ANUÁRIO
DA PROTEÇÃO DE DADOS
2023

COORDENAÇÃO
FRANCISCO PEREIRA COUTINHO
GRAÇA CANTO MONIZ

CEDIS
CENTRO DE I&D SOBRE DIREITO E SOCIEDADE

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

ANUÁRIO DA PROTEÇÃO DE DADOS 2023
Ano 5 – 2023

Coordenação:
Francisco Pereira Coutinho e Graça Canto Moniz

Secretariado Executivo:
Emellin de Oliveira

Paginação:
Gráfica 99

Edição:
Universidade Nova de Lisboa. Faculdade de Direito.
CEDIS, Centro de I & D sobre Direito e Sociedade
Campus de Campolide, 1099-032 Lisboa, Portugal

Suporte: Impresso
Impressão: 150 exemplares

Dezembro, 2023
ISSN 2184-5468

Catalogação na Publicação
Pereira Coutinho, Francisco e Canto Moniz, Graça (coord.). Anuário da Proteção de Dados 2023. Lisboa: CEDIS, 2023.

Índice

Nota Introdutória

O Anuário da Proteção de Dados é uma revista jurídica de livre acesso, disponível em linha no sítio https://protecaodedadosue.cedis.fd.unl.pt, que pretende divulgar estudos sobre o direito da proteção de dados pessoais. A revista é editada desde 2018 pelo Observatório da Proteção de Dados Pessoais, um grupo de investigação criado em 2016 no CEDIS – Centro de I & D sobre Direito e Sociedade da *NOVA School of Law*.

Os nove artigos publicados na edição de 2023 do Anuário resultam de uma chamada lançada em setembro de 2022 no sítio da internet do Observatório da Proteção de Dados Pessoais. Os textos foram sujeitos a um processo de *blind peer review* e posteriormente revistos pelos coordenadores do Anuário. Aos autores foi permitido escrever de acordo com a nova ou a antiga grafia.

O Anuário inicia-se com um texto da autoria do Javier Muñiz sobre a proteção dos dados de saúde dos trabalhadores no ordenamento jurídico espanhol, seguindo-se um artigo do Saul Leite que trata da proteção de dados pessoais no contexto da avaliação a distância no ensino superior. A responsabilidade civil pelo tratamento é o tema do texto do Daniel de Melo. De seguida, o Francisco Júnior debruça-se sobre a avaliação que deve ser realizada quando o responsável pelo tratamento recorre ao interesse legítimo para fundamentar o tratamento de dados pessoais. A Patrícia Carneiro apresenta uma análise do Regulamento de Governação de Dados e da sua relação com o Regulamento Geral Sobre a Proteção de Dados (RGPD), em especial no que diz respeito à licitude dos tratamentos. A Amanda Novaes analisa o regime das transferências

de dados pessoais à luz do caso Schrems II e a Diana Camões aborda a relação entre proteção de dados pessoais e concorrência. Por fim, a Madanela Cruz e a Iakovina Kindylid analisam os espaços europeus de dados e a sua relação com o RGPD, e a Elisabete Castela e o Tiago Branco da Costa debruçam-se sobre o altruísmo de dados no contexto da investigação clínica.

Esta obra não teria sido possível sem o patrocínio da SRS Advogados e da FUTURA, a quem agradecemos, nas pessoas do Luís Neto Galvão (SRS Advogados) e do Rodrigo Adão da Fonseca (FUTURA), o apoio que têm prestado desde a primeira hora a este projeto. Igualmente devidos são agradecimentos aos revisores deste número, ao Domingos Soares Farinho, ao Diogo Matos Brandão, à Helena Tapp Barroso, à Vera Raposo, ao João Rebelo, ao Marco Aurélio Rodrigues da Cunha e Cruz, ao Lúcio Tomé Feteira, ao Vinicius Mozetic e ao Jorge Morais de Carvalho. Por fim, agradecemos à Emellin Oliveira o auxílio prestado na edição do Anuário, bem como a todos os autores que participam nesta edição.

Lisboa, 17 de novembro de 2023

Francisco Pereira Coutinho
Graça Canto Moniz
Coordenadores do Observatório da Proteção de Dados

El tratamiento y protección de los datos de salud de los trabajadores en el ordenamiento español

Javier Fernández-Costales Muñiz[1]

Resumen: La vigilancia de la salud es uno de los principios básicos de la salud y la seguridad en el trabajo. La legislación ha venido a construir un sistema amplio y complejo de vigilancia de la salud dotado de no pocos y variados fundamentos y cuestiones de evidente interés, tanto a nivel doctrinal como práctico, entre los cuales, y por lo que aquí interesa, cabe destacar las importantes connotaciones del respeto a la intimidad, la dignidad de la persona y la confidencialidad de los datos de salud obtenidos en el marco de los reconocimientos médicos efectuados a los trabajadores.

