COVID-19, TELETRABAJO Y ADMINISTRACIÓN DE JUSTICIA: O DE CÓMO OTROS VIRUS ENFERMAN NUESTRO ESTADO DE DERECHO

Covid-19, teleworking and administration of justice: or how other viruses make our rule of law sick

Por Fernando Javier Cremades López de Teruel

Letrado de la Administración de Justicia. España.
cremades_ferlop@gva.es

Artículo recibido: 15/05/2020 | Artículo aceptado: 20/06/2020

RESUMEN

Tiempo hemos dedicado estos últimos años a reflexionar sobre la protección de datos de carácter personal y su cumplimiento, aplicación e influencia en el Poder Judicial. Ahora, tras la declaración de un Estado de Alarma y en atónita expectación por los acontecimientos que se han sucedido, y especialmente, por las decisiones que se han adoptado, acometemos el presente trabajo para que sirva, tal vez, de lúgubre testimonio de la garantía de un derecho fundamental condenado, en el ámbito judicial, a ser mera nominalidad por no quedar ya, probablemente, datos personales que proteger.

ABSTRACT

In recent years we have spent time reflecting on the protection of personal data and its compliance, application and influence in the Judiciary. Now, after the declaration of a State of Alarma and in astonished expectation for the events that have occurred, and especially, for the decisions that have been adopted, we undertake this work so that it may serve, perhaps, as a lugrubious testimony of the garantee of a fundamental right condemned, in the judicial sphere, to be a mere nominality because there is probably no longer personal data to protect.

PALABRAS CLAVE

Protección de datos, derecho fundamental, seguridad jurídica, teletrabajo, intimidad, separación de poderes.

KEYWORDS

Data protection, fundamental right, legal security, teleworking, privacy, separation of powers.

Sumario: 1. Alarma de Estado. 2. La mercancía. 3. El productor. 4. El mercado. 5. El proveedor.

1. Alarma de Estado

No pretendemos con este trabajo hacer un ejercicio valorativo de cómo ha soportado la Administración de Justicia el test de resistencia a que ha sido sometida por la declaración del Estado de Alarma como consecuencia de la crisis sanitaria por la propagación del Covid-19. Y no pretende serlo pues su redacción discurre durante la vigencia del citado Estado de Alarma y conviviendo con las múltiples vicisitudes que día a día acompañan esta situación.

Tampoco se pretende aquí hacer relación de los precipitados y caóticos aconteceres que dominan estos días el sector judicial, ni un ejercicio de análisis sobre el comportamiento endémico de los distintos operadores, tradicionalmente en disputa, en el sector de la justicia que parecen estar, con franco empeño, en plena disputa estratégica para un mejor posicionamiento, no se sabe muy bien para qué, para cuándo, ni para quién.

Tras dedicar estos últimos años a publicar sendos trabajos sobre la protección de datos de carácter personal y su cumplimiento, aplicación e influencia en el Poder Judicial, ahora, en pleno estado de confinamiento y en atónita expectación por los acontecimientos que se suceden, y por las decisiones que se adoptan, acometemos el presente para que, tal vez, sirva de testimonio del lúgubre epílogo de la garantía, protección y cumplimiento del derecho fundamental a la protección de los datos personales.

A través de esos trabajos hemos ido analizando detenidamente los entornos normativos que deben envolver la actividad del sistema judicial en materia de protección de los datos de carácter personal, y con ello hemos ido alcanzando una serie de conclusiones que es necesario rescatar aquí a fin de obtener una muy breve, pero necesario, punto de partida.

2. La mercancía

Para llegar a la conclusión que declara el título de este trabajo hemos de partir de la enumeración de una serie de evidencias:

a) el sistema normativo en materia de protección de datos de carácter personal pasa por la primacía y prevalencia del Reglamento (UE) 2016/679;

b) la protección de datos de carácter personal es un derecho fundamental de las personas;

c) en el sistema judicial no hay constituida una autoridad de control que garantice la aplicación del Reglamento (UE) 2016/679 (en adelante, RGPD) en los términos que éste exige;

d) el Ministerio de Justicia y las Comunidades Autónomas con competencias transferidas en materia de justicia tienen el control absoluto, la llave maestra, de todo el sistema de almacenamiento electrónico de datos de carácter personal que manejan los juzgados y tribunales en el ejercicio de sus funciones judiciales; y

e) en la protección de los datos que manejan los juzgados y tribunales en el ejercicio de su función judicial no se cumple la esencial separación de poderes con el Poder Ejecutivo, tal y como obliga la Unión Europea.

Detengámonos unos párrafos en estas evidencias antes de ingresar en la materia que informa este trabajo.

El tratamiento que hace la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales de la protección de datos en el ámbito del Poder Judicial resulta escueto y remite el tratamiento de datos llevado a cabo con ocasión de la tramitación por los órganos judiciales de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina Judicial, a lo «dispuesto en el Reglamento (UE) 2016/679 y la presente ley orgánica, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, que le sean aplicables». Así pues, para una adecuada aproximación a esta materia es necesario atender al sistema de fuentes normativas que regula la protección de datos de carácter personal en el ámbito del Poder Judicial, esto es:

1º Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, RGPD).

