Dentro de los temas jurídicos que involucra se puede mencionar su incidencia sobre la jurisdicción, en tanto se va a desarrollar en varios países con marcos normativos divergentes. Otro tema es la privacidad puesto que hay quienes entienden que se incrementa el riesgo de tratamiento de datos sin consentimiento de sus titulares. Relacionado con lo anterior encontramos la *big data* entendida como el tratamiento de enormes volúmenes de información. También se debe analizar

---

<sup>18</sup> Documento disponible en [http://www.lexology.com/library/detail.aspx?g=7a3a51eb-1680-4df6-b72a-5d9c867dd774&utm\\_source=Lexology+Daily+Newsfeed&utm\\_medium=HTML+email+-+Body+-+Federal+section&utm\\_campaign=ITechLaw+subscriber+daily+feed&utm\\_content=Lexology+Daily+Newsfeed+2013-11-06&utm\\_term=](http://www.lexology.com/library/detail.aspx?g=7a3a51eb-1680-4df6-b72a-5d9c867dd774&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email+-+Body+-+Federal+section&utm_campaign=ITechLaw+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2013-11-06&utm_term=)

<sup>19</sup> Fundación de la Innovación Bankinter: “El Internet de las Cosas: En un mundo conectado de objetos inteligentes”, p. 3. Consultable en [http://www.fundacionbankinter.org/system/documents/8168/original/XV\\_FTF\\_El\\_internet\\_de\\_las\\_cosas.pdf](http://www.fundacionbankinter.org/system/documents/8168/original/XV_FTF_El_internet_de_las_cosas.pdf)



qué sucede con el cumplimiento de las normas sobre seguridad de la información. Otro tema es el de los delitos informáticos. El marco que brinda la Internet de las cosas abre posibilidades al desarrollo de nuevas conductas delictivas, o la dificultad en identificar a los titulares de los datos.

Más allá de la incidencia sobre temas ya identificados, se habla de otros nuevos aspectos que merecen un análisis mayor. Por ejemplo, el derecho al silencio de los chips, en el sentido de que las personas tienen derecho a no estar conectados a Internet de ninguna forma, o la legalidad del reconocimiento de la identidad legal de la cosa, esto es, si la cosa puede ser sujeto de derecho.

### **13. E – Discovery**

El E-Discovery o E-descubrimiento es la petición formal de información electrónica almacenada durante un juicio, que puede incluir correo electrónico, historial de navegación en Internet, transacciones en línea, documentos de procesamiento de textos, fotos almacenadas electrónicamente, mensajes grabados, entre otros. Estos datos pueden encontrarse almacenados en distintos tipos de dispositivos electrónicos tales como computadores, teléfonos inteligentes, tablets<sup>20</sup>. El E-discovery debe ser solicitado por una parte en un juicio de conformidad con las normas que se establecen en un procedimiento civil. En los casos que se han dado, se ha entendido que la solicitud debe especificar razonablemente los asuntos buscados.

Desde el punto de vista jurídico el E-discovery está dando lugar a ciertos problemas jurídicos, entre ellos, la conservación de los datos en el entendido que la naturaleza dinámica y cambiante de los datos electrónicos puede hacer dificultoso encontrar la información pertinente si aquéllos se modifican o destruyen. Otro punto es el ámbito del descubrimiento, la cantidad de información que la parte puede obtener, que puede ser enorme y por ende dificultar la recuperación de la información relevante.

<sup>20</sup> <http://abogados.lawinfo.com/es/articulos/leyes-de-comercio-electronico/federal/-qu-es-el-e-discovery.html>

En Estados Unidos se ha llevado adelante un programa piloto de E-discovery. Este programa se realizó entre los años 2010 y 2012 e involucró a 40 jueces, 700 abogados, y se aplicó en 296 casos. Del proyecto surgieron una serie de estándares para el uso de esta herramienta. También es interesante saber que los Estados de Pensilvania y Florida han aprobado enmiendas que versan sobre este tema, y que se han añadido a sus normas civiles. No menos importante es tomar en consideración que existe ya una herramienta de E-discovery agregada a aplicaciones de Google llamada Google Apps Vault, que permite conservar, archivar, buscar y exportar el correo electrónico de la organización para satisfacer los requisitos del régimen.<sup>21</sup>

#### **14. Telecomunicaciones y protección de datos.**

Aunque la protección de datos en el ámbito de las telecomunicaciones es un tema recurrente. De todos modos no faltan referencias actuales a la regulación de las cookies, las comunicaciones no deseadas (spam), la seguridad y confidencialidad de los tratamientos, y las guías públicas, entre otros.

