Problemáticas de la protección de los datos personales en las redes sociales

Luca Christian Natali*
RVLJ, ISSN 2343-5925, ISSN-e 2791-3317, N.º 18, 2022, pp. 149-166.

Sumario

Introducción: problemáticas emergentes y objetivos del presente artículo

Según información que circula en las redes sociales, y que se transmite informalmente, se han producido casos de suspensión o cierre de las cuentas de algunos usuarios, entre los que se incluyen numerosos trabajadores dependientes y autónomos, por parte de las redes sociales. Con frecuencia,

* **Università Cattolica** (Piacenza), Licenciado en Derecho. **Università Cattolica** (Milano), Doctor en Derecho Laboral y Relaciones Industriales. **Scuola Superiore di Studi Universitari e di Perfezionamento Sant'Anna** (Pisa), Doctor en Derecho Civil. **Garante per la Protezione dei Dati Personali** (Italia), Funcionario Ejecutivo. La posición del autor es estrictamente personal y, en ningún modo, vincula al órgano de la Administración Pública italiana al que pertenece. El presente artículo recoge las consideraciones expuestas por el autor en los seminarios que impartió, como ponente, en el Curso de Formación Avanzada «Gestión de la Privacidad y Seguridad de la Información» en la Universidad Magna Grecia de Catanzaro (abril-mayo de 2021), organizado por la Prof. Maria Luisa Chiarella.

estas suspensiones o cierres de las cuentas en las redes sociales tienen lugar de manera repentina y se motiva genéricamente en la supuesta violación de los «términos y condiciones» del servicio, impuestos por las redes sociales. En la mayoría de los casos, las suspensiones o cierres de cuentas en las redes sociales se produjeron en concomitancia con acontecimientos políticos, que fueron comentados, alabados o estigmatizados por los usuarios, incluso de aquellos que, aunque no ejerzan cargos políticos, tienen capacidad de influenciar de manera determinante a la opinión pública nacional.

Los sujetos afectados por el cierre o la suspensión de las cuentas en las redes sociales se quejan de las posibles pérdidas económicas por la indisponibilidad temporal del servicio; que, para muchos usuarios (como periodistas, columnistas, comerciantes y emprendedores o trabajadores autónomos), es parte integrante de su actividad de comunicación, difusión, denuncia y crítica, así como de su red laboral y profesional, incluso para establecer nuevas y futuras relaciones de trabajo.

Ciertamente, se trata de una problemática distinta a la imposibilidad de acceder a la cuenta o a la suspensión de esta última por otras razones, en ciertos casos ambiguos, como problemas de autenticación del titular de la cuenta o supuestos accesos de dispositivos no reconocidos, etc. Situaciones estas que, aunque son denunciadas o impugnadas por los usuarios afectados, no se relacionan con motivaciones o ideologías políticas.

De hecho, cuando la suspensión o cierre de las cuentas en las redes sociales está vinculado al contenido de los comentarios y de las publicaciones de los usuarios podría configurarse una afectación a la libertad de expresión; la cual, en Italia, es esencialmente competencia de diversas autoridades públicas, como la *Autorità per le Garanzie nelle Communicazioni* (AGCOM) o la autoridad judicial ordinaria. Sin embargo, si se analiza con detenimiento, algunos aspectos (que identificaremos y explicaremos brevemente a continuación) también podrían ser competencia del *Garante per la Protezione dei Dati Personali*.

Específicamente, respecto a los trabajadores, hay que preliminarmente tomar en cuenta que la libre expresión de su pensamiento y, en particular, su derecho de crítica en las redes sociales –especialmente, en el contexto de los perfiles públicos o, en todo caso, «abiertos»– se enfrenta a las posibles «represalias» del empleador, cuya actividad ha sido criticada o que considere perjudicada su imagen, reputación o la de la empresa que dirige. En efecto, son numerosos los casos de despidos, a veces sin recurrir a la necesaria aplicación progresiva de las medidas disciplinarias, que posteriormente han sido impugnados extrajudicial o judicialmente por el trabajador. Sin embargo, la Corte Suprema de Justicia italiana ha frecuentemente confirmado dichos despidos aparentemente «extremos»[1].