2º La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPD).

3º Las especialidades recogidas en la Ley Orgánica del Poder del Poder Judicial (arts. 236 bis a 236 decies), (en adelante, LOPJ) en lo que no se opongan al contenido del RGPD.

4º El RD 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la LO 15/1999, de 13 de diciembre, en lo que no se oponga y no haya sido derogado, aunque sea de forma tácita, por el RGPD y la LOPD.

5º Reglamento 1/2005, aspectos accesorios de las actuaciones judiciales, en lo que no se oponga o haya sido derogado, aunque sea de forma tácita, por el RGPD, la LOPD y la LOPJ.

La protección de datos de carácter personal ha sido una gran preocupación en Europa tras la segunda guerra mundial habida cuenta el éxito que los servicios de inteligencia del régimen nazi habían tenido en el tratamiento de los datos personales, convirtiendo meros ficheros de datos creados, muchos de ellos, en los Estados ocupados con fines de servicio y

gestión de recursos públicos en verdaderas armas de exterminio. Un ejemplo fue el caso de Holanda donde un censo creado para gestionar adecuadamente los recursos públicos en favor de las distintas culturas fue utilizado por los nazis para una finalidad completamente distinta. Sólo sobrevivió el 10% de los judíos holandeses. Fue el uso del dato y no su publicidad lo que hizo de esa información un arma extraordinaria.

La construcción europea del derecho fundamental a la protección de datos personales nació con el Tribunal Constitucional Federal de Alemania y su sentencia de 1983 en la que vino a examinar la compatibilidad de la Ley Fundamental de Bonn con la impugnada ley federal del censo poblacional. Con esta ley se solicitaba a los ciudadanos que respondiesen un interrogatorio con el único propósito, a partir de los datos obtenidos, de mejorar y optimizar el aprovechamiento de los recursos sociales. El problema surgía cuando los datos aportados, anónimos e inocentes, fueran cotejados con los registrados en los Estados Federados -Länder-, lo que podía permitir identificar a sus titulares, es decir, había un riesgo de individualización.

Lo singular de esta impugnación al Tribunal Constitucional Federal alemán no fue la pretensión de proteger la información íntima de una persona sino el hecho de que los datos aportados por ella, una vez sometidos a las correspondientes operaciones de tratamiento, podían relacionarse con otros datos de esa misma persona y posibilitando, finalmente, revelar los aspectos más variados de su vida y comportamiento. Los recurrentes centraron su atención, por lo tanto, no en la protección estricta del dato personal, que por sí solo puede resultar intrascendente, sino en la limitación del tratamiento informatizado de cualquier dato de carácter personal, que conduce al fenómeno que ellos denominan "enmallamiento", esto es, la asociación de datos a modo de una malla que permita identificar patrones de comportamiento y aspectos secuenciados de la vida de las personas.

Este fue el elemento fundamental de la impugnación al no limitar su planteamiento a solicitar la tutela y protección a los datos denominados sensibles, sino también para aquellos que sin pertenecer a la esfera más próxima al individuo, son susceptibles de dañar su imagen o el ejercicio pleno de sus derechos.

En la Unión Europea este derecho fundamental aparece expresamente reconocido en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea (2016/C 202/02) bajo el título "Protección de datos de carácter personal"[1], y tiene su traducción aplicativa directa en el RGPD, en cuyo artículo

[1] CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (2016/C 202/02). "Artículo 8. Protección de datos de carácter personal 1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratarán de

1.2 se dispone que "El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales".

En nuestro ordenamiento jurídico interno, el derecho fundamental a la protección de datos personales se recoge implícitamente en el artículo 18.4 de la Constitución Española (en adelante, CE)[2]; un derecho que el Tribunal Constitucional configuró como autónomo a partir, especialmente, de las sentencias 290/2000 y 292/2000, y que a partir de la entrada en vigor la señalada normativa europea, en tanto que prevalente en nuestro sistema de fuentes, presenta ya una identidad y sustantividad indiscutible, a la par que el resto de derechos fundamentales reconocidos.

Así pues, el derecho a la protección de datos de carácter personal es un derecho fundamental de las personas sujeto a las mismas exigencias de respeto, garantías de ejercicio y amparo de protección que el resto de derechos fundamentales.

Ya la Carta de los Derechos Fundamentales de la Unión Europea establece en el apartado 3 de su artículo 8 que el respeto del derecho de las personas a la protección de los datos de carácter personal que le conciernan "estará sujeto al control de una autoridad independiente", lo que nos conduce a la determinación de esta autoridad.