La Unión Europea con fecha 24 de junio de 2013 determinó la entrada en vigencia del Reglamento N° 611/2013, que obliga a los proveedores de servicios de comunicaciones electrónicas disponibles al público a notificar las violaciones de datos personales a las autoridades nacionales. Sin embargo, la Comisión Europea ha descubierto recientemente una falta de armonización entre los Estados miembros a este respecto, y ejerció su poder para dictar medidas técnicas de ejecución. La nueva regla se aplica a todos los prestadores de servicios públicos de comunicación electrónica. Si el proveedor detecta una violación de los datos personales debe notificar a la autoridad nacional competente de dicho incumplimiento dentro de las 24 horas. El Reglamento establece una escapatoria al afirmar que la notificación debe ocurrir dentro de

<sup>21</sup> Más información sobre Google Apps Vault en:

<https://support.google.com/vault/answer/2462365?hl=es>

24 horas "cuando sea posible". Por lo tanto, en los casos en que el proveedor no pueda proporcionar toda la información sobre el incidente dentro de este plazo, el reglamento permite presentar sólo una notificación inicial para completarla luego. En los tres días siguientes a la notificación inicial, el proveedor debe proporcionar un segundo conjunto de información que da más detalles sobre la violación de los datos. Además, el proveedor debe notificar a las personas afectadas y sin "dilaciones indebidas", si existe probabilidad que afecte negativamente sus datos personales o la privacidad.<sup>22</sup>

## 15. Privacidad móvil

Según el Grupo de Trabajo del Artículo 29 de Protección de Datos *“Existen cientos de miles de aplicaciones disponibles en toda una serie de tiendas de aplicaciones para cada tipo de dispositivo inteligente de cierta popularidad. Las aplicaciones pueden recoger grandes cantidades de datos a partir de dispositivos y procesarlos para proporcionar servicios nuevos e innovadores al usuario final. Sin embargo, esas mismas fuentes de datos pueden ser objeto de un tratamiento adicional, normalmente para generar ingresos, de forma desconocida o no deseada por el usuario final”*<sup>23</sup>.

Ante este panorama, el Grupo ha emitido un dictamen orientador sobre el marco jurídico aplicable al tratamiento de los datos personales en el desarrollo, distribución y uso de aplicaciones en dispositivos inteligentes, centrándose en el requisito del consentimiento, los principios de finalidad y de minimización de los datos, la necesidad de adoptar medidas de seguridad adecuadas, la obligación de informar correctamente a los usuarios finales y respetar sus derechos, los períodos de conservación razonables y, especialmente, el tratamiento leal de los

---

<sup>22</sup> Documento disponible en:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:ES:PDF>

<sup>23</sup> Dictamen 2/2013 sobre las aplicaciones de los dispositivos inteligentes del Grupo de Trabajo del Artículo 29 sobre protección de datos, pág. 2 disponible en [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index\\_en.htm](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm)

datos recopilados a partir de niños o sobre ellos.