El anterior supuesto debe ser evidentemente diferenciado de aquel relativo al despido del trabajador por el uso de las redes sociales en horario laboral, quizás de forma excesiva y, en todo caso, desviándose significativamente de sus funciones laborales. No obstante, existe un mínimo común denominador entre estas situaciones, es decir, la (presunta) ruptura del *intuitus personae* que ineludiblemente debe caracterizar el vínculo laboral, especialmente en el sistema privado, incluyendo particularmente a los contratos de trabajo subordinado, los contratos de obra, las licitaciones, los contratos de mandato, los poderes, etc[2]. De hecho, la problemática del uso de las redes sociales por parte de los trabajadores también está estrechamente vinculada con los posibles abusos y efectos discriminatorios de la rectitud política (o de lo «políticamente correcto»), cuya adecuada y equilibrada gestión es de importancia constitucional, en atención al artículo 21 de la Constitución de la República italiana, inclusive por su impacto en la estabilidad del sistema pluralista y democrático.

---

1 Entre otras, véase, Casación Civil, sec. Laboral, auto N.º 28 878, de 12-11-18.

2 En cambio, en el sistema de empleo público, dada la preponderancia de los principios de buen desempeño e imparcialidad, establecidos en el artículo 97 de la Constitución italiana, el criterio del *intuitus personae* se encuentra solo de forma residual –pero, con el fundamento racional de la protección del principio fundamental del buen desempeño de la actividad (de orientación) política–, en particular, en lo relativo a las relaciones de colaboración entre los órganos políticos (por ejemplo: Ministros, miembros del Colegio, o del Consejo de las Autoridades) y el personal de planta o plantilla, o de colaboración directa.

Con relación a la intimidad y privacidad del trabajador y, especialmente, respecto al tratamiento de sus datos personales, se presentan diversas problemáticas que pareciera caracterizar distintas redes sociales usadas tanto por los trabajadores como por otros usuarios. Por lo que se trata de un problema general. Sin embargo, no podemos ni queremos estigmatizar o culpar a algún responsable del tratamiento de los datos personales. De hecho, las críticas que se expondrán a continuación se refieren al plano formal de la red social y, por lo tanto, son formuladas en términos potenciales, debido a que a las empresas responsables del tratamiento de los datos personales se les debe reconocer una presunción de legalidad, o se debe admitir que el tratamiento de los datos personales en el caso concreto puede ser plenamente conforme con la legislación en materia.

Además, son notorios y deben reconocerse los esfuerzos de diversa índole (técnicos, jurídicos y económicos), así como las inevitables dificultades, de las redes sociales (casi siempre pertenecientes a sistemas extranjeros, como los de Estados Unidos de América o China) para adaptarse al modelo comunitario europeo de protección y seguridad de los datos y demás información almacenada y tratada; el cual no solo es profundamente diferente al aplicado en esos sistemas extranjeros, sino que también fue modificado por el Reglamento General de Protección de Datos de la Unión Europea N.º 679/2016, que introdujo nuevos principios «estructurales», nuevas obligaciones y nuevas responsabilidades.

Por otra parte, hay que tener en cuenta las peculiaridades de otros modelos legales (como el estadounidense), en los que no está prohibida la denominada «monetización de los datos», es decir, la prestación de diversos y útiles servicios y funcionalidades ofrecidos por las redes sociales a cambio de la cesión de datos personales. Este principio ha llegado al ordenamiento jurídico de la Unión Europea, a través de la reciente legislación en materia de bienes y servicios digitales (véanse las Directivas de la UE 790, 770 y 771/2019)[3],

[3] Específicamente: Directiva (UE) 2019/770, de 20-05-19, sobre determinados aspectos de los contratos de suministro de contenidos digitales y servicios digitales; Directiva (UE) 2019/771, de 20-05-19, sobre determinados aspectos de los contratos

que pronto se aplicará en los ordenamientos jurídicos nacionales de la Unión Europea.

En razón de todo lo anterior, el objetivo del presente trabajo es coadyuvar al conocimiento de los aspectos críticos del tratamiento de los datos personales en el universo de las redes sociales, así como contribuir a la reflexión sobre el funcionamiento de dichas redes –las cuales son indudablemente imprescindibles en la cotidianidad, y ventajosas gracias a sus funcionalidades– para mejorar el nivel de cumplimiento de la legislación en materia de protección de datos personales por parte de los responsables del tratamiento de dichos datos y, con ello, incrementar la confianza de los usuarios para acercarse a las redes sociales, lo cual tendría inevitables repercusiones positivas en su correcto uso, en su expansión y en su imagen, tal y como se percibe en el universo de la Red[4].