Hasta el 25 de mayo de 2018, fecha de entrada en vigor del RGPD, la función de autoridad de control sobre las operaciones de tratamiento de los juzgados y tribunales en el ejercicio de sus funciones, por aplicación de la LOPJ, la venía ostentando, formal y nominalmente, el Consejo General del Poder Judicial (en adelante, CGPJ). Entrado en vigor el RGPD las autoridades de control para poder ser tales deben cumplir un estricto catálogo de requisitos que son primera exigencia de su independencia y propia garantía de la función que tienen encomendada. La Ley Orgánica 3/2018 lo reitera al remitir el tratamiento de datos llevado a cabo con ocasión de la tramitación por los órganos judiciales de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina Judicial, a lo "dispuesto en el Reglamento (UE) 2016/679 y la presente ley orgánica, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, que le sean aplicables".

---

modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente".

[2] Artículo 18.4 CE: "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."

Así pues, solo será autoridad de control el organismo específico del sistema judicial al que así se encomiende y que se configure con los requisitos que exige el RGPD, y no otra cosa, en los términos que exige el considerando 20 del propio Reglamento.

¿Y qué requisitos son estos? Lo concreta el RGPD en sus artículos 51 a 59, que podemos sintetizar del siguiente modo:

1º. La autoridad de control ha de actuar con total independencia en el desempeño de sus funciones y en el ejercicio de sus poderes de conformidad con el Reglamento UE.

2º. La autoridad de control que se constituya habrá de disponer en todo momento de los recursos humanos, técnicos y financieros, así como de los locales y las infraestructuras necesarios para el cumplimiento efectivo de sus funciones y el ejercicio de sus poderes.

3º. El miembro o los miembros de la autoridad de control serán ajenos a toda influencia externa, ya sea directa o indirecta, y no solicitarán ni admitirán ninguna instrucción.

4º. El miembro o los miembros de la autoridad de control se abstendrán de cualquier acción que sea incompatible con sus funciones y no participarán, mientras dure su mandato, en ninguna actividad profesional que sea incompatible, remunerada o no.

5º. La autoridad de control que se constituya habrá de elegir y disponer de su propio personal, que estará sujeto a la autoridad exclusiva del miembro o miembros de la propia autoridad de control interesada.

6º. La autoridad de control habrá de estar sujeta a un control financiero que no afecte a su independencia y que disponga de un presupuesto anual, público e independiente.

7º. Los miembros de la autoridad de control:

a) han de ser nombrados mediante un procedimiento transparente

b) han de poseer la titulación, la experiencia y las aptitudes, en particular en el ámbito de la protección de datos personales, necesarias para el cumplimiento de sus funciones y el ejercicio de sus poderes.

c) concluirán sus funciones en caso de terminación del mandato, dimisión o jubilación obligatoria, de conformidad con el Derecho del Estado miembro de que se trate.

d) sólo podrán ser destituidos en caso de conducta irregular grave o si deja de cumplir las condiciones exigidas en el desempeño de sus funciones.

8º. Se habrá de regular por ley:

a) la creación de la propia autoridad de control;

b) las cualificaciones y condiciones de idoneidad necesarias para ser nombrado miembro de la autoridad de control;

c) las normas y los procedimientos para el nombramiento del miembro o miembros de cada autoridad de control;

d) la duración del mandato del miembro o los miembros de cada autoridad de control, que habrá de ser no inferior a cuatro años;

e) el carácter renovable o no del mandato del miembro o los miembros de cada autoridad de control y, en su caso, el número de veces que podrá renovarse;

f) las condiciones por las que se rigen las obligaciones del miembro o los miembros y del personal de cada autoridad de control, las prohibiciones relativas a acciones, ocupaciones y prestaciones incompatibles con el cargo durante el mandato y después del mismo, y las normas que rigen el cese en el empleo.

9º. Finalmente, el miembro o miembros y el personal de la autoridad de control estarán sujetos, de conformidad con el Derecho de la Unión o de los Estados miembros, al deber de secreto profesional, tanto durante su mandato como después del mismo, con relación a las informaciones confidenciales de las que hayan tenido conocimiento en el cumplimiento de sus funciones o el ejercicio de sus poderes.

La cuestión que hemos de respondernos, pues, es si el CGPJ, tal cual está constituido, cumple estas exigencias, y la respuesta ha de ser concluyentemente negativa.

El CGPJ es un órgano de naturaleza administrativo y, en tal condición, el propio art. 236 decies de la LOPJ, ya establece que el tratamiento de datos de carácter personal llevado a cabo en el ejercicio de sus competencias queda sometido a la legislación general sobre protección de datos, esto es, a la Agencia Española de Protección de Datos (en adelante, AEPD). De este modo, si el CGPJ está sujeto a la autoridad de control del poder ejecutivo no puede, por razón obvia, preservar la independencia del poder judicial en materia de protección de datos que tiene por principio primero y fundamental evitar que los datos de este poder pasen a manos de otro poder sin un previo control y tratamiento, en los términos que exige el RGPD.