Además de lo señalado, es interesante tomar en consideración los avances de la iniciativa en línea “AppRights”, y el proyecto de ley en consideración en Senado Norteamericano, para regular los datos personales de los consumidores que son recopilados por aplicaciones móviles.<sup>24</sup>

## **16. Derecho al olvido**

Cuando hablamos de derecho al olvido se hace referencia a la protección frente a las lesiones de derechos producidas por la difusión universal de datos personales en Internet y su accesibilidad a través de buscadores. Desde el punto de vista de la protección de datos se relaciona con la proyección en Internet de derechos existentes tales como la revocación del consentimiento, los derechos de rectificación, cancelación y oposición. Siempre hay que tener en consideración que no es un derecho absoluto, en el sentido que no da el derecho a cancelar informaciones “a voluntad”, a borrar toda la información personal de Internet o a “salir de Internet”. Es un derecho a oponerse a la difusión a través de Internet de informaciones personales sin relevancia pública ni interés general.

Este derecho al olvido en general se ejerce ante los editores como responsables del primer tratamiento y a los buscadores como responsables de tratamientos posteriores. Este tema ha cobrado relevancia en los últimos años ante el uso masivo de Internet, por lo que los problemas jurídicos en relación con el derecho al olvido han sufrido un gran incremento. Es por ello que tanto la Agencia Española de Protección de Datos como el Grupo de Trabajo del Artículo 29 han emitido opiniones recientes, que es recomendable tener presente.<sup>25</sup>

---

<sup>24</sup> Más sobre la iniciativa en línea AppRight disponible en <https://apprights-hankjohnson.house.gov/>

<sup>25</sup> Memoria de la Agencia Española de Protección de Datos 2012 disponible en [http://www.agpd.es/portalwebAGPD/revista\\_prensa/revista\\_prensa/2013/notas\\_prensa/news/2013\\_10\\_29-ides-idphp.php](http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2013/notas_prensa/news/2013_10_29-ides-idphp.php)

## 17. Reglas corporativas vinculantes (“binding rules”)

Las “reglas corporativas vinculantes” (binding rules) han sido y seguirán siéndolo un factor de apoyo al crecimiento de las transferencias internacionales de datos personales, desde el momento que son pocos los países o unidades territoriales que gozan de estatuto oficial y pleno en la materia, particularmente fuera del espacio europeo.

El mecanismo permite que, ante casos concretos donde el país importador no goza del citado estatuto prevalente al nivel de país (la declaración de adecuación), pueda sin embargo habilitarse a empresas o instituciones específicas el tráfico consiguiente, cumpliendo un conjunto de cláusulas contractuales.

En términos del artículo 26, apartado 2, de la Directiva 95/46 de la UE, *«los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado[...], cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas»*.<sup>26</sup>

No es del caso extendernos en esta oportunidad sobre contenidos y alcances concretos de estas reglas, bastando señalar su importancia así como una constante ocupación del asunto por parte del Grupo del Art. 29 de la Directiva, el último de los cuales aborda lo más actual en esta materia.<sup>27</sup>

---

<sup>26</sup> Documento disponible en:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML>

<sup>27</sup> Documento explicativo del Grupo del Art. 29 sobre las normas corporativas vinculantes para los encargados de tratamiento, WP 204/2013 del 19 de abril de 2013 disponible en: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index\\_en.htm#h2-1](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-1).

## 18. Big data

Es importante definir qué es la *big data*. En el plano internacional se la conceptualiza como una tendencia en el avance de la tecnología que ha abierto las puertas hacia un nuevo enfoque de entendimiento y toma de decisiones, la que es utilizada para procesar enormes cantidades de datos (estructurados, no estructurados y semi estructurados) que tomaría demasiado tiempo y sería muy costoso cargarlos a una base de datos relacional para su análisis. De tal manera que, el concepto de Big Data aplica para toda aquella información que no puede ser procesada o analizada utilizando procesos o herramientas tradicionales. Sin embargo, la Big Data no se refiere a alguna cantidad en específico, y usualmente es utilizada cuando se llega a términos de pentabytes y exabytes de datos.<sup>28</sup>

Uno de los desafíos legales más significativos asociados con la Big Data, especialmente en la parte de marketing de consumo, es la privacidad. Las normativas de protección de datos personales obligan a que el interesado de quien se recogerán datos sea consciente de los usos a los que se someterá su información personal, y al que se dará a conocer dicha información personal. Dicho consentimiento tiene por objeto permitir al interesado tomar una decisión informada en cuanto a la recopilación y uso de su información personal, y para dar su consentimiento a la recopilación y el uso. Aquí el problema es doble: en primer lugar, la persona puede no entender que su información personal termine siendo combinada con otros datos de perfil existentes, de una manera que revela más sobre ella que la contemplada en el momento de su divulgación; y en segundo lugar, el interesado normalmente carece de una íntegra comprensión de las interpretaciones, inferencias y/o deducciones que se pueden extraer de sus datos combinados con técnicas de *data mining* y análisis.