Las informaciones relativas a la salud son datos especialmente sensibles a los cuales el legislador ha proporcionado una especial protección en distintas y diversas normas, salvaguardia que surge del hecho de encontrarse ante datos estrechamente vinculados a la dignidad y personalidad humanas.

Palabras clave*: salud, protección de datos, digitalización, nuevas tecnologías.*

Abstract: Monitoring health is one of the basic principles of Occupational Health and Safety. The legislation has built up a broad and complex system of health surveillance with many and varied foundations and questions of obvious interest, both doctrinal and practical, among which,

[1] Catedrático de Derecho del Trabajo y de la Seguridad Social, Universidad de León. E-mail: javier.costales@unileon.es

and as far as we are concerned here, the important connotations of respect for privacy, personal dignity and the confidentiality of health data obtained in the framework of medical examinations carried out on workers should be highlighted.

Health-related information is particularly sensitive data to which the legislator has afforded special protection in different and diverse rules, a safeguard that arises from the fact that the data in question are closely linked to human dignity and personality.

***Key words**: health, data protection, digitalisation, new technologies.*

1. Introducción

El imparable y continuo avance de las nuevas tecnologías y la transformación digital constituye, a día de hoy, uno de los aspectos más destacados, característicos y definitorios de nuestro actual entorno. La que ya se ha calificado como nueva revolución tecnológica o Cuarta Revolución Industrial ha introducido a la sociedad en una nueva dimensión de avances y desarrollos técnicos aplicables a todos los ámbitos a nivel social, productivo o económico, además de estar condicionando y haciendo evolucionar nuestros sistemas conceptuales, así como las formas de organización y gestión de nuestra vida personal y cotidiana.

El sistema productivo está transformándose desde hace mucho tiempo merced a esa cuarta revolución industrial y la industria 4.0 o "industria inteligente" supone "un salto cualitativo en la organización y gestión de la cadena de valor del sector"[2], implicando la incorporación de las nuevas tecnologías a la considerada "tradicional", permitiendo que dispositivos y sistemas colaboren entre ellos y con otros para crear

[2] ÁLVAREZ CUESTA, H.: *El futuro del trabajo vs. el trabajo del futuro*, A Coruña (Colex), 2017, pág. 15.

una industria inteligente[3]. La industria transforma, al tiempo, la economía tradicional en digital, y adquiere cuatro características específicas: "la irrelevancia de la ubicación geográfica, el papel clave de las plataformas, la importancia de los efectos de red y el uso de grandes datos"[4].

Cabe destacar cómo, respecto a esta utilización masiva de datos, se está ante una nueva forma de creación de valor que, como lo hicieran la agricultura o la revolución industrial en su momento, permitirá una transformación no solo cuantitativa, sino cualitativa de la sociedad, pues los datos masivos tienen la capacidad de "revolucionarlo todo, desde las empresas y las ciencias hasta la atención médica, la administración, la educación, la economía, las humanidades y todos los demás aspectos de la sociedad"[5]. Así, los anclajes de la cuarta revolución industrial redimensionan, en su conjunto, los procesos de automatización y digitalización, vuelven a profundizar en las consecuencias del cambio tecnológico, y complejizan aún más las dimensiones del mismo[6] hasta llegar a la esfera laboral, en cuyo ámbito, y por lo que aquí interesa, la protección d ellos datos de salud de los trabajadores cobra una especial dimensión, dadas las múltiples implicaciones existentes y las posibles vulneraciones de derechos que se pueden producir en este campo.

---

[3] AA.VV.: *Industria conectada* 4.0. *La transformación digital de la industria española*, Madrid (Ministerio de Industria), 2015, pág. 5 y ss., señalando cómo "la industria está abocada a una transformación digital que afectará a todas las empresas y todas tendrán la necesidad de adaptarse a esa transformación".

[4] ÁLVAREZ CUESTA, H.: *El futuro del trabajo vs. el trabajo del futuro*, cit., pág. 16.

[5] Un análisis exhaustivo general de la materia en MAYER-SCHÖENBERG, V. y CUKIER, K.: *Big Data. A revolution that will transform how we live, work and think*, Boston/Nueva York (Eamon Dolan Book/Mariner Books/Houghton Mifflin Harcourt), 2013, (en version traducida: *Big Data. La revolución de los datos masivos*, Madrid (Turner), 2013), pág. 3 y ss., quienes señalan cómo la salud pública es solo un área en la cual el big data marca una gran diferencia y destacan el hecho de que no existe ninguna definición rigurosa de los datos masivos, o *big data*, que deben ser entendidos en un contexto en el que el volumen de información ha aumentado de manera exponencial, lo que ha favorecido nuevas tecnologías de procesamiento que permiten recopilar y analizar cientos de miles de millones de puntos de datos.