1. Política de la plataforma o red social

Para aproximativamente identificar el ámbito del tratamiento de los datos personales del trabajador y, en caso de que existieran, las problemáticas de la legislación en materia de protección de datos personales, se procederá de manera novedosa a examinar la puesta en marcha y el funcionamiento de una red o plataforma social típica, cual resultado de las críticas encontradas en varias redes sociales similares, como «muestra» significativa de análisis.

En este sentido, y en aras de mayor exhaustividad y claridad expositiva, a continuación, se presenta un extracto de las políticas de una red o plataforma social típica (en lo sucesivo, «PS»).

---

de compraventa de bienes; Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo, de 17-04-19, relativa a los derechos de autor y derechos afines en el mercado único digital y por la que se modifican las Directivas 96/9/CE y 2001/29/CE (texto pertinente a efectos del EEE).

4 Para mayores detalles, se permita el reenvío a Natali, Luca Christian y Piselli, Sabrina: «*Libertà d'espressione e protezione dei dati dei lavoratori nelle piattaforme social*». En: *Diritto e Pratica del Lavoro*. N.º 14. Milán, 2021, pp. 866 y ss.

Con relación al «contrato entre la red social y el usuario», la red modelo propone la siguiente fórmula de propuesta contractual global: «El consentimiento del usuario de la PS incluye los presentes términos y condiciones del servicio, nuestra política de privacidad, las políticas de la PS, y todas las políticas incorporadas».

Respecto a los «términos y condiciones del servicio» prevé:

> Los presentes términos y condiciones del servicio («Términos y Condiciones») rigen el acceso a y el uso de nuestros servicios, incluyendo nuestras diversas páginas web, SMS, API, notificaciones por correo electrónico, aplicaciones, botones, *widgets*, anuncios y servicios comerciales (…) a los que se refieren estos Términos y Condiciones (conjuntamente, los «Servicios»), y a cualquier información, mensaje, enlace, imagen, foto, vídeo u otros documentos o configuraciones de documentos cargados, descargados o que aparezcan en los Servicios (conjuntamente denominados «Contenido(s)»). Al utilizar los Servicios, usted acepta someterse a estos Términos y Condiciones (…) En caso de cualquier interrogante sobre estos Términos y Condiciones, lo invitamos a contactarnos.

Entre estos términos y condiciones, la red o plataforma social típica (PS) –al igual que otras redes sociales– incluye la posibilidad de suspender o restringir (de forma temporal o permanente) las funcionalidades de la cuenta del usuario.

2. Primeras reflexiones lógico-jurídicas

Adicionalmente, al natural sentimiento de asombro o aturdimiento en los directamente afectados, el cierre o la suspensión repentina de cuentas en las redes sociales podría generar un daño, potencialmente injusto, es decir, *contra ius* o contrario a derecho, bajo distintos aspectos.

En este contexto, debe tomarse preliminarmente en cuenta la incapacidad del precitado contrato (entre la red social y sus usuarios) para servir de fundamento

jurídico de cualquier decisión y conducta en la red, debido a que se podría poner en entredicho la validez y la eficacia de la citada cláusula contractual.

Por otra parte, un contrato, como el de la red y el usuario, podría estar en conflicto con algunos derechos fundamentales de la persona, de rango constitucional y, por lo tanto, susceptibles de ser apreciados a los fines de determinar la eventual nulidad parcial y relativa. Entre dichos derechos fundamentales, se pueden incluir: el derecho a la libre expresión del pensamiento, reconocido a nivel constitucional por el artículo 21 de la Constitución italiana, y a nivel comunitario europeo por el artículo 10 del Convenio Europeo de Derechos Humanos; así como, el derecho a la defensa, consagrado por el artículo 24 de la Magna Carta italiana, en virtud del carácter abrupto de la suspensión de la red social, aunque sea temporal.

Igualmente, como se observará, podría contrastar con el derecho a la protección de datos personales, que debe ser considerado en su polifacética composición de múltiples, diferentes e incisivos derechos de protesta, en atención a los artículos 15 al 22 del Reglamento General de la UE (acceso, oposición, limitación, cancelación), y que podría generar diversos tipos de daños (graves y apreciables, en criterio constante de las *Sezioni Unite* de la Suprema Corte italiana)[5]; los cuales, a pesar de ser difícilmente impugnables respecto al *an* (entidad del daño) y son de *quantum* incierto, quedan a la