¿Es entonces el CGPJ la autoridad de control independiente incardinada en el sistema judicial? La respuesta ha de ser categóricamente negativa: porque no cumple los requisitos que el RGPD ordena para toda autoridad de control en sus artículos 51 a 59; porque la propia LOPJ lo sujeta, por su propia naturaleza de órgano administrativo-gubernativo, al control por la AEPD, autoridad de control incardinada en el Poder Ejecutivo del Estado; y porque, finalmente, esta sujeción al Poder Ejecutivo le impide por definición preservar la independencia del Poder Judicial en materia de protección de datos que tiene por principio primero y fundamental evitar que los datos de este Poder pasen a manos de

otro Poder del Estado sin un previo control y tratamiento, en los términos que exige el RGPD.

Concluimos, pues, que en el sistema judicial español no hay una autoridad de control y por, ende, no existe el organismo encargado de supervisar la aplicación del RGPD.

El Ministerio de Justicia y las Comunidades Autónomas con competencias transferidas en materia de justicia, Poder Ejecutivo del Estado, contratan y controlan las herramientas informáticas que se utilizan para gestionar y tramitar los procedimientos judiciales; controlan el acceso a los soportes, servidores, bases de datos y terminales informáticas de los juzgados y tribunales; intervienen en la programación y diseño de las aplicaciones y programas informáticos utilizados en la Administración de Justicia; y tienen bajo su dependencia directa a un personal, que accede, puede acceder, o puede permitir el acceso, a toda suerte de aplicaciones, soportes, programas y herramientas informáticas, ficheros, locales, equipos, sistemas, servidores y demás infraestructuras electrónicas destinadas o aplicadas al uso de juzgados y tribunales. En definitiva, estos órganos tienen el control absoluto, la llave maestra de todo el sistema informático y electrónico en el que se plasman todos los datos que aportan los ciudadanos a un procedimiento judicial o se obtienen para fines judiciales.

El RGPD exige que el tratamiento de datos que se realice cuando los tribunales actúen en ejercicio de su función judicial ha de estar sujeto al control, no por las autoridades de control incardinadas en el ámbito del poder ejecutivo, como es el caso de la AEPD, sino por "organismos específicos establecidos dentro del sistema judicial", esto es, por una autoridad de control propia dentro del sistema judicial que, constituida con los requisitos que ordena el propio RGPD, garantice el cumplimiento del Reglamento. Y ello por una razón básica inherente a todo Estado de configuración democrática: la preservación de la separación de poderes, también en el tratamiento de datos de carácter personal, con el evidente propósito que explicita el propio considerando 20 del RGPD[3], esto es, preservar la independencia del Poder Judicial.

[3] Considerando 20 del REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016: "(...) A fin de preservar la independencia del poder judicial en el desempeño de sus funciones, incluida la toma de decisiones, la competencia de las autoridades de control no debe abarcar el tratamiento de datos personales cuando los tribunales actúen en ejercicio de su función judicial. El control de esas operaciones de tratamiento de datos ha de poder encomendarse a organismos específicos establecidos dentro del sistema judicial del Estado miembro, los cuales deben, en particular, garantizar el cumplimiento de las normas del presente Reglamento, concienciar más a los miembros del poder judicial acerca de sus obligaciones en virtud de este y atender las reclamaciones en relación con tales operaciones de tratamiento de datos".

Por lo tanto, si ya hemos concluido que el Poder Ejecutivo es el dueño de toda la infraestructura técnica, que tiene bajo su directa dependencia al personal técnico que maneja toda esa infraestructura, y que dentro del sistema judicial no hay una autoridad de control que garantice el cumplimiento del RGPD, no podemos llegar a otra evidencia que el control material y efectivo de aquello que está llamado legalmente a ser protegido, esto es, los ficheros de los datos judiciales, está, precisamente, en manos de quien pretende evitar el RGPD pues compromete la independencia del Poder Judicial. Hay pues una absoluta confusión entre el dueño de la "caja" (los servidores, soportes, programas y herramientas informáticas) y el dueño de su "contenido" (los datos), una confusión que no es más que un terreno compartido y sin fronteras entre dos Poderes del Estado.

3. El productor

Como ya hemos anticipado al iniciar este trabajo, no es propósito aquí efectuar una relación y, menos aún, una valoración de las decisiones adoptadas en el ámbito judicial por la autoridad competente durante el Estado de Alarma, por muy variados calificativos que puedan merecer, por su grado de idoneidad, oportunidad o, simplemente, mera y simple razonabilidad. Y tampoco de las decisiones que se han tomado en este mismo ámbito judicial durante los últimos 15 años, bajo el eslogan de planes de modernización, digitalización judicial, interconexión e intercambio electrónico de documentos, transparencia y avance tecnológico y el apoyo de centenares de millones de euros dando fe presupuestada en boletines y diarios oficiales de una acción política aparentemente encomendada a ese empeño modernizador.