---

<sup>28</sup><http://www.ibm.com/developerworks/ssa/local/im/que-es-big-data/index.html?cmp=BS&ct=SocialMedia&cr=twitter#toggle>

Por lo tanto, en un mundo de Big Data, se podría argumentar que los interesados tienen, generalmente, una menor conciencia y capacidad de dar un real consentimiento al manejo de sus datos y, por tal motivo, las empresas que se dedican a su comercialización proponen mitigar los riesgos relacionados con la privacidad, asociados con grandes datos por medio de la anonimización o disociación de los datos con su titular.<sup>29</sup>

## **19. Fronteras inteligentes**

El control de la migración y movilidad transfronterizos constituyen problemas actuales donde las tecnologías aportan soluciones.

En el año 2013 los europeos han puesto en consideración dos propuestas facilitadoras en torno a este asunto: un Sistema de Entrada/Salida (EES) y un Programa de Registro de Viajeros (RTP) para el espacio Schengen, que en conjunto se denominan «Fronteras inteligentes», seguidas de ajustes del Código de fronteras Schengen.<sup>30</sup>

En esencia se trata de la creación de bases de datos que permiten ahorrar tareas de verificación individuales, cálculos de temporalidad y sellos oficinescos, sustituyéndolos por lecturas automatizadas de programas informáticos donde quedan registrados, por ejemplo, los tiempos máximos de estadía de un viajero, motivos de permanencia dentro del territorio, etc.

Ese tipo de tecnologías facilita el control de ingresos y retornos interfronterizos, permitiendo contar, además, con datos y estadísticas fiables en la materia, al servicio de las políticas del caso sobre visados y otras facilidades o

---

<sup>29</sup>[http://www.eldial.com.ar/nuevo/lite-tcc\\_detalle.asp?id=14107&base=99&id\\_publicar=&fecha\\_publicar=09/10/2013&indice=editorial&suple=DAT](http://www.eldial.com.ar/nuevo/lite-tcc_detalle.asp?id=14107&base=99&id_publicar=&fecha_publicar=09/10/2013&indice=editorial&suple=DAT)

<sup>30</sup>Dictamen 05/2013 de 16 de junio de 2013, sobre el programa «Fronteras inteligentes» del Grupo del Art. 29 de la Unión Europea – WP 206/2013. Consultable en [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index\\_en.htm](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm)

restricciones a los viajeros.

El seguimiento en profundidad de esta tendencia es recomendable desde el momento que está en juego el régimen de protección de datos personales, por lo que debe sopesarse su verdadera dimensión y justificación en punto a la proporcionalidad de la recolección y tratamientos consiguientes, así como otras garantías propias del régimen.

## **20. Testamentos digitales**

Es fácil constatar que existe una tendencia mundial que indica que muchas personas están pasando más tiempo que nunca antes en Internet. Una gran parte de estas personas solamente se conectan a los efectos de descargar información, pero hay otros tantos, que dedican esfuerzo, tiempo y dinero para tener una presencia constante en línea. Como consecuencia de ello, no es de extrañar que el contenido en línea de una persona pueda resultar sumamente importante, no sólo en vida del afectado sino, también, luego de su deceso.