[5] Véase, *ex pluribus*, Tribunal de Casación, sent. N.º 16 133, de 15-07-14, comentada, *ex pluribus* (con un título perfectamente explicativo) por LO VOI, V., «*Il danno non patrimoniale per violazione della privacy richiede la verifica della "gravità della lesione»" e della "serietà del danno"*», disponible en www.dirittocivilecontemporaneo.com. Asimismo, véase, Tribunal de Casación, sent. N.º 83, de 20-08-20; en la cual la Corte de Casación reafirmó el principio según el cual el daño inmaterial indemnizable, resultante de la violación de la normativa en materia de protección de dato personales, al causar la vulneración de un derecho fundamental, reconocido por los artículos 2 y 21 de la Constitución italiana, y por el artículo 8 del Convenio Europeo de Derechos Humanos, no puede sustraerse de la verificación de la «gravedad del perjuicio» y de la «gravedad del daño», ya que este derecho también se equilibra con el principio de solidaridad, consagrado en el artículo 2 de la Carta Magna italiana, que se expresa en la necesidad de tolerar la más mínima violación de este derecho.

valoración –esencialmente equitativa– de la autoridad judicial en atención al artículo 1226 Código Civil italiano.

Los daños deben ser reparados, de acuerdo con el artículo 82 del Reglamento General de la UE y, por tanto, en virtud de un mecanismo de responsabilidad civil agravada y semiobjetiva. En general, se pueden identificar dos tipos de daños: de un lado, los daños materiales (o patrimoniales); y, del otro lado, los daños inmateriales[6] (o extrapatrimoniales).

El daño material se refiere a la posible pérdida, temporal o definitiva, de la propia red de contactos y a la posibilidad de desarrollar colaboraciones, incluso de tipo profesional y laboral, así como de recibir patrocinios, debido al elevadísimo número seguidores (*followers*).

Además de los precitados derechos a la libre expresión del pensamiento y a la defensa, el daño inmaterial puede referirse al derecho a la propia imagen y a la reputación en la red; pero, especialmente, en los supuestos de falta de acceso a los datos contenidos en la cuenta, también puede referirse al derecho a la identidad digital que, como es conocido, encuentra en las redes sociales su principal instrumento de expresión y construcción progresiva, en particular, en lo relativo a la información, audios, vídeos, subidos, recibidos, compartidos –incluso en la versión efímera y menos exigente de los *fleet*[7], es decir, pensamientos a comentarios «a tiempo», no visibles por nadie y «sin reacciones públicas» –inclusive respecto a informaciones de contenido político, sindical y religioso, y, en consecuencia, extremadamente «sensibles»–.

---

6 Sobre el tema, se permita el reenvío a Natali, Antonio Ivan; Natali, Luca Christian y Cassano, Giuseppe: *Danno non patrimoniale da inadempimenti di contratti e obbligazioni.* Maggioli Editore. Santarcangelo di Romagna (RN), 2010; en particular, véase los capítulos: *Il danno non patrimoniale da violazione del contratto di telefonia* y *Il danno non patrimoniale da violazione del contratto sulla privacy.* Igualmente, véase: «*Il danno non patrimoniale da lesione della riservatezza*» (cap. VI), en Natali, Antonio Ivan: *Il danno non patrimoniale nel processo civile*. Maggioli Editore. Santarcangelo di Romagna (RN), 2009, pp. 235 y ss.

7 https://help.twitter.com/it/using-twitter/fleets.

No se puede descuidar que, para la mayoría de las personas, la esfera digital se ha convertido en parte sustancial y relevante de la vida cotidiana, especialmente, en virtud de la facilidad de conexión digital, mediante teléfonos inteligentes, y debido a que se extiende al mismo tiempo a redes sociales de diversa índole (trabajo: *Linkedin*; búsqueda de amigos, familiares y afectos: *Facebook;* diario en línea: *Instagram*; críticas y comentarios: *Twitter*), aunque todas participen el mínimo común denominador de compartir en tiempo real una vasta y compleja cantidad de información de diversa naturaleza, incluyendo información muy sensible. Tal es la relevancia de la esfera digital que podría incluso constituir la parte más auténtica y, por tanto, merecedora de protección de la vida cotidiana, en particular si tomamos en cuenta que, bajo algunos aspectos, la gestión de datos por parte de las redes sociales es en cierta medida incomprensible[8].