Como decimos no es este el propósito del presente trabajo, sino tomar como punto de partida este ecosistema judicial resultante cuando llegado el momento de la necesidad durante esta crisis de que se moviera un papel en los juzgados y tribunales, esas mismas administraciones prestacionales impulsoras de modernización, tecnología y digitalización terminaron por solicitar prestado a los distintos cuerpos funcionariales sus equipos informáticos domésticos, señales de internet y fluido eléctrico para dar forma a eso que se ha dado en llamar teletrabajo, una asignatura pendiente en España aunque no tanto por falta de recursos tecnológicos sino de cultura laboral.

La necesidad ha irrumpido abruptamente y lo que era hasta hace bien poco una opción anecdótica se ha tenido que asumir con necesidad y urgencia estratégica y en cuestión de días. Las empresas se han tratado de dotar rápidamente de infraestructuras adecuadas, aunque en muchos casos no haya sido posible o lo hayan hecho con muchas limitaciones. En la Administración de Justicia, además, con apreciable imprudencia y desprecio por el material tan sensible que maneja.

El propósito de las Administraciones prestacionales (Ministerio de Justicia y Comunidades Autónomas) ha sido tratar de que el funcionario, desde su casa y utilizando su equipo informático doméstico, se conectara a una red privada virtual (VPN) que da acceso al servidor en cuyo seno está la llamada sede judicial, con el sistema de gestión procesal y demás herramientas judiciales.

¿Ordenador doméstico? Es un dicho habitual entre los profesionales de la informática que el ordenador más seguro es el que está todavía precintado y en su embalaje original. A partir de aquí toda contaminación es posible, más que probable y, muy posiblemente, segura. Cuando hablamos de informática en red hay que hablar necesariamente de ciberseguridad, esto es, la práctica de defender los ordenadores, los servidores, las redes y los datos de los posibles ataques maliciosos. ¿Y cómo se presenta la ciberseguridad en los hogares españoles? Veamos unos datos a partir del "Estudio sobre la Ciberseguridad y Confianza en los hogares españoles" elaborado por el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) de mayo de 2018.

El 72,4 % de los ordenadores domésticos de los hogares españoles están infectados con algún código malicioso (malware), presentando en la práctica totalidad de los casos (72,8 %) un nivel de riesgo alto debido al potencial peligro que suponen estos archivos maliciosos. Se entiende peligrosidad alta aquellos casos de archivos que permiten al atacante el acceso remoto al sistema de la víctima, facilitan la obtención de información sensible y sirven de pasarelas para atacar otros equipos o sistemas. El 68,5%, casi 7 de cada 10 usuarios, considera que su equipo doméstico está razonablemente protegido frente a las potenciales amenazas de Internet. El 40,3% de los usuarios desconoce si su red Wi-Fi está protegida o desconoce el sistema utilizado para protegerla.

¿Red privada virtual?. VPN son las siglas de Virtual Private Network o red privada virtual. Con este concepto se alude a una modalidad de conexión que permite que un conjunto de dispositivos puedan compartir archivos, programas y herramientas sin necesidad de estar físicamente conectados entre sí, sino a través de Internet, aunque con una diferencia esencial con el uso habitual que le damos a esta red de comunicación. Si habitualmente cuando navegamos el ordenador doméstico se pone en contacto con nuestro proveedor de Internet para que, a su vez, nos ponga en contacto con el servicio web al que pretendemos acceder, por ejemplo *Youtube*, cuando nos conectamos a una VPN nuestro tráfico de red se sigue dirigiendo a nuestro proveedor de Internet pero éste nos conectará directamente al servidor VPN creando lo que se ha venido en llamar un "túnel de datos". Teóricamente, y aquí empezamos con los actos de fe, la conexión debe estar cifrada y el proveedor de Internet no debe saber dónde

estamos accediendo, pues nuestra salida a Internet se hace a través del servidor VPN.

Una de las más importantes funcionalidades de las conexiones VPN es la aplicada al teletrabajo. Una de sus ventajas teóricas es su mayor seguridad, pues realizar la conexión a la red común del centro de trabajo a través de Internet, sin más, es realmente temerario aún cuando se tenga protección a través de una contraseña. Con la conexión VPN el acceso está protegido, la conexión debe estar teóricamente cifrada y el trabajador tiene el mismo acceso como si estuviera presencialmente en el espacio protegido del centro de trabajo.

Ahora bien, si se desconfía de los peligros de una conexión pura y simple a través de Internet, ahora debemos depositar toda nuestra fe en el servidor de VPN dado que tendría la posibilidad de capturar todo nuestro tráfico y guardar registros de todo lo que hacemos. Es decir, es como tener el enemigo en casa y mirando absolutamente todo lo que hacemos.

Y aún más, en la mayoría de los casos la conexión doméstica a Internet se realiza a través de un router de los que habitualmente proporcionan las operadoras de telecomunicaciones, de calidad media-baja, que son fácilmente atacables y permiten que, a través de ellos, se pueda acceder maliciosamente al ordenador utilizado para teletrabajar. Una vez el hacker ingresa en el ordenador puede fácilmente acceder al servidor, aunque se esté haciendo uso de una VPN y una vez dentro tiene a su disposición toda la información de la red privada así como de cada uno de los terminales conectados.