Cuando se habla de testamentos digitales la referencia es simplemente a una instalación de almacenamiento seguro en línea que le permite al interesado mantener sus datos de acceso a Internet, y todos los mensajes relacionados, dentro de un espacio en línea. A su muerte, se transmite el nombre de usuario y la contraseña del testamento digital a quien haya sido designado. El mecanismo y el medio por el que se hace esta disposición pueden variar entre los proveedores. Lo más probable es que habrá una cuota de suscripción a pagar para mantener la cuenta. En 2013, Google inauguró un proceso llamado Inactive Account Manager <sup>31</sup>, que permite a los usuarios planificar lo que quieren hacer con su cuenta en caso de fallecimiento. Facebook y Yahoo han adoptado una postura más estricta y no entregan datos sin una orden judicial, pero Facebook permite que los familiares elijan si quieren cerrar la cuenta o convertirla en una página conmemorativa sin interacción alguna, más que de los usuarios y

---

<sup>31</sup> Más información disponible en <https://support.google.com/accounts/answer/3036546?hl=es>



familiares que escriban en su muro. Evidentemente esto acarrea una serie de consecuencias jurídicas que deben ser consideradas, y por ello es que se hace mención del tema en el presente informe, a los efectos de considerar su seguimiento.

## **D - Recomendaciones**

En función de lo señalado en el presente informe y habiéndose considerado la normatividad existente o inexistente en los distintos temas, sumado a la prospectiva nacional e internacional es que se propone avanzar en la profundización de los siguientes temas:

### **a. Internet de las cosas.**

Como se señalara, este tema es sustancial sobre todo a partir de la consideración de la enormidad de dispositivos conectados sea en forma fija o inalámbrica, que además se espera siga creciendo exponencialmente.

En este sentido se verifica la existencia de una serie de intersecciones importantes y de imprescindible análisis jurídico.

**1.- Apertura y libertad en internet.-** La apertura de internet constituye su rasgo fundamental, motivo por el cual la libertad en su interior y en su contexto es central y connatural a su desarrollo. Si a esto se adiciona la creciente incidencia de internet en la vida personal de los individuos, la defensa de la libertad verifica entonces, mayor centralidad aún.

Ahora bien, esta defensa de la libertad en el entorno cuantitativo de internet es cada vez más compleja e imprescindible. Su análisis y consolidación postural en perspectiva humanista, aparece como uno de los elementos imprescindibles para alinear criterios en los que el centro de la tecnología sea la efectividad de los derechos de las personas.

**2.- Jurisdicción.-** Debido a la necesaria e importante descentralización de internet, indudablemente la jurisdicción es uno de los elementos más complejos a los efectos de realizar análisis y obtener acuerdos, ya que la normatividad nacional es indudablemente insuficiente y la eventualidad de un acuerdo internacional no parece demasiado efectivo, ni justo.

**3.- Conductas delictivas.-** La responsabilidad penal en aplicación de la tecnología informática – en particular de esta internet de las cosas - implica avanzar en la catalogación de conductas inimaginables hasta hace relativamente poco tiempo y que por la vertiginosidad con que avanzan las tecnologías impone la necesidad de encontrar soluciones a una realidad que se verifica instalada.

A ésta no escapa la aparición de conductas que por medio de la aplicación de internet generan trastornos importantes en la comunidad nacional e internacional, los que se ven agravados por la inexistencia de disposiciones normativas acordes que faciliten la punición de las mismas. Es imprescindible entonces, avanzar en una regulación normativa a efectos de que el país incluya en su ordenamiento jurídico un marco apropiado que facilite el combate a la ciberdelincuencia. Sin embargo, es importante considerar que el régimen que se adopte debería ser minimalista y sin posiciones definitivas en términos tecnológicos de forma tal de evitar una obsolescencia inexorable pero no inmediata.

**4.- Privacidad en la red.-** Indudablemente por sus características este tema implica una mayor intrusión y por ende injerencia, de internet y las TIC en general, en la vida de las personas.

Así es que avanzar en la consideración del carácter adecuado y suficiente o no, de las regulaciones en materia de protección de datos, intimidad, identidad personal por un lado y en aquéllas vinculadas con la lealtad comercial, la publicidad personalizada y defensa del consumidor por otro, se plantea como un desafío de imprescindible acometimiento.