[6] ALEMÁN PÁEZ, F.: "El derecho de desconexión digital. Una aproximación conceptual, crítica y contextualizadora al hilo de la Loi Travail n.º 2016-1088", *Trabajo y Derecho. Nueva revista de actualidad y relaciones laborales*, núm. 30, 2017, pág. 12 y ss.

En este sentido, lógicamente, el mundo del trabajo y de la prevención de riesgos laborales no ha sido ni mucho menos ajeno a esta realidad, sino más bien al contrario, se ha erigido como uno de sus grandes protagonistas, habida cuenta de que en el marco del indudable impacto del tan inexorable como forzoso avance de las nuevas tecnologías en todos los órdenes de nuestra vida, las relaciones laborales son, obviamente, uno de los aspectos en los cuales más se va a ver su influencia. La irrupción de la digitalización en el ámbito laboral, tanto desde una perspectiva individual como colectiva, ha provocado "un profundo impacto transversal sobre el conjunto de las instituciones reguladoras de las relaciones laborales"[7].

La transformación digital ha traído de la mano múltiples nuevas formas de trabajo, tipo de organizaciones y perfiles profesionales que requieren la adopción de una estrategia de seguridad y Prevención de Riesgos Laborales adecuada, avanzada, moderna y adaptada a cada uno de ellos y, por otra parte, respetuosa con la protección de datos del trabajador, un derecho en riesgo permanente por sus propias características, pues la amenaza y la inseguridad del afectado pueden provenir no solo de la empresa para la que se prestan servicios, sino también del exterior por diferentes medios como los miles de ciberataques diarios que se producen a distintos niveles, riesgos ante los cuales el Derecho está reaccionando para proteger la privacidad y la intimidad de las personas, pero necesitado de pasos más profundos en el día a día de la empresa en cuanto a la protección de datos y cuestiones relativas a los datos de salud de los trabajadores.

La introducción de nuevas tecnologías en las actividades humanas provoca la aparición de supuestos de hecho hasta ahora inéditos[8], habida cuenta de que en muchas ocasiones no se encuentran regulados en la normativa y constituyen auténticas lagunas, de forma tal que un

[7] CRUZ VILLALÓN, J. "El impacto de la digitalización sobre los derechos fundamentales laborales", en AA.VV. (RODRÍGUEZ-PIÑERO ROYO, M. y TODOLÍ SIGNES, A., Dirs.): *Vigilancia y control en el Derecho del Trabajo digital*, Pamplona (Aranzadi), 2020, pág. 35.

[8] FERNÁNDEZ COSTALES, J.: "La aplicación y la incidencia de la informática en el ámbito del Derecho Civil", *Revista General de Legislación y Jurisprudencia*, núm.4, 1985, pág. 508.

cambio tecnológico en su incidencia en el ordenamiento jurídico provoca la aparición de un supuesto de hecho enteramente nuevo respecto a la cual falta la normativa concreta y genera una laguna legal[9]. Además, la reiteración típica de una serie de hechos nuevos constituye o crea una nueva problemática social que, a su vez, exige un tratamiento jurídico nuevo, distinto en sus principios rectores y en sus directrices.

2. El tratamiento y protección de datos de salud

Un aspecto que guarda evidente relación con algunas de las cuestiones anteriormente tratadas y acrecienta las dificultades es la voluntariedad y el respeto a la intimidad y confidencialidad de datos del trabajador en los reconocimientos médicos, no en vano la protección de los datos e informaciones relativas a la salud y, en especial, la historia clínica[10], "es uno de los aspectos del derecho a la intimidad que presenta mayor relevancia desde el punto de vista de su titularidad por parte del usuario de los servicios sanitarios"[11].

La nueva realidad digital y conectada viene a añadir relevancia a ciertos aspectos preventivos que hasta ahora podían pasar desapercibidos o no tener apenas importancia en la mayoría de las empresas. En este punto, entraría en juego la protección de datos como un elemento a tener muy en cuenta, también en materia preventiva. La utilización y manipulación de datos personales integrados en ficheros informáticos hace necesaria una protección jurídica de la persona y de tales datos, en tanto se ve afectado un derecho fundamental, como es la intimidad personal, tal y como ya se destacó, sin olvidar tampoco cómo el propio artículo 18

[9] DÍEZ-PICAZO, L.: *Experiencias jurídicas y teoría del Derecho*, 3.ª ed., Barcelona (Ariel), 1993, págs. 314-315.

[10] Sobre la materia, RODRÍGUIEZ ESCANCIANO, S.: "La intimidad del trabajador en el uso de diagnósticos médicos informatizados", *Revista Española de Derecho del Trabajo*, núm. 101, 2000, pág. 176 y ss.

[11] TARODO SORIA, S.: *Libertad de conciencia y derechos del usuario de los servicios sanitarios*, Bilbao (Universidad del País Vasco), 2005, pág. 353.