El uso de servicios VPN ha aumentado mucho en los últimos tiempos, no solo por el creciente recurso al teletrabajo sino también por las ventajas de la "desconexión" física de las organizaciones. Precisamente por eso son uno de los principales objetivos de los ciberdelincuentes que están rastreando permanentemente vulnerabilidades en los servicios VPN para poder atacarlos, especialmente durante esta crisis sanitaria en que decisiones precipitadas, poco vigilantes e indiligentes están siendo reclamo para los piratas informáticos.

4. El mercado

Decíamos más arriba que las conexiones VPN ofrecen una mayor privacidad al ser un entorno protegido, ahora bien esa privacidad no significa anonimato. El proveedor VPN puede ver y controlar la actividad de los usuarios. Muchos servicios VPN manifiestan operar bajo una política de no guardar registros y, por lo tanto, no recopilar, almacenar ni compartir información sobre la actividad de los usuarios. Aunque esto es, en sí, otro acto de fe, como los que ya hemos relatado con anterioridad. Se nos pide confianza sin otra garantía que esa.

Como dijo Matthew Guariglia, analista de políticas de la Electronic Frontier Foundation, una organización sin fines de lucro dedicada a la defensa

de los derechos digitales, "Cuando le entregas tus datos a una compañía, no tienes idea de quién más tendrá acceso a ellos, porque gran parte del proceso ocurre detrás de la caja negra del hermetismo empresarial"[4].

¿Y qué valor tienen esos datos? Incuestionablemente, económico. Tienen su carta de precios y su mercado de compraventa. Aunque no hay cifras oficiales, investigaciones como la llevada a cabo por la compañía británica Experian permiten hacernos una idea de los precios que se manejan en lo que se viene a llamar la dark web (web oscura), un verdadero mercado negro virtual de compra y venta de datos que se organiza en las profundidades de Internet:

- por el pack completo de los datos de una persona se pagan aproximadamente 870 euros.
- por los datos de una cuenta de una red social, entre 3 y 8 euros.
- por los datos de una cuenta de Amazon Prime, unos 11 euros.
- por los datos bancarios hasta 700 euros.
- hasta 1.000 euros por un historial médico completo.

Este es un ejemplo del precio que se pagan por los datos de una persona, pero también existen otras ofertas de datos que los ofrecen agregados pero por segmentación en función de raza, religión, creencias, ideología o tendencias sexuales.

En definitiva, el negocio de los datos es una actividad extraordinariamente lucrativa -el gran negocio de Amazón, por ejemplo, no es la venta de productos on-line sino el almacenamiento de datos, controlando un tercio del mercado mundial y con una facturación anual de 70.000 millones de euros- y, en consecuencia, la cibercriminalidad centrada en su robo u obtención ilícita es una actividad altamente lucrativa.

Pulse Secure, Citrix, Fortinet son algunas de las empresas que proporcionan servicios VPN. Y los proporcionan a empresas y organizaciones de toda clase de sectores y actividades, desde gobiernos, administraciones públicas, entidades financieras, sanitarias, militares, multinacionales etc. Por esa razón son objeto prioritario de los hakers y ciberdelincuentes APT (Amenaza Persistente Avanzada).

Una Amenaza Persistente Avanzada es un conjunto de técnicas de hackeo organizadas por un tercero (una empresa, un Estado, una organización criminal...) para, de forma continua, clandestina y avanzada, penetrar en un sistema, atacando sus debilidades, y con propósitos varios como espiar,

[4] https://www-nytimes-com.cdn.ampproject.org/v/s/www.nytimes.com/es/2020/04/15/espanol/ciencia-y-tecnologia/zoom-privacidad-virus.amp.html?usqp=mq331AQFKAGwASA%3D&amp_js_v=0 [consulta: 15/05/2020].

destruir, robar información, sabotear y, en general, obtener un beneficio económico con su actividad delictiva. Hay incluso grupos APT que se ofrecen para realizar operaciones mercenarias de ciberespionaje centrando su actividad en víctimas determinadas o en determinados tipos de datos especialmente sensibles.

¿Y en qué consisten estos ataques? Obviamente, presentan tantas variantes como las de cualquier otra actividad delictiva que persiga un propósito definido, pero haciendo abstracción de un modus operandi tipo podemos llegar a una conclusión de base: lo que pretenden generalmente los hackers cuando diseñan un ataque APT es tener un acceso continuo al sistema. El ataque comienza forzando la puerta de entrada en el sistema a través de cualquier medio -como el ladrón con la puerta de un inmueble- ya sea un archivo infectado, un correo electrónico, una aplicación vulnerable, contraseñas débiles, etc. Una vez ingresan en el sistema implantan un malware[5] que les permite crear una serie de puertas traseras y túneles en el sistema al que han accedido y que les va a permitir transitar por él sin ser detectados. Una vez dentro de forma invisible, los hackers van intensificando su control sobre el sistema, moviéndose cada vez con más libertad y accediendo a todo tipo de archivos, e incluso accediendo a otros servidores asociados. Se quedarán dentro del sistema de forma indefinida, o cumplida su misión se retirarán, aunque normalmente dejando una puerta abierta para poder acceder en el futuro.