En ocasiones, la red o plataforma social típica (PS) regula la gestión de la limitación de la visibilidad-oscurecimiento y eliminación de los *tuits* de los usuarios, estableciendo una aparente graduación de estas herramientas; la cual, sin embargo, no pareciera estar prevista –o, por lo menos, no se encuentra fácilmente– para el supuesto de la suspensión provisional o definitiva de las cuentas. De hecho, la nota informativa de la red o plataforma social típica (PS) relativa a la suspensión de la cuenta es imprecisa y ambigua, indicando de forma genérica sus posibles causas; entre las que se incluyen, las denuncias recibidas de otros usuarios, como eventuales «delatores», y el comportamiento ofensivo. Sin embargo, dicha nota informativa no pareciera contemplar ningún medio para verificar las denuncias y su confiabilidad, ni tampoco un procedimiento de «garantía» que permita al usuario ser escuchado y le asegure la posibilidad de oponerse a la suspensión antes de que esta se aplique.

---

[8] Estamos en una fase de transformación radical que Luciano Floridi, filósofo de la Información y la Tecnología de la Universidad de Oxford, denomina «cuarta revolución», entendida como revolución del ser, de nuestra comprensión sobre nosotros mismos y en cuyo núcleo se encuentra la infoesfera, es decir, el espacio de la información de la era digital que involucra todos los ámbitos de la vida, y plantea retos desconocidos. Esta noción, conceptualizada por Floridi desde 2009, es el corazón de su último libro: *Pensare l'infosfera*. Milán, 2020.

En una óptica de protección, que pareciera ser solo *a posteriori* y eventual, la red o plataforma social típica (PS) prevé que el usuario «podría» intentar solicitar la reactivación de la cuenta suspendida. De esta manera, revela que no existe ninguna garantía cierta al respecto. Al mismo tiempo, es posible reconocer a la red social un poder discrecional, que adquiere el peligroso gusto de la arbitrariedad, no solo con relación a la libertad de expresión de los usuarios, sino también bajo múltiples aspecto, que serán identificados sucesivamente, respecto al derecho a la protección de datos.

No obstante, debe tomarse en cuenta que, aunque en ciertas ocasiones exija condiciones estrictas, la violación de la privacidad podría constituir delito, en atención a los artículos 167, 167 *bis*, y 167 *ter* del Código de la Privacidad italiano; así como, del artículo 84 del Reglamento General de Protección de Datos de la UE N.º 679 del 2016.

3. Posibles aspectos críticos

Como resulta de un análisis meramente formal de sus políticas (que, para mayor comprensión, merecería un examen preliminar sobre el efectivo funcionamiento en concreto), la red o plataforma social típica (PS) pareciera violar los artículos 12 y 13 del Reglamento General de Protección de Datos de la Unión Europea, así como el derecho a oponerse al tratamiento (o sea, a la repentina suspensión), en virtud del artículo 21 del Reglamento General de Protección de Datos. De manera relacionada, parecería también entrar en conflicto con el aparte 1.º del artículo 22 del Reglamento relativo a las «decisiones automatizadas», según el cual «Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado (…) que produzca efectos jurídicos en él o le afecte significativamente de modo similar».

Esta problemática podría repercutirse también en la violación del principio de privacidad por diseño (*privacy by design*), en atención al aparte 1.º del artículo 25 del Reglamento General de Protección de Datos, dado que el diseño del relativo tratamiento de los datos pareciera no haber sido suficientemente

cuidadoso y, por tanto, sustancialmente inadecuado, respecto a los derechos de los interesados[9].

La aceptación de las cláusulas contractuales no implica por sí misma un válido (y menos invencible) vínculo para los consumidores; debido a que, con relación a las redes sociales, los usuarios son generalmente «consumidores». En consecuencia, están protegidos por los principios y las normativa europea en materia de protección del consumidor y, a nivel italiano, por el «Código del Consumo» (Decreto Legislativo N.º 206, de 06-09-05).

En el contexto de la normativa europea e italiana de protección del consumidor, adquiere relevancia la ineficacia «relativa» –es decir, cuya legitimación está limitada al usuario-consumidor (incluyendo al empresario o profesional que actúa por causas ajenas a su propia actividad, excluyendo a la empresa prestadora del servicio y autora unilateral de las condiciones del servicio– de las cláusulas contractuales relativas al derecho de suspensión de las cuentas o a la limitación de la responsabilidad de la empresa. De hecho, puede afirmarse que dichas cláusulas crean un importante desequilibrio jurídico entre la red social y el usuario, desequilibrio que también puede dar lugar a pérdidas económicas relacionadas con la intempestiva suspensión de la cuenta, con la consiguiente imposibilidad de acceder y gestionar los propios datos y contactos y de mantener-desarrollar sus propias actividades.