CE que lo regula, en su apartado 4 establece que "la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

Aun cuando en un primer momento el derecho a la intimidad se configuraba como un derecho del titular a exigir la no inferencia de terceros en su vida privada, al apreciarse la necesidad de su protección frente al creciente desarrollo de los medios y procedimientos de captación, divulgación y difusión de la misma y de datos y circunstancias pertenecientes a ella, pasó a concebirse en virtud de la doctrina del Tribunal Constitucional[12] como un bien jurídico que se relaciona con la libertad de acción del sujeto, las facultades positivas de actuación para controlar la información relativa a su persona y su familia en el ámbito público, dando forma a lo que se ha dado en llamar segunda dimensión de la intimidad, conocida como libertad informática o habeas data que encuentra su apoyo en el artículo 18.4 CE.

Las continuas innovaciones tecnológicas encuentran "pilar y exponente fundamental" en la cada vez más extensa e intensa utilización de la informática en la actividad productiva[13]. Tal circunstancia no solo ha venido a afectar de forma determinante a los instrumentos de trabajo y al desarrollo de las relaciones en la empresa, sino que también ha generado nuevos problemas que, lógicamente, cuestionan la validez de determinadas soluciones dadas por el ordenamiento ante una realidad empresarial que día a día se ve superada[14] por una realidad social en continuo avance, de forma tal que el ordenamiento en su conjunto, y la disciplina laboral por lo que aquí interesa, deben afrontar una necesaria y permanente adaptación a los nuevos tiempos y a los cambios tecnológicos en curso[15].

---

[12] Así, STCo 144/99 de 22 de julio.

[13] RODRÍGUEZ ESCANCIANO, S.: "La potencialidad lesiva de la informática sobre los derechos de los trabajadores", en *Revista Española de Protección de Datos*, núm. 2, 2007, pág. 97.

[14] LUJÁN ALCARAZ, J.: "Uso y control en la empresa de los medios informáticos de comunicación", *Aranzadi Social*, T. II, 2005, pág. 55.

[15] GOÑI SEIN, J. L.: "Flexibilidad y revisión del ámbito del Derecho del Trabajo", en AA.VV. (RIVERO LAMAS, J., Coord.): *La flexibilidad laboral en España*, Zaragoza (Instituto de Relaciones Laborales), 1993, pág. 71.

La gestión informatizada del personal facilita que todos los datos concernientes al desarrollo del contrato de trabajo, desde el momento de la selección de personal, pasando por la constitución del vínculo contractual hasta su resolución, sean incluidos en los soportes informáticos de la empresa. Además, no se puede obviar cómo la incorporación del trabajador a la organización productiva empresarial favorece tanto una continua adquisición de información sobre extremos personales de diversa naturaleza como su minuciosa puesta al día. Al aumentar los medios técnicos, el poder del empresario sobre la prestación laboral y sobre el propio trabajador también crece, hecho que constituye una amenaza real para los derechos del empleado. La protección de tales derechos frente al uso ilegítimo de la informática es una necesidad "que se deja sentir con la mayor crudeza en el ámbito objetivo de las relaciones laborales"[16] en tanto en cuanto el tratamiento de datos constituye una práctica cada día más extendida, incluso imprescindible en ya numerosísimos supuestos, hasta el punto de poder afirmar que "gestión de personal e informática son, hoy en día, términos parejos"[17].

Desde tales premisas, cobra especial relevancia la necesidad de proteger el interés legítimo del trabajador de controlar sus datos personales insertos en los sistemas de comunicación empresariales, habida cuenta de que únicamente de tal forma se podrá evitar una afectación negativa durante la relación laboral, máxime si se trata de datos especialmente sensibles, obtenidos en el cumplimiento de las obligaciones relacionadas con la Prevención de Riesgos Laborales principalmente a través de la realización de los pertinentes reconocimientos médicos.

El Tribunal Constitucional ha mantenido en algunos pronunciamientos la idea de que la práctica totalidad de los derechos de la persona pueden verse afectados por un indebido tratamiento de datos,

[16] RODRÍGUEZ ESCANCIANO, S.: "La potencialidad lesiva de la informática sobre los derechos de los trabajadores", cit., pág. 115.

[17] BORRAJO DACRUZ, E.: "El impacto de tecnologías y medios de información en el Derecho del Trabajo", en AA.VV.: *Implicaciones socio-jurídicas de las tecnologías de la información: encuentros 1980-1990: los juristas ante la revolución informática*, Madrid (CITEMA), 1991, pág. 71.

considerando la protección de los mismos como un derecho fundamental que "amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona"[18].