El Centro Criptológico Nacional (en adelante, CCN)[6] es un organismo adscrito al Centro Nacional de Inteligencia (en adelante, CNI). No es una agencia independiente sino que forma parte integrada del servicio de inteligencia español y tiene a su cargo, entre otras muchas funciones y cometidos, en lo que aquí nos interesa, velar por la seguridad de los sistemas de las tecnologías de la información de la Administración que procesan, almacenan o transmiten información en formato electrónico, legalmente protegido, y que incluyen medios de cifra, así como información clasificada. También está entre sus funciones elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración del Estado.

El Equipo de Respuesta a Incidentes del Centro Criptológico Nacional avisó en comunicación de 28/8/2019, con nivel de peligrosidad declarado alto, de la explotación masiva de una vulnerabilidad grave en el servicio de VPN Pulse Secure. Esta vulnerabilidad permitía a un atacante leer en forma remota el

[5] Malware es un acrónimo del inglés que procede de la expresión malicious software (código malicioso). Los malwares son programas diseñados para infiltrarse en un sistema con el fin de dañar o robar datos e información.

[6] https://www.boe.es/buscar/doc.php?id=BOE-A-2004-5051

contenido de ficheros en el servidor afectado, potencialmente en aquellos que contuvieran contraseñas o datos sensibles, y poniendo en riesgo el acceso a la infraestructura interna de la organización[7]. En comunicación de 30 de agosto de 2019 avisó, con nivel declarado de peligrosidad alto, de la explotación masiva de una vulnerabilidad grave en el servicio de VPN sobre SSL de Fortinet que permitiría a un atacante acceder de forma remota a información sensible del equipo, como por ejemplo credenciales[8]. El 14 de enero de 2020, de nuevo con nivel declarado de peligrosidad alto, el Equipo de Respuesta a Incidentes del Centro Criptológico Nacional, avisa de una vulnerabilidad crítica en cientos de servidores de Citrix que permite a los atacantes ejecutar comandos de manera remota en el servidor-objetivo e incluso dándoles la posibilidad de entrar en las redes-objetivo y realizar actividades altamente dañinas[9].

A finales de 2019 son crecientes las informaciones que relatan múltiples ataques a redes VPN. Fortinet y Pulse Secure son servicios VPN con masiva implantación a nivel mundial y, en consecuencia, son objetivo prioritario de la ciberdelincuencia y, en particular, de los grupos de amenazas avanzadas (APT). En septiembre de 2019 se informó que las vulnerabilidades descubiertas en las citadas VPN empresariales estaban siendo explotadas masivamente permitiendo a los atacantes robar claves privadas y contraseñas del usuario y posibilitando, con ello, al atacante la ejecución remota de códigos y su acceso a la red VPN. Episodios como los ataques masivos a la empresa Travelex o por APT chinas son dos ejemplos de la actuación de estos grupos de ciberdelincuentes organizados, muchas veces financiados por los propios Estados, que penetran en las redes de empresas, universidades y órganos gubernamentales con el propósito de obtener información. El asedio a estas VPN es constante a fin de descubrir vulnerabilidades que permitan a estos atacantes conectarse a la red virtual sin necesidad de usuario y contraseña válidos y, ya dentro, examinar archivos y registros, desactivar autenticaciones, descargar archivos y ejecutar códigos maliciosos. También Citrix, entre enero y marzo de 2020 ha sido objeto de una campaña de piratería masiva en la que un grupo chino APT ha estado atacando a organizaciones de todo el mundo explotando sus vulnerabilidades y afectando a sectores como banca, gobierno, salud, educación superior, legal, medios de comunicación y servicios públicos.

7 https://www.ccn-cert.cni.es/en/updated-security/alertas-ccn-cert/8540-ccn-cert-al-04-19-vulnerabilidad-grave-en-pulse-secure-vpn.html [consulta: 15/05/2020]

8 https://www.ccn-cert.cni.es/seguridad-al-dia/alertas-ccn-cert/8552-ccn-cert-al-05-19-vulnerabilidad-grave-en-fortinet-vpn.html [consulta: 15/05/2020]

9 https://www.ccn-cert.cni.es/seguridad-al-dia/alertas-ccn-cert/9331-ccn-cert-al-01-20-vulnerabilidad-critica-en-servidores-de-citrix.html [consulta: 15/05/2020]