Dejando de lado el enfoque estrictamente contractual, es importante destacar que, desde la óptica de la protección de datos, el consentimiento solicitado al usuario incluye, por expresa política de la empresa, cuatro elementos totalmente heterogéneos y ciertamente no superponibles, los cuales son claramente identificados por la propia red o plataforma social típica (PS), a saber:

a. «Términos y Condiciones del Servicio» (contrato);

b. «Política de Privacidad», que adicionalmente prevé múltiples y diversos tratamientos de datos que, a su vez, exigirían un consentimiento

[9] Véase la disposición 15.1.20, documento web N.º 9256486.

libre y específico (por ejemplo: *marketing*; elaboración de perfiles; comunicación de datos a terceros; geolocalización);

c. «Normas PS»; y

d. «Políticas integradas», las cuales también poseen un contenido variado.

De acuerdo con el artículo 7, y diversos considerandos, del Reglamento General de Protección de Datos, así como de la práctica constante del *Garante per la Protezione dei Dati Personali*, estos elementos requerirían un consentimiento específico, libre y concreto; obligación que, sin embargo, pareciera ser descuidada por la red o plataforma social típica (PS), la cual impone un consentimiento *ómnibus* (global), sin el cual el usuario no puede registrarse y utilizar la plataforma.

Por lo tanto, la voluntad de los interesados se desvía en varios niveles. En consecuencia, el consentimiento para el tratamiento de los datos, solicitado por la red o plataforma social típica (PS), pareciera viciado y, por tanto, inválido por carecer de una adecuada base jurídica (artículo 6 del Reglamento General de Protección de Datos), con la consiguiente invalidez (no subsanable) de los distintos tratamientos realizados posteriormente por la empresa.

4. Conservación de datos: otro posible aspecto crítico

De un examen preliminar, pareciera que a los usuarios de las cuentas suspendidas se les impide volver a acceder a los datos, y a tratarlos en el ámbito del uso de la red y en sus diversas funcionalidades sociales. En parcial «compensación» a dicha limitación, la red o plataforma social típica (PS) –siempre, a nivel abstracto, de sus políticas– concedería el ejercicio de una facultad de descarga, que pareciera subsumible en el (diferente) derecho a la portabilidad (artículo 20 del Reglamento General de Protección de Datos)[10]. Esto no deja de ser un aspecto que debe destacarse de manera positiva, respecto a la esfera de protección de los usuarios, Igualmente, debe observarse

[10] Véase, por ejemplo: https://help.twitter.com/it/managing-your-account/how-to-download-your-twitter-archive.

de forma muy positiva la posibilidad ofrecida a los usuarios, en varias modalidades y oportunidades, de contactar a dichas redes sociales.

En contraste, no es clara, y es potencialmente riesgoso para los derechos de protección de los datos, la forma en que, de manera sucinta, la red o plataforma social típica (PS) especifica a veces que los datos de la cuenta se conservarán, a pesar de la suspensión-desactivación definitiva de las cuentas «para garantizar la seguridad y la protección de su plataforma y sus usuarios».

Pareciera tratarse de un almacenamiento de ciertos datos e informaciones, que quizás podría ser indefinido en el tiempo y, por lo tanto, podría contrastar el artículo 5.1.e del Reglamento General de Protección de Datos. En este sentido, es conveniente recordar la amplitud y variedad del concepto de «datos personales» que, como es notorio, incluye también las direcciones IP, los datos de localización y cualquier otra información inclusive indirectamente referible a la persona, según la reiterada jurisprudencia comunitaria europea.

5. La posible criticidad del consentimiento

Más allá del problema de la suspensión de la cuenta y de la ausencia de un válido vínculo, derivada de las políticas de la red social, surge la problemática de la ausencia de una adecuada base jurídica para las finalidades distintas a la prestación del servicio, es decir, aquellas relativas al *marketing*, elaboración de perfiles, comunicación a terceros, geolocalización; debido a que, como previamente se ha indicado, no existe un consentimiento distinto al contractual, ni mucho menos el necesario consentimiento libre y específico para cada una de estas –variadas e invasivas– finalidades[11].