Los reconocimientos médicos permiten, mediante la realización de pruebas clínicas, averiguaciones biológicas o biométricas, la evaluación del estado de salud del trabajador, el conocimiento de sus posibles patologías y su origen así como la aplicación de los oportunos remedios en orden a un eventual restablecimiento del bienestar, tratamientos en los cuales las nuevas tecnologías pueden estar muy presentes a través de mecanismos como la vigilancia del paciente en sus patrones de ingesta y seguimiento de estos, por lo que habría que abordar los riesgos que conllevaría un control invasivo de la persona utilizando tecnologías embebidas dentro del medicamento y adheridas al cuerpo del individuo, con la finalidad de facilitar a los facultativos un control de los patrones de correcto o incorrecto seguimiento de su tratamiento, con lo que ello puede afectar a la autonomía del paciente/trabajador, tecnologías que, en definitiva, facilitan un control exhaustivo de la conducta de la persona sometida a un tratamiento y el acceso por parte de terceros a una importante cantidad de datos de salud[19].

---

[18] "Sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar o a cualquier otro bien constitucionalmente amparado… [de forma tal que] el objeto de protección del derecho fundamental a la protección de datos no se reduce solo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es solo la intimidad individual, que para ello está la protección que el artículo 18.1 de la CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos", SSTCo 292/2000, de 30 de noviembre o 70/2009, de 23 de marzo.

[19] Sobre la materia, de interés, DE MIGUEL BERIAIN, I. y MORLA GONZÁLEZ, M.: "Digital pills for mental diseases: an ethical and social analysis of the issues behind the concept", *Journal of Law and the Biosciences*, agosto 2020, pág. 3 y ss. quienes señalan que, además, podría ser un medio esencial para el sostenimiento y mejora del sistema sanitario, dado que habitualmente la información que el paciente proporciona a su profesional no siempre resulta plenamente fiable y los métodos de control del paciente son ineficientes.

En este sentido, los riesgos fundamentales que el uso de la informática entrañan para los derechos de quien presta servicios por cuenta ajena aparecen fundamentalmente derivados de su capacidad para recopilar y transmitir datos sobre la persona del trabajador, así como la capacidad de tratamiento o elaboración de la información obtenida, permitiendo un ilimitado e indiscriminado manejo de informaciones sobre los empleados, lo que facilita a la empresa el acceso al conocimiento de circunstancias personales con su total desconocimiento[20].

Resulta fácil, por tanto, observar el potencial peligro que derivaría de un inadecuado uso de tales informaciones, que adecuadamente tratadas y cruzadas llegarían a permitir a la unidad productiva elaborar perfiles extremadamente precisos sobre sus empleados que incluyan datos de su más estricta intimidad (estado de salud, tendencias sexuales, afiliación sindical o política, aficiones…), circunstancia que podría dar lugar al inicio de actuaciones discriminatorias camufladas bajo otras formas y basadas en tales conocimientos, momento en el cual la información como poder deja atrás "su carácter de tópico para convertirse en una muy tangible realidad"[21].

Así, vista la agresividad que la informática puede poseer frente a los derechos del individuo en el marco de una prestación de servicios, lo importante será, por tanto, establecer un punto de equilibrio entre el derecho del empresario a utilizar de la forma más óptima las posibilidades que las nuevas tecnologías ponen a su alcance y la correcta preservación y respeto de los derechos y libertades fundamentales del trabajador[22].

---

[20] GOÑI SEIN, J. L.: "Vulneración de derechos fundamentales en el trabajo mediante instrumentos informáticos, de comunicación y archivo de datos", en AA.VV. (ALARCÓN CARACUEL, M. R. y ESTEBAN LEGARRETA, R., Coords.): *Nuevas tecnologías de la información y la comunicación y Derecho del Trabajo*, Albacete (Bomarzo), 2004, pág. 51.

[21] TASCÓN LÓPEZ, R.: "Sobre la ejecución procesal de las obligaciones derivadas de la legislación sobre protección de datos personales; en este caso, eliminar los datos relativos a los diagnósticos médicos de los trabajadores de un archivo empresarial sobre absentismo con baja médica (Comentario a la STCo 153/2004, de 20 de septiembre)", *Revista Española de Protección de Datos*, núm. 2, 2007, pág. 223.

[22] Al respecto, LUJÁN ALCARAZ, J.: "Uso y control en la empresa de los medios informáticos de comunicación", *Aranzadi Social*, cit., pág. 55.

El ordenamiento social permanece, no obstante, ayuno de una regulación específica, de forma tal que, en este intento, como suele ser habitual, la normativa laboral debe iniciar su regulación desde reglas jurídicas que ordenan con carácter general el tratamiento automatizado de datos personales para, a partir de las mismas, y como un plus a través del cual atender a las circunstancias específicas presentes en la relación de trabajo, proceder a la construcción de principios y reglas especiales[23].

