Datuak Babesteko
Euskal Bulegoa
Agencia Vasca de
Protección de Datos

El derecho a la privacidad y a la protección de datos personales.
Primeras reflexiones sobre prácticas de gestión de la información por parte de los profesionales de la Psicología

La protección de datos personales debe considerarse como parte de una cuestión más amplia: el de la protección de la vida privada y la dignidad humana.

El derecho a la vida privada tiene relación con la naturaleza y el alcance del derecho de todo individuo a actuar solo y al abrigo de entrometimientos injustificables. Se entiende también como la capacidad de controlar la información referente a uno mismo. A cada individuo se le reconoce la libertad para decidir si se han de difundir datos sobre su persona, dentro de las limitaciones impuestas por la salvaguardia de los intereses legítimos del estado o de terceros.

El análisis de las implicaciones de este derecho en el ejercicio profesional de los psicólogos remite a la perspectiva ética de su conducta profesional. En particular, se concreta en principios generales y normas específicas recogidas, de manera más o menos comprensiva, en los códigos deontológicos de aplicación en cada país. Para ilustrar dos casos, estas normas de conducta se encuentran en capítulos referidos a la *Obtención y Uso de la Información* (Código Deontológico estatal del Colegio Oficial Psicólogos) o al *Principio de Respeto por los derechos y la dignidad de la persona*, con sus específicos estándares sobre el derecho a la *Privacidad y Confidencialidad*, y al derecho a la *Información*, que se materializa en el *Consentimiento Informado y la Libertad de Consentimiento* (Code of Professional Ethics, The Psychological Society of Ireland).

Muchas prácticas profesionales específicas del campo de la Educación y la Psicología, como la evaluación educativa, el empleo de test de medida, etc., contemplan estándares o principios consensuados de práctica profesional. Entre estos principios se reconocen los derechos de las personas, que se basan en leyes, otros en una práctica ética ampliamente aceptada, el sentido común y la cortesía. Estos derechos de las personas recogen cuestiones como el consentimiento para la participación, el derecho a la renuncia, la privacidad de ciertas opiniones o informaciones, la confidencialidad de la información y la protección de la salud y la seguridad.

En general, se puede afirmar que los psicólogos, si se comparan con otros colectivos profesionales, han sido especialmente conscientes de la importancia de la confidencialidad o reserva de la información que manejan, y de que ella es una condición necesaria para que las personas depositen su confianza en el profesional, y por ende, le confíen sus problemas, sus necesidades y sus deseos. Esto es así, que los códigos de conducta profesional de los psicólogos contemplan, como se ha señalado más arriba, principios orientadores del ejercicio profesional relacionados con la protección de los datos personales.

Ahora bien, si el respeto a la privacidad es una parte inherente al comportamiento profesional de este colectivo, que además está suficientemente sensibilizado con este tema, ¿es necesario cambiar alguna práctica profesional para garantizar el respeto a este derecho fundamental a la protección de la información personal? La respuesta es que sí y posteriormente se expondrá una síntesis de las medidas básicas a adoptar.

Cabe preguntarse también qué ha cambiado en el contexto social, legal e individual que está en el origen de la necesidad de adoptar nuevas prácticas profesionales. De forma resumida, pueden identificarse dos hechos decisivos: por un lado, el desarrollo de las tecnologías de la

información y la comunicación, y por el otro, una creciente conciencia sobre los derechos individuales y colectivos relacionados con el valor de la información y su gestión.

El desarrollo de las tecnologías de la información y de la comunicación ha posibilitado un flujo de información sin precedentes desde la última década del siglo XX. Pero ha traído consigo también una mayor vulnerabilidad respecto a poder controlar la información sobre la propia persona, ya que ésta fluye en diferentes soportes electrónicos y telemáticos, y es difícil controlarla y eliminarla una vez puesta en circulación.

Una mayor conciencia por parte de las sociedades y de sus individuos respecto a derechos relacionados con la información se puede concretar en dos demandas crecientes. Una de ellas relacionada con una mayor transparencia de las administraciones públicas, que han de informar más y mejor a los ciudadanos sobre cómo gestionan los bienes y servicios públicos en desarrollo de sus políticas (*derecho a la información*, todavía sin legislar en el ordenamiento jurídico español). Un fenómeno similar se observa en la importancia creciente que presentan, en el ámbito de la empresa privada, las conductas corporativas que se conocen como *Responsabilidad Social*. La otra demanda es la protección o salvaguarda acerca de usos no deseados o indebidos de la información sobre cada persona, tales como la información comercial nominativa no deseada, los perfiles como consumidores no consentidos o informados, difusión en Internet de información personal excesiva o no deseada, por citar los más generalizados.