## **b. Bring your own device**

Esta práctica puede generar un sinnúmero de situaciones que requieren un análisis jurídico detallado y además sin dudas la inclusión en disposiciones normativas generales y particulares, de niveles de especificidad considerables.

Así es que se propone analizar los siguientes problemas identificados sin perjuicio que pudieren surgir algunos conexos en la consideración particular:

**1.- Contratos de trabajo.-** Es necesario analizar la viabilidad de incorporar cláusulas contractuales – en el caso de la actividad privada - o disposiciones en los estatutos y reglamentos generales – en el caso de la actividad pública – a los efectos de la incorporación del BYOD. Es importante además que las cláusulas que se establezcan cuenten con el conocimiento efectivo y el consentimiento de los trabajadores, dadas las connotaciones que se entiende éste puede implicar, motivo por el cual es fundamental avanzar en propuestas para la inclusión en unos y otros mecanismos contractuales.

**2.- Seguridad de los datos.-** La normativa vigente consagra el derecho a la protección de los datos personales, motivo por el cual la protección contra los daños, pérdida, alteración, acceso no autorizado y divulgación, suministro y publicación es sustancial.

Por tanto es imprescindible avanzar en la consideración de la inclusión de reglas que impliquen las posibilidades de borrado remoto de los datos de los dispositivos en caso de extravío así como las obligaciones de información inequívoca hacia el empleador frente a estas situaciones, en mérito al eventual riesgo que esto pudiere ocasionarle. Asimismo, es importante considerar cuestiones vinculadas con las obligaciones de respaldo de los datos, la protección de los mismos con códigos de acceso, y fundamentalmente las medidas de seguridad que se consideren imprescindibles. Todo esto debe ser analizado para su inclusión en el vínculo laboral.

**3.- Compensaciones por la utilización de un dispositivo personal.-** Es

necesario considerar cláusulas vinculadas con la posibilidad de que el empleador otorgue al empleado una contribución para o por comprar el dispositivo, pagar una parte de su costo operativo o una cantidad fija para compensar su uso. La forma específica de la indemnización es una cuestión de acuerdo entre el empleador y el empleado, y debería ser objeto de regulación específica en las condiciones de trabajo.

Asimismo, es necesario analizar diferentes situaciones y sus consecuencias jurídicas vinculadas por ejemplo con la suspensión del servicio por ausencia de pago, pérdida del dispositivo, excesos en el límite de datos, entre otras.

**4.- Separación en el dispositivo del ámbito personal y aquél laboral.-** El trabajo y las actividades personales deben estar completamente separadas en el dispositivo del empleado. Esto requiere analizar mecanismos jurídicos que determinen los derechos, las obligaciones y las responsabilidades de diferente índole para las distintas situaciones, como por ejemplo, la utilización de diferentes mecanismos de seguridad, ya sea mediante el bloqueo o la restricción al acceso de determinadas páginas web y aplicaciones durante las horas de trabajo, el manejo de escritorios virtuales para evitar que los datos de la empresa que se almacenen en el dispositivo de un empleado, la determinación de los procedimientos en el caso de que la relación laboral se extinga.

**5.- Responsabilidad penal.-** Es necesario analizar las eventuales conductas delictivas que este mecanismo de trabajo podría implicar y, bajo una lógica de Derecho Penal mínimo considerar si las tipificaciones existentes permiten las correspondientes imputaciones de responsabilidad penal. Ante una posible respuesta negativa, se impone estudiar la posibilidad de alguna propuesta normativa general y abstracta.

### **c. Derecho al olvido**

Es importante en este punto efectuar diferentes tipos de análisis en perspectiva jurídica en mérito a que no se trata de un derecho que pueda ejercerse

transversalmente y en cualquier momento, sólo a instancias del requirente y sin consideración contextual.

En efecto, se propone analizar los impactos que éste tiene en función de las diferentes áreas – económico-financiera, social, delictiva o sancionatoria, entre otras – así como también los tiempos necesarios para el ejercicio y los plazos para su concreción en cada caso.