En cualquier caso, la elaboración de un concepto de dato relativo a la salud constituye una de esas cuestiones pendientes de culminación[24], en tanto a día de hoy no existe texto legal interno alguno que aporte una definición vinculante, aun cuando afortunadamente sí cabe destacar la existencia de una categoría de datos sensibles o especialmente protegidos[25] en la cual aparecen incardinados aquellos relativos a la salud.

Se está, por tanto, ante un derecho en riesgo permanente por sus propias características, pues la amenaza y la inseguridad del trabajador pueden provenir no solo de la empresa para la que se prestan servicios, sino también del exterior por diferentes medios como los miles de ciberataques diarios que se producen a distintos niveles, riesgos ante los cuales el Derecho está reaccionando para proteger la privacidad y la intimidad de las personas, pero necesitado de pasos más profundos en el día a día de la empresa en cuanto a la protección de datos y cuestiones relativas a los datos de salud de los trabajadores.

En esta línea, el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección

---

[23] FERNÁNDEZ DOMÍNGUEZ, J. J. y RODRÍGUEZ ESCANCIANO, S.: *Utilización y control de datos laborales automatizados*, Madrid (Agencia de Protección de Datos), 1997, pág. 101.

[24] Al respecto, DE MIGUEL SÁNCHEZ, N.: "Investigación y protección de datos de carácter personal: una aproximación a la Ley 14/2007, de 3 de julio, de investigación biomédica", *Revista Española de Protección de Datos*, núm. 1, 2006, págs. 146-147.

[25] Sobre la materia, y en torno al concepto de los datos de salud, FERNÁNDEZ LÓPEZ, J. M.: "El derecho fundamental a la protección de datos personales. Obligaciones que derivan para el personal sanitario", *Derecho y Salud*, Número extraordinario del XI Congreso de Derecho y Salud, 2003, págs. 42 y ss.

de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[26], ha venido a destacar, en su considerando 35, cómo "entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro", incluyendo la información sobre la persona física recogida con ocasión de su inscripción "a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia…; todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro".

En este sentido, algún autor ha venido a entender que este concepto abarcaría los datos de carácter médico, pero también los que mantengan conexión con fines relacionados con la salud, ya sean tratados en el ámbito de la salud pública, en seguros de enfermedad o en actividades científicas o estadísticas, incorporando todo lo relativo al cuerpo humano y afectando, por tanto, a la sexualidad, raza y código genético[27] e incluyendo antecedentes familiares, hábitos de vida y consumo y

[26] Un amplio estudio sobre la norma en PRECIADO DOMÈNECH, C. H.: *El Derecho a la Protección de Datos en el contrato de trabajo. Adaptado al nuevo Reglamento 679/2016, de 27 de abril*, Pamplona, (Aranzadi), 2017, pág. 29 y ss. o BLÁZQUEZ AGUDO, E. M.ª.: *Aplicación práctica de la protección de datos en las relaciones laborales*, Madrid (CISS), 2018, pág 21 y ss.

[27] HEREDERO HIGUERAS, M.: "La protección de datos de salud informatizados en la Ley Orgánica 5/1992, de 29 de octubre", *Derecho y Salud*, Vol. 2, 1994, pág. 19.

enfermedades presentes, pasada o previsibles en un futuro[28], así como los datos psicológicos y referentes a la salud mental[29].

Destacar cómo, y aun cuando la primera parte del concepto señalado resulta válida en tanto efectivamente se trata de datos de carácter personal, no puede obviarse que jurídicamente la inclusión en el expediente médico-laboral de datos como los señalados supondría, salvo consentimiento expreso del afectado, una clara y flagrante vulneración del derecho a la intimidad de la persona. Más aún si a datos médicos en el marco de la relación laboral se está haciendo referencia, en tanto el personal médico no podrá realizar más pruebas que las estrictamente necesarias e imprescindibles, dado que, de otra forma, constituiría una intromisión ilegítima en la intimidad del trabajador.

En todo caso, y por mor de la propia actividad médica, la información de carácter personal en torno a esta cuestión incluirá tanto datos sobre salud que tengan que ver con el puesto de trabajo como otros que no tienen tal relación pero han surgido inevitablemente de la práctica del examen médico, por lo que cabe colegir que será necesaria una acepción amplia del concepto de información médica de carácter personal, aun cuando no cabe olvidar en ningún momento que las conclusiones extraídas de dicha información deben aparecer relacionadas exclusivamente con la aptitud del trabajador para desempeñar sus obligaciones profesionales o con la necesidad de mejorar o introducir nuevas medidas preventivas y protectoras frente a determinados riesgos, pues no puede obviarse el hecho de que los reconocimientos realizados tienen