Al derecho a acceder a información pública y al derecho a la protección de información personal, ambos de desarrollo incipiente pero rápido, ha de sumarse el deber de los gobiernos de velar por la seguridad física de los ciudadanos; es preciso notar que el fin de procurar la mencionada seguridad física está produciendo tensiones con respecto al derecho a la protección de datos personales, de tal manera que parece que en ocasiones la consecución de un bien hace imprescindible el sacrificio del otro. Piénsese en la nueva ley que obliga a las compañías de telecomunicaciones a mantener durante un prolongado período de tiempo un registro de todas las comunicaciones telefónicas, correos electrónicos y accesos a Internet habidos, en aras a una deseable seguridad y prevención del terrorismo y la criminalidad en general.

Se ha descrito hasta aquí el escenario social y legal que contextualiza la oportunidad de una ley que pretende garantizar un derecho a la protección de los datos personales. Ahora bien, ¿cómo impacta el nuevo escenario en el quehacer del colectivo profesional de los psicólogos?

Se expone a continuación cómo el derecho a la protección de datos personales se traduce en determinadas limitaciones y procedimientos de gestión de la información en la práctica profesional. Para comprender estas últimas es necesario enunciar, de manera paralela, algunos de los conceptos, principios y derechos involucrados en la protección de datos, así como las principales fases u operaciones en el tratamiento de datos.

*¿Qué es la **Protección de datos de carácter personal**?*

En esencia, la protección de datos parte de la tesis de que la información personal pertenece a las personas a las que hace referencia y que, por ello, éstas tienen una serie de derechos. Aquellos otros individuos que deciden cómo y por qué los datos personales son manejados deben cumplir ciertos principios de la protección de datos, para asegurar que la información es utilizada adecuadamente.

La norma básica en nuestro marco legal es la *Ley Orgánica de 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal* (en adelante, LOPD).

Algunos autores denominan este derecho como de *autodeterminación informativa* y se trata de poder conocer y controlar la gestión de la información personal, esto es, qué información existe, quién tiene acceso a ella, quién tiene capacidad para crear y difundir información sobre terceras personas, para qué se usan estos datos personales, qué decisiones se toman con ellos, etc.

Desde un punto de vista práctico, es deseable que las organizaciones y las asociaciones de profesionales consensúen y regulen una serie de estándares o prácticas que se consideren respetuosas con el derecho a la privacidad y a la protección de datos personales.

*¿Qué son "**datos personales**"?*

Se entiende por "dato personal" cualquier información (numérica, alfabética, gráfica, fotográfica, acústica, etc.) relativa a una persona física identificada o identificable. Así, están bajo el ámbito de aplicación de la LOPD, los datos personales que se tratan con ocasión de tareas propias de la selección, la orientación, la terapia, la investigación, etc., esto es, distintas intervenciones que emplean tests y otros métodos como las entrevistas, etc. El término "identificable" no se aplica cuando se requeriría una gran cantidad de tiempo y de esfuerzo para identificar a una persona a partir de los datos utilizados en varios ficheros o documentos. Tampoco se aplica la normativa sobre protección de datos personales si la información es anónima o si se presenta como datos agregados (por ejemplo, el perfil de la estructura de edad de los trabajadores de una organización).

*¿Qué son "**datos especialmente protegidos**"?*

Algunos datos tienen la consideración de particularmente delicados, en cuanto a que pertenecen a la esfera más íntima de la persona o a que su comunicación pueden hacerla vulnerable, y por ello son reconocidos como datos especialmente protegidos, de tal manera que su tratamiento conlleva un plus de medidas para garantizar su seguridad. Estos datos son los que revelan, respecto a una persona, su ideología, afiliación sindical, religión, creencias, origen racial, salud, vida sexual e infracciones penales o administrativas.

*¿Qué significa "**tratamiento de datos**", sea manual o automático?*

La expresión "tratamiento de datos" incluye la recogida, conservación, combinación, comunicación o cualquier otra forma de utilización de datos personales, sea de forma manual o informatizada. En ocasiones, un tratamiento de datos es tanto manual como automático, pues es habitual combinar los métodos de archivado tradicionales con sistemas informáticos, de tal manera que éstos últimos conservan sólo una parte de los datos disponibles y remiten a los archivos para el resto de la información.