5. El proveedor

Declarado el Estado de Alarma, el Ministerio de Justicia y algunas Comunidades Autónomas con competencias transferidas en la materia, ante las presiones de reactivación de la actividad judicial, iniciaron un plan de impulso de la actividad laboral a través de la modalidad del llamado teletrabajo. Inicialmente improvisado y por la vía de hecho, a través del reclamo al funcionariado por parte de su estructura orgánica. Seguidamente, previsto normativamente a través del Real Decreto-ley 16/2020, de 28 de abril, de medidas procesales y organizativas para hacer frente al COVID-19 en el ámbito de la Administración de Justicia. En su disposición final primera se modifica la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, a fin de facilitar el acceso remoto a las aplicaciones utilizadas para la gestión procesal, imponiendo a las administraciones competentes la obligación de proporcionar "los medios seguros para que estos sistemas sean plenamente accesibles y operativos sin necesidad de que los usuarios se encuentren físicamente en las sedes de sus respectivos órganos, oficinas o fiscalías".

Seguidamente, y en desarrollo de este Real Decreto, se dictó la Orden JUS/394/2020, de 8 de mayo, por la que se aprueba el Esquema de Seguridad Laboral y el Plan de Desescalada para la Administración de Justicia ante el COVID-19 que determina que la reanudación de la actividad debe guiarse por el principio de minimización del riesgo, declara el teletrabajo como medida de organización del trabajo que evita o limita los riesgos de contagio y señala que el personal judicial que no deba prestar servicio en un turno concreto deberá realizar sus funciones mediante teletrabajo siempre que lo haya solicitado voluntariamente y se le haya proporcionado dispositivos con accesos securizados a los sistemas y aplicaciones de gestión procesal o un medio de acceso a los mismos desde sus dispositivos personales en similares condiciones.

Pues bien, el llamamiento a este teletrabajo se realizó masivamente al funcionariado apelando a sus equipos y dispositivos domésticos. Transcurridas las primeras semanas del Estado de Alarma se empezaron a recibir en los correos corporativos de los funcionarios de justicia mensajes en los que se les informaba por la Administración prestacional de la habilitación de una VPN, facilitándoles en adjunto un archivo ejecutable que contenía un certificado digital a fin de habilitar la red privada. Al tiempo, se publicaron manuales de instalación accesibles a través de la web de la Administración correspondiente en que se iniciaba la necesidad de descargar ficheros, aceptar a ciegas los permisos de ejecución y, finalmente, ejecutarlos. Así, a través de los proveedores de VPN Citrix, Pulse Secure y Fortinet, se empezaron a conectar de forma remota los dispositivos informáticos y accesos de red domésticos a los sistemas y aplicaciones de gestión procesal de los juzgados y tribunales.

Sin un control mínimo de la seguridad de los dispositivos informáticos y accesos de red domésticos cuya conexión se pretende a la VPN; sin un control de las licencias de los sistemas operativos instalados en esos dispositivos informáticos domésticos; sin un control del "ecosistema informático" que gobierna cada uno de esos ordenadores domésticos con programas destinados a usos particulares y con una concreta política de transmisión de datos dispuesta por su titular; sin un control de calidad de los programas VPN que se pretenden instalar para posibilitar el acceso remoto y sin examen de su código fuente propietario; sin someter estos programas a una auditoria particular de seguridad; sin someter el conjunto de esta pretendida red de acceso remoto a una auditoria general de seguridad conciliada con los requisitos de seguridad que exige la protección de datos; sin dar cuenta de todo ello a los letrados de la administración de justicia; y sin una autoridad de control en el Poder Judicial que levante la mano para hacer uso de sus poderes de investigación en forma de auditorías de protección de datos que le otorga el RGPD; el Poder Ejecutivo del Estado, Ministerio de Justicia y Comunidades Autónomas con competencias transferidas en materia de justicia, titulares de los soportes, sistemas y aplicaciones informáticas pero no de los datos que contienen, ha dispuesto unilateral y trascendentemente sobre la seguridad, sin la más mínima demostración de vigilancia, poniendo en letal riesgo los datos de millones de ciudadanos.

Estos días de crisis sanitaria en que la fundamentalidad de derechos como la tutela judicial efectiva o de defensa han engordado los argumentos de las urgencias y los atajos, los ciudadanos, titulares también del derecho fundamental a la protección de sus datos de carácter personal, han de saber que los datos que hayan aportado o estén aportando a los ficheros judiciales sobre su familia, hijos, patrimonio, fiscalidad, actividades empresariales, relaciones afectivas, conflictos sucesorios, actividades económicas, relaciones laborales, relaciones contractuales, y toda suerte de intimidades resultantes que se manifiesten en un pleito civil, o en una investigación penal, están en riesgo manifiesto de ser género de tráfico en el mercado negro de los datos.

En pleno Estado de Alarma otros virus también se propagan y estos afectantes a la salud de nuestro Estado de Derecho.

Conflicto de intereses
El autor declara no tener ningún conflicto de intereses.

Financiación
El documento ha sido elaborado sin financiación.