[28] LUCAS MURILLO DE LA CUEVA, P.: "El tratamiento jurídico de los documentos y registros sanitarios informatizados y no informatizados", en AA.VV.: ***Información y documentación clínica (Actas del Seminario Conjunto sobre Información y Documentación Clínica celebrado en Madrid los días 22 y 23 de septiembre de 1997), Vol. II*, Madrid (CGPJ/ MSC), 1997, págs. 586-587.**

[29] SÁNCHEZ-CARO, J. y ABELLÁN, F.: *Telemedicina y protección de datos sanitarios. Aspectos legales y éticos*, Granada (Comares), 2002, pág. 45, quienes incluyen los datos de salud mental y psíquicos en el concepto de salud "bien deriven expresamente de historiales médicos (de un determinado tratamiento psicológico o psiquiátrico), bien provengan de encuestas, y en este último supuesto por considerar que, en cualquier caso, se trata de datos referentes a la salud de las personas, que concierne directamente a su salud mental o se encuentran estrechamente relacionados con esta última".

en todo momento una finalidad preventiva y no terapéutica, que se enmarcaría en otro estadio.

Así, partiendo del principio de la pertinencia y proporcionalidad de las pruebas y los resultados a los supuestos que justifican la vigilancia de la salud, no ha faltado algún autor para quien cabría plantearse la legitimidad de incluir en el historial clínico de un trabajador las noticias o datos sobre su estado de salud que no resulten relevantes dentro de la política de Prevención de Riesgos Laborales[30].

Desde la óptica del cumplimiento de la obligación empresarial de proporcionar seguridad en el trabajo, los resultados de los reconocimientos médicos "permitirán planificar y, en su caso, reorientar la actividad preventiva en la empresa. Ahora bien, ocurre que el reconocimiento médico implica, en sí mismo, una intromisión en la esfera privativa del trabajador. Tal contraposición de intereses exige la búsqueda de un punto de equilibrio"[31]. Así, vista la agresividad que la informática puede poseer frente a los derechos del individuo en el marco de una prestación de servicios, lo importante será, por tanto, establecer ese punto de equidad entre el derecho del empresario a utilizar de la forma más óptima las posibilidades que las nuevas tecnologías ponen a su alcance y la correcta preservación y respeto de los derechos y libertades fundamentales del trabajador[32].

Cuestión distinta la constituye la facultad otorgada al empresario ya mencionada en epígrafes anteriores que le permite verificar el estado de salud alegado por el trabajador para justificar su falta de asistencia al trabajo mediante la realización de un reconocimiento a cargo del personal médico, pudiendo significar una negativa del empleado la

[30] Principio que "parece ser el adoptado en el artículo 37 RSP", MARTÍNEZ FONS, D.: *La vigilancia de la salud de los trabajadores en la Ley de Prevención de Riesgos Laborales*, Valencia (Tirant lo Blanch), 2002, págs. 97-98.

[31] RODRÍGUEZ ESCANCIANO, S.: "El tratamiento de datos sensibles vinculados a la Prevención de Riesgos Laborales", *Revista Jurídica de la Universidad de León*, núm. 5, 2018, pág. 168.

[32] Al respecto, LUJÁN ALCARAZ, J.: "Uso y control en la empresa de los medios informáticos de comunicación", *Aranzadi Social*, cit., pág. 55.

suspensión de los derechos económicos que pudieran existir a cargo de quien proporciona empleo por dichas situaciones (art. 20.4 ET)[33].

Dicho control ni es equiparable ni sigue las mismas reglas que la vigilancia de la salud en materia de Prevención de Riesgos Laborales, pues sus objetivos se centran básicamente en un control del absentismo. En cualquier caso, afecta a la materia ahora tratada en tanto en cuanto implica la verificación de la existencia de enfermedad, circunstancia que va a significar un tratamiento de datos de salud, y por tanto de una categoría especial de datos, teniendo como base jurídica para el tratamiento de estos el propio contrato de trabajo (art. 6.2.b del RGPD) en relación con las facultades concedidas por el artículo 20.4 ET, de forma tal que no se requiere el consentimiento del afectado.

En cualquier caso, la empresa tampoco se encuentra legitimada en este supuesto para conocer los detalles concretos del reconocimiento médico, sino únicamente su conclusión, que no puede ser otra que determinar si la persona está o no en condiciones psicofísicas de reincorporarse a su puesto de trabajo.