[11] Confirmando la centralidad del consentimiento y su conexión con los derechos fundamentales de la persona, y desde una perspectiva necesariamente integrada y coherente del ordenamiento jurídico, se encuentra la interesante posición de la Suprema Corte italiana (véase Corte de Casación, N.º 28 985, 2 de julio-11 de noviembre de 2019) también en el diferente ámbito médico, según la cual, «el consentimiento del paciente a los servicios médicos constituye el ejercicio de un derecho subjetivo autónomo de autodeterminación propio de la persona natural», que es diferente y diverso del derecho fundamental a la salud entendido como el derecho del

El fundamento del «interés legítimo», como es recogido en la nota informativa de la red o plataforma social típica (PS), tampoco puede considerarse adecuado para legitimar dicho tratamiento. A este respecto, es necesario reiterar las consideraciones realizadas por el Garante de la Privacidad italiano, en la providencia del 15 de enero de 2020 (doc. Web N.º 9256486), (par. 3.1); en particular, cuando señala:

> … no puede invocarse como base jurídica (…) la del «interés legítimo» en las actividades de *marketing*, quizás conjuntamente con el presunto interés del sujeto «en referencia», que envuelve en la promoción al amigo o familiar. Cabe destacar que el interés legítimo, al que se refiere el artículo 6, apartado 1, letra f del Reglamento –ya previsto tanto en la derogada Directiva 95/46/CE, como en el Código antes de las modificaciones introducidas por el Decreto Legislativo N.º 101/2018 (Decreto Legislativo N.º 196/2003, artículo 24, apartado 1, letra g)– no puede sustituir en general el consentimiento del interesado como base jurídica del *marketing*. De hecho, el propio Reglamento –al igual que el artículo 7.1.f de la Directiva 95/46/CE)– únicamente lo permite «a condición de que no prevalezcan los intereses, o los derechos y libertades fundamentales del interesado que requieran la protección de los datos personales» (…) En cualquier caso, la existencia de intereses legítimos requiere una evaluación cuidadosa también en lo que respecta a si el interesado, en el momento y en el contexto de la recolección de datos personales, podía esperar razonablemente que el tratamiento de los datos tuviera lugar con ese fin[12].

---

sujeto a su propia integridad psicofísica. Se trata de un cumplimiento, estricto e ineludiblemente, vinculado a la información, como en materia de protección de datos. De hecho, como observa la Suprema Corte, todo individuo tiene derecho a recibir la información adecuada sobre la naturaleza y la posible evolución del tratamiento terapéutico al que puede ser sometido, así como de las posibles terapias alternativas. Una perspectiva similar de desarrollo y reverberaciones, incluso arriesgadas, puede identificarse con respecto a la circulación de datos y al tratamiento posterior, por lo que la información se convierte en una garantía esencial en la identificación exacta del perímetro del propio tratamiento.

12 Sobre el tema, véase, Piselli, Sabrina: «*Il recente provvedimento del Garante verso TIM come possibile nuove "linea guida" per il marketin*g? En: *Privacy&*. N.º 1. Egea. Milán, 2020, disponible en https://privacyand.egeaonline.it/it/21/archivio-rivista/rivista/3447042/articolo/3447056.

Igualmente, hay que recordar –como aclarado en la precitada providencia del Garante del 15 de enero de 2020– que:

> La aplicación del fundamento jurídico del interés legítimo presupone entonces la prevalencia en concreto (con base en una ponderación otorgada al titular, pero siempre evaluable por la Autoridad de Control) de este último sobre los derechos, libertades y meros intereses de los interesados (específicamente, los destinatarios de las comunicaciones promocionales no apoyadas por el consentimiento). En tal ponderación, es necesario sopesar cuidadosamente el impacto del tratamiento, que se entiende realizar, sobre esos derechos, libertades e intereses (entre los cuales, en el caso del *marketing*, se encuentran en primer lugar el derecho a la protección de datos y el derecho a la tranquilidad individual del interesado[13].

Conclusión

Ciertamente, las redes sociales constituyen un mundo variado y complejo; pero, sobre todo, son un «laboratorio de análisis» y una dimensión aplicativa que permite comprender cómo los datos y los derechos de los usuarios –incluyendo las diversas tipologías de trabajadores– pueden estar expuestos a riesgos aún desconocidos y por comprender. Sin embargo, hay que reconocerles a las redes sociales, además de la indudable utilidad de los servicios ofrecidos y el apreciable uso del lenguaje amigable para el usuario, el importante esfuerzo de adaptarse en varias ocasiones a la nueva legislación de la Unión Europea, a partir de la renovación de la información según el artículo 13 del Reglamento General de Protección de Datos.