*¿Qué se entiende por "**calidad de los datos**"?*

Es uno de los principios básicos y garantiza a las personas que sus datos serán:

- recogidos por medios lícitos, leales y no fraudulentos
- tratados para propósitos explícitos y limitados y no para otros fines distintos.
- adecuados, pertinentes y no excesivos

- exactos y puestos al día
- no almacenados más tiempo que el necesario

*¿Qué es el **derecho de Información en la recogida de datos**?*

Las personas a las que se soliciten datos personales deberán ser previamente informadas de modo expreso de que existe un fichero o tratamiento de datos personales, de su finalidad y de los destinatarios de la información; de si es obligatorio o no responder a las preguntas, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; y de la identidad y dirección del responsable del tratamiento de datos (artículo 5, LOPD).

Esta información suele facilitarse de forma oral y a través de un impreso escrito o electrónico, en el cual se introducen las anteriores cláusulas informativas, y que puede ser entregado al cliente o puede exponerse en una zona, sea física o electrónica, que resulte visible para las personas.

La cuestión esencial es la siguiente: ¿Pueden los candidatos a un puesto o la persona que demanda una intervención o asesoramiento, etc., comprender las implicaciones de la información que tendrá que dar? Esto es especialmente importante cuando se realizan investigaciones sobre niños o personas con discapacidades mentales, en cuyo caso será necesario obtener el consentimiento de los tutores.

*¿Es necesario que el profesional de la Psicología solicite el **consentimiento del afectado para recoger sus datos**?*

Aunque, como norma general, es necesario el consentimiento inequívoco de una persona para tratar sus datos, en determinadas circunstancias no lo es: así, no se necesitará el consentimiento para tratar los datos cuando una persona acude a un psicólogo solicitándole sus servicios (artículo 6.2., de la LOPD, *relación negocial*), ni siquiera para recoger sus datos especialmente protegidos (artículo 7.6., de la LOPD). Pero, si la información obtenida va a ser utilizada para otros propósitos no obvios o esperables, tales como la publicidad de otros servicios psicológicos, debe obtenerse el consentimiento de la persona afectada. También será necesario el consentimiento expreso, generalmente firmado, para la participación voluntaria en investigaciones, cuando el psicólogo considere necesario solicitar documentaciones u otras informaciones de otras personas u organizaciones, tales como empleadores anteriores, otros profesionales, etc.

*La regulación en **códigos profesionales de los psicólogos** del **Consentimiento Informado y la Libertad de Consentimiento** de un cliente*

Las personas tienen el derecho de saber en qué se van a involucrar antes de hacer compromisos significativos. Este consentimiento informado y la libertad de consentimiento que se regula en los códigos éticos de práctica profesional hacen referencia no sólo a informar al cliente sobre el uso de sus datos personales y, en su caso, a obtener consentimiento para ello. Se trata de una práctica derivada del derecho de información de las personas para tomar decisiones, en cualquier momento, respecto a su participación en una actividad de índole psicológica.

En el Código Deontológico estatal de los Psicólogos, esta cuestión se aborda en los artículos 25 y 27 del Título III *De la Intervención*, en los cuales se especifica que el psicólogo ofrecerá información adecuada sobre las características de la relación establecida, los problemas que

está abordando, los objetivos que se propone y el método utilizado; asimismo, se favorecerá al máximo la capacidad de decisión bien informada del cliente.

Este consentimiento informado, distinto al contemplado por la LOPD en su artículo 6, ha de interpretarse no sólo como la firma de un formulario de consentimiento, sino como resultado de un acuerdo de trabajar en colaboración. En última instancia, subyace el deber ético de respetar e integrar, en la mayor medida posible, las opiniones y los deseos de los otros en relación con las decisiones que les afectan. En la obtención de consentimiento informado se ha de proveer, tanta información como la que una persona, familia, grupo o comunidad querría razonablemente conocer antes de tomar una decisión o de consentir respecto a una determinada actividad o intervención. Los psicólogos deben comunicar esta información en un lenguaje que las personas comprendan y deben asegurarse que efectivamente se ha producido tal comprensión. Concretamente, y según el *Code of Professional Ethics* de los psicólogos de Irlanda, la información proporcionada previa a la obtención del consentimiento informado ha de contener los siguientes puntos: propósito y naturaleza de la actividad o servicio; responsabilidades mutuas; beneficios y riesgos probables; alternativas; las consecuencias probables de la no intervención; la opción de negarse o retirarse de la intervención en cualquier momento, sin perjuicios; período de tiempo durante el cual el consentimiento está en vigor o se aplica; y cómo rescindir el consentimiento si se desea.

*El principio de la **Seguridad de los datos personales***

Las personas responsables de los ficheros están obligadas a establecer **medidas técnicas y organizativas** de uso de los sistemas de información para garantizar la seguridad de los datos**,** esto es, para asegurar que se restrinja el acceso a dichos datos, estén protegidos contra pérdidas y se excluya la posibilidad de acceder a ellos, utilizarlos, modificarlo o divulgarlos sin autorización. Las medidas técnicas pueden ser el uso de contraseñas, antivirus, etc.; las medidas organizativas implican la designación de responsables de ficheros, responsables de seguridad, la identificación de perfiles de usuarios de sistemas de información, etc. Ambos tipos de medidas se describen en un *Reglamento de Medidas de Seguridad*, que puede consultarse en la página web de la Agencia Vasca de Protección de Datos (www.avpd.es).

En el caso de entidades con un número considerable de trabajadores, estas medidas comprenden una vigilancia o control de todas las personas que trabajan con los servicios informáticos (quién ha accedido a qué, permisos para acceder a informaciones, etc.). Esta vigilancia ha de compensarse mediante una limitación estricta de los usos que se hacen de los datos personales reunidos por estos medios.

En el caso de los profesionales de la psicología, mucha de la información sobre sus clientes que conocen contiene datos especialmente protegidos, por lo que tendrán que aplicar medidas de seguridad de nivel alto. Algunas de estas medidas, tanto en archivos manuales como informatizados, consisten en cifrar o hacer ininteligibles y no manipulables los datos personales, bien cuando se transmiten a través de redes de telecomunicaciones (correo electrónico, etc.) bien cuando se distribuyen mediante soportes móviles como los lápices ópticos o los ordenadores portátiles.

Ciertamente, algunas otras medidas de seguridad de nivel alto pueden estar atenuadas en su aplicación cuando sólo sea un profesional el que maneja la información personal y no comparta con otros profesionales los sistemas de información que contienen los datos personales manejados.

*El **deber de secreto** y el principio de confidencialidad de la información*

El deber de secreto, regulado en el artículo 10 de la LOPD, y el reconocimiento de la confidencialidad de la información personal, constituyen un principio básico del respeto a la privacidad y, por ende, de la protección de datos personales.

A su vez, en el Código Deontológico de los Psicólogos el secreto profesional se regula describiendo la norma general y distintas situaciones prácticas. Así, el deber de secreto se exime sólo por consentimiento expreso de la persona afectada (artículo 40) y para poder comunicar información a terceras personas es necesaria una autorización previa y expresa (artículo 41). Los informes elaborados a petición de terceros son también confidenciales a todos los efectos y en los mismos se han de incluir sólo los datos personales imprescindibles (artículo 43). La exposición didáctica y la divulgación científica de datos y casos ilustrativos deben hacerse convirtiendo la información en anónima o, en su defecto, con consentimiento previo explícito (artículo 45). También es imprescindible el consentimiento de la persona afectada para autorizar la presencia innecesaria de terceras personas, por ejemplo, alumnos en prácticas o profesionales en formación (artículo 47), y finalmente, el cumplimiento del secreto profesional no queda eximido aunque fallezca el cliente o desaparezca la organización empleadora del profesional (artículo 49).

En síntesis, la información personal es confidencial y sólo es posible compartirla con el consentimiento informado de las personas involucradas o de tal modo que los individuos no puedan ser identificados, excepto cuando sea requerido o justificado por ley o en circunstancias de posible grave daño físico o muerte.

En este sentido, es preciso notar que no se pueden facilitar datos personales ni a familiares directos sin consentimiento de la persona implicada. La LOPD califica como infracción muy grave la vulneración del deber de guardar secreto sobre los datos especialmente protegidos y, además, regula un régimen sancionador con relación a las infracciones leves, graves y muy graves.

*Algunos **derechos individuales** relacionados con la protección de datos personales*

Además del **derecho a la información** en la recogida de datos, las personas tienen derecho a ser informadas con regularidad sobre los datos personales que les conciernen y sobre el tratamiento de éstos.

Así, por ejemplo, y según lo contemplado en el Código Deontológico de Psicólogos en su artículo 42, el sujeto de un Informe Psicológico tiene derecho a ser informado del hecho de una evaluación o una intervención y a conocer el contenido del mismo, aunque la solicitud de su realización haya sido hecha por otras personas, tales como jueces, empleadores, profesionales de la enseñanza, etc., siempre que de ello no se derive un grave perjuicio para la persona o para el psicólogo,

Las personas **deben tener acceso a todos sus datos personales**, independientemente de que sean objeto de tratamiento automático o de que los conserven en un expediente manual. El derecho a saber cómo se tratan sus datos personales debe comprender el de examinar y obtener copia de todos ellos (derecho de acceso regulado en la LOPD). La única información que puede no ser accesible al titular de un dato es la información que revela la identidad de otros individuos, tales como el autor de una referencia laboral.

Las personas tienen derecho a solicitar que se supriman o rectifiquen los datos personales inexactos o incompletos, así como los sometidos a un tratamiento que vulnere las leyes de aplicación (**derecho de rectificación y cancelación,** regulado en la LOPD). En algunas circunstancias, la persona también pueden impedir que se use determinada información sobre ella o que se haga de una manera concreta (**derecho de oposición,** en la LOPD).

El **derecho de impugnación de valoraciones** reconoce que las decisiones relativas a una persona no deberían basarse exclusivamente en un tratamiento informático de los datos personales que a ella se refieran. Esto es, los procedimientos informáticos no dispensan a los profesionales de consultar todos los datos necesarios para evaluar de manera acertada los resultados del tratamiento. Por ejemplo, tomar decisiones de despido en base a datos cuantitativos de absentismo, sin calibrar las causas del mismo, no está justificado. Por ello, se recomienda rechazar toda adopción mecánica de decisiones y se prefiere en lugar de ello una evaluación claramente individualizada de las personas. En el mismo sentido, en el área de Psicología del Trabajo y de las Organizaciones, es razonable proponer que los datos personales obtenidos por medios de vigilancia electrónica no sean los únicos factores de evaluación profesional del trabajador.

Una vez descritos algunos conceptos básicos de la protección de datos personales, es útil terminar esta presentación del tema con una visión cronológica de las principales fases u operaciones comunes en el tratamiento de datos personales.

Fase 1. Declaración de Ficheros de Datos Personales a la Agencia Española de Protección de Datos (AEPD)

El primer paso para un eficiente uso de la información es organizar en ficheros, manuales y/o informatizados, los tipos de datos personales que se manejan y determinar sus usos.

Por ejemplo, para profesionales autónomos que procuran sus servicios a personas, es recomendable organizar la información personal utilizada, al menos, en dos ficheros distintos:

- un fichero de clientes, que incluye datos de identificación y contacto para el mantenimiento de la relación contractual. Este fichero requiere medidas de seguridad sólo de nivel bajo.

- Un fichero de personas atendidas, que comprende la información personal propia de una historia clínica o de la intervención, sea ésta diagnóstica, terapéutica, de orientación y asesoramiento, etc. Muchos de estos datos pertenecen a la esfera íntima de la persona y requieren medidas de seguridad de nivel alto.

Después de decidir la organización de la información en ficheros, los psicólogos, como responsables de los ficheros, han de realizar una declaración formal de los ficheros de datos personales en la *Agencia Española de Protección de Datos* (www.agpd.es) y ésta procederá a su inscripción en el Registro Oficial de la AEPD. La AEPD tiene constancia del tipo de datos manejados (datos escolares, datos psicológicos, etc.), pero en ningún caso de los datos concretos relativos a clientes atendidos por los profesionales.

Además de la Agencia Española, existen Agencias de Protección de Datos en Cataluña, Madrid y Euskadi; estas agencias autonómicas tienen competencias de control sólo sobre las administraciones públicas de su comunidad autónoma.

Fase 2. Adopción de medidas de seguridad de la información

De forma previa al acopio de datos personales, que tiene lugar cuando se inicia una relación profesional con un cliente, cuando se planifica una investigación o bien cuando se seleccionan datos sobre personas para ilustrar un caso con fines didácticos, en un momento anterior a la realización de estas tareas han de identificarse y aplicarse las medidas técnicas y organizativas que correspondan según las características de los datos personales que vayan a tratarse y los soportes manuales o automatizados en los que se archiven. Para recordar algunas ideas generales sobre este tema, se remite nuevamente al lector al apartado de *El Principio de la Seguridad de los datos personales*.

Fase 3. Recogida de datos personales

En esta operación, son particularmente importantes algunos de los conceptos descritos anteriormente como por ejemplo: el momento de informar a la persona sobre sus derechos, de requerir su consentimiento para solicitar o comunicar datos personales a terceras personas o entidades, de velar por la calidad de los datos que se van a acopiar, etc.

Probablemente, la mejor manera de preservar la confidencialidad es, en primer lugar, evitar recoger más información de la necesaria, pues de esta manera no puede ser mal utilizada. Por ejemplo, los formularios y las entrevistas en selección de personal no deberían ser excesivas ni preguntar cuestiones irrelevantes; así, en la mayoría de las ocasiones no es necesario preguntar a las personas acerca de su vida fuera del trabajo.

Si bien la persona debería ser quién proporcione todo los datos personales, si resultara necesario **recabar datos personales facilitados por terceros**, se debería informar por adelantado a la persona, que habrá de dar su **consentimiento explícito**. El profesional debería indicar la finalidad del tratamiento de los datos, las fuentes y los medios que se propone utilizar, el tipo de datos que vayan a acopiarse y las consecuencias, si las hubiere, de negar el consentimiento.

Si el profesional hubiere obtenido el consentimiento de la persona para el acopio de datos personales, debería **cerciorarse de que toda persona u organización a la que él solicite datos tenga presente en todo momento la finalidad de la indagación**, para evitar toda interpretación falsa o engañosa.

Se menciona aquí la cuestión de la idoneidad de los datos recabados para una determinada intervención psicológica sin pretender especificar, en ningún caso, cuáles son los tipos de datos idóneos. Y esto porque lo que el profesional necesite saber dependerá de la persona, de su situación, del objetivo de la intervención psicológica, etc. En lugar de enumerar todos los datos que puedan manejarse, es más lógico enunciar reglas destinadas a garantizar la claridad de la operación y el conocimiento de la misma por la persona o personas afectadas.

Fase 4. Comunicación de Datos

Los datos acerca de personas deberían ser transmitidos de una manera segura y confidencial. Al menos, las comunicaciones internas que contengan datos personales deberían ser introducidas en sobre cerrado cuando vayan a ser enviadas a otra persona. No debería ser posible encontrar datos personales a la vista sobre fotocopiadoras, en mesas o en salas de reuniones. Los datos personales enviados por Internet deberían ser encriptados, por ejemplo, cuando los candidatos a puestos de trabajo cumplimentan los formularios de solicitud vía electrónica. Los datos personales no deberían ser enviados por fax a máquinas de uso compartido, a menos que se efectúe una llamada telefónica justo antes del envío para asegurar la confidencialidad de la información.

Si se pide a la persona que firme una **declaración para autorizar al profesional a reunir o comunicar información sobre ella,** esta declaración debería estar redactada con sencillez, mencionándose específicamente en la misma las personas, instituciones u organizaciones que la recibirán, los datos personales que serán comunicados, la finalidad del acopio de datos personales y el tiempo durante el cual su contenido podrá utilizarse.

Fase 5. Conservación y Borrado de Datos

La información sobre personas ha de ser guardada en un lugar seguro – generalmente en un armario– al que sólo tengan acceso personas específicas. El almacenamiento computerizado de datos especialmente delicados, tales como formularios de recogida de datos para la historia clínica, informes, etc., conlleva riesgos potencialmente más graves que su archivo manual, en el sentido de que puede divulgarse por medios telemáticos dificultando su control posterior. Por ello, han de aplicarse las medidas de seguridad que resulten adecuadas y sobre las que ya se han apuntado algunas ideas básicas en el apartado de la *Seguridad de los Datos Personales.*

Como norma, la información debería ser destruida tan pronto como sea usada para la finalidad para la que se obtuvo. Por ejemplo, los datos de candidatos a un puesto obtenidos en la fase de reclutamiento no deben ser transferidos rutinariamente a archivos de personal, sino solamente la información que sea relevante para el empleo y el resto debe ser destruido, después de transcurridos los períodos de tiempo suficientes para dar respuesta a los procedimientos legales de los que pudieran ser objeto.

En este escrito se ha pretendido dar una visión global, y por ello muy simplificada, de cómo el derecho a la privacidad y a la protección de datos personales afecta a la gestión de la información que manejan los profesionales de la Psicología.

En este área de conocimiento, una línea de actuación futura puede ser evaluar la necesidad de elaborar, de forma consensuada, nuevos estándares de actuación específicos para los profesionales de la Psicología, que proporcionen respuestas más comprensivas a los nuevos retos éticos que el derecho a la protección de datos y el derecho a la información de las personas traen consigo.

Edurne Barañano

Agencia Vasca de Protección de Datos
Lda. Psicología
Postgrado en Gestión Formación Continua en las Organizaciones