En este sentido, la incorporación de datos de salud a un fichero con la única finalidad de realizar controles del absentismo resulta desproporcionada, habida cuenta de que mediante la creación de tal base de datos "parece perseguirse un control más eficaz del absentismo laboral, según las facultades que al efecto reconoce al empresario la legislación vigente. En este sentido, lo primero que conviene advertir es que entre dichas facultades no figura la de proceder al almacenamiento en soporte informático de los datos atinentes a la salud de los trabajadores -y en concreto del diagnóstico médico- prescindiendo del consentimiento de estos. Por otra parte, y con independencia de ello, lo verdaderamente relevante es que la medida adoptada por la empresa, sometida a los cánones establecidos para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, no reviste la

[33] Sobre la cuestión, AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS: *La protección de datos en las relaciones laborales*, Madrid (Agencia Española de Protección de Datos), 2021, pág. 57.

consideración de solución idónea, necesaria y proporcionada para la consecución del fin, en este caso, el control del absentismo laboral", en tanto en cuanto no constituye una medida "ponderada y equilibrada, ya que de ella no se derivan más beneficios o ventajas para el interés general o para el interés empresarial que perjuicios sobre el invocado derecho a la intimidad"[34].

Así, y atendiendo al contenido del fichero cabe destacar que su mantenimiento "no se dirige a la preservación de la salud de los trabajadores sino al control del absentismo laboral, lo que, por otra parte, resulta plenamente acorde con la denominación "absentismo con baja médica" que recibe el fichero. Consecuentemente, la creación y actualización del fichero, en los términos en que se ha llevado a efecto, no puede ampararse, frente a lo sostenido por la empresa, en la existencia de un interés general (art. 7.3 L.O.R.T.A.D. y, por remisión, arts. 10.11 y 61 L.G.S.), que justificaría la autorización por ley, sin necesidad del consentimiento del trabajador, para el tratamiento Control de la actividad laboral… [como no puede serlo en la protección de datos automatizados] en las relaciones laborales de los datos atinentes a su salud, ni tampoco en lo dispuesto en los arts. 22 y 23 de la Ley de Prevención de Riesgos Laborales, habida cuenta de que en el fichero en cuestión no se reflejan los resultados arrojados por la vigilancia periódica -y consentida por los afectados- del estado de salud de los trabajadores en función de los riesgos inherentes a su actividad laboral"[35].

Por otra parte, este control del absentismo adquiere una relevancia particular cuando su desarrollo corre a cargo de un prestador de servicios externo ya que, además de cumplir con las obligaciones propias de un encargado del tratamiento, debe atenerse a ciertas condiciones: en primer término, la información a la persona trabajadora debe ser muy precisa e indicar que se trata de un control laboral, debiendo tal

[34] STC 202/1999, de 8 de noviembre. Sobre la materia, también, SSTC 207/1996, de 16 de diciembre o 69/1999, de 26 de abril.

[35] STSJ Madrid 8 marzo 2019 (JUR 118324).

información referirse a que se están verificando sus condiciones de aptitud por cuenta de la empresa y que el tratamiento de datos se ampara en el art. 20.4 del ET; de otro lado, la incorporación de los datos de salud de la persona trabajadora por parte del prestador de ese servicio a una historia clínica le convertirá en responsable del tratamiento[36].

Será también válido en estos supuestos que la empresa subcontrate los servicios médicos de una sociedad externa para reconocer a los trabajadores que se ausentan por motivos de salud, siempre y cuando esta se realice dentro de los límites de la buena fe y sea proporcional con los objetivos buscados[37], encontrándose legitimadas para elaborar estadísticas sobre el índice de absentismo y sus causas, aunque, eso sí, estas no pueden contener datos personales, sino únicamente datos disociados al objeto de impedir la identificación de las personas concretas que constan en fichero.

2.1. La Ley de Protección de Datos y los daños a la salud de los trabajadores

Tras la aprobación de la nueva Ley de Protección de Datos se hace necesario analizar sus contenidos y los principios y garantías recogidos en el Reglamento UE 2016/679 del Parlamento europeo y del Consejo de 27 de abril de 2016, de Protección de Datos Personales[38], sin olvidar tampoco las pautas introducidas al respecto en la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales, que acoge como postulado básico la autonomía de la persona del trabajador para someterse o no a los reconocimientos médicos, propuestos por la empresa, permitiendo, en su caso, exploraciones y analíticas sobre datos corporales, o impidiendo pruebas clínicas ajenas a la finalidad de la vigilancia de la

[36] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS: *La protección de datos en las relaciones laborales*, cit., pág. 58.

[37] STS 25 enero 2018 (RJ 725).

[38] Al respecto, GARCÍA MURCIA, J. y RODRÍGUEZ CARDO, I. A.: "La protección de datos personales en el ámbito del trabajo: una aproximación desde el nuevo marco normativo", *Nueva Revista Española de Derecho del Trabajo*, núm. 216, 2019, pág. 20 y ss.

salud en relación con los riegos inherentes al trabajo. Este criterio se conecta directamente con la obligación de información previa, de forma que el trabajador debe ser expresamente alertado sobre los exámenes médicos especialmente invasores de su intimidad al tiempo de otorgar su consentimiento[39].

La redacción utilizada por la Ley de Prevención de Riesgos al señalar la confidencialidad de estos datos y la imposibilidad de su uso con fines discriminatorios o