---

[13] En este sentido, véase, Informe Anual Garante, 2018, p. 107, la providencia del 22-05-18, doc. web N.º 8995274, así como el Dictamen del Grupo de Trabajo del artículo 29, N.º 6/2014, WP 217, p. 35, según el cual, la institución del interés legítimo «garantiza una mayor protección del interesado; en particular, prevé que se tengan en cuenta no solo los derechos y libertades fundamentales del interesado, sino también su "interés" –mero y no calificado– (…) todas las categorías de intereses del interesado deben ser tenidas en cuenta y ponderadas frente a las del responsable del tratamiento, en la medida en que sean pertinentes en el ámbito de la Directiva».

Los aspectos más críticos se refieren a la efectiva autonomía contractual, a la confidencialidad y la protección de datos en sus diversas estratificaciones, así como al pleno respeto de otros derechos fundamentales, como la imagen y la identidad digital.

Por lo tanto, es deseable la intervención de las diversas autoridades competentes, entre las cuales se incluyen las Autoridades que garantizan la protección de los datos personales en atención al «revolucionario» principio de competencia, previsto en el segundo párrafo del artículo 2 del Reglamento General de Protección de Datos, que permite a dichas Autoridades actuar incluso respecto a las «*Over The Top*» extranjeras, como Facebook, Google, Amazon, debido a la mera oferta, inclusive a título gratuito, de bienes y servicios a los usuarios europeos. En este sentido, podría ser conveniente adoptar directrices u otros instrumentos de *soft law* dirigidos a esclarecer determinados aspectos (como los de la información y el consentimiento), siguiendo el ejemplo de anteriores actuaciones, como las Directrices de 4 de julio de 2013 del Garante italiano[14], que han sido de gran utilidad.

La Autoridad Garante italiana ha demostrado su atención respecto a las dinámicas de los grandes proveedores y los riesgos relacionados con la protección de los datos personales, así como su tempestividad y valentía, especialmente al actuar contra la conocida plataforma china Tik Tok, a los fines de proteger a los menores afectados en respeto de los principios y derechos previstos en el Reglamento General de Protección de Datos, y de la responsabilidad (*accountability*) del titular[15].

Mientras se procede a la activación de otros mecanismos de protección, como los de cooperación europea, previstos en el Reglamento General de Protección de Datos, es oportuno que los empresarios, en el marco de sus

---

14 Directrices sobre la actividad promocional y la lucha contra el *spam*, 04-07-13, doc. web N.º 2542348.

15 Providencia 22-01-21, N.º 20, doc. web N.º 9524194, que ordena la medida de bloqueo temporal del tratamiento, garantizando así la protección oportuna de los menores afectados.

buenas prácticas empresariales, orienten a los trabajadores respecto al prudente y consciente uso de sus datos (en el contexto del amplio concepto de información personal y corporativa), incluyendo fotos, vídeos, opiniones y contenidos «sensibles», de carácter sexual o de salud, así como cualquier información relativa al *know-how* corporativo, y tomando en cuenta los principios de finalidad y minimización.

Igualmente, sería aconsejable que los empresarios implementaran anuncios o avisos, por ejemplo, en la red de intranet, dirigidos a aumentar el nivel de conciencia de los usuarios y, de forma compatible con los recursos disponibles, que periódicamente impartieran a los empleados sesiones de formación sobre la protección de datos, prestando también atención a su dimensión social. De ahí, la necesidad de contar con un Delegado de Protección de Datos (DPO, por sus siglas en inglés), nombrado por la empresa, y capaz de operar eficientemente con los recursos adecuados, en pleno cumplimiento de las normas establecidas en los artículos 37 y siguientes del Reglamento General de Protección de Datos.

Teniendo en cuenta la actual configuración de algunas redes sociales, el principal riesgo es exponerse a diversas finalidades de tratamiento de los datos personales sin suficiente conocimiento, incluso por una superficial revisión y aceptación de los términos y condiciones del servicio por parte de los trabajadores-usuarios, o perder el acceso o el uso de su cuenta y, por lo tanto, a un mundo de datos y de relaciones, quizá minuciosamente construidas a lo largo del tiempo por el trabajador, con posibles perjuicios tanto para el trabajador como para la empresa en la que trabaja.

* * *

Resumen: El presente artículo examina las problemáticas relativas a la protección de los datos personales de los usuarios, especialmente de los trabajadores, en las redes sociales, tomando también en cuenta el rol de la Autoridad Garante de la Protección de los Datos Personales en Italia. **Palabras clave**: Protección de datos personales, redes sociales, derechos del trabajador, términos y condiciones del servicio, privacidad. Recibido: 02-05-22. Aprobado: 25-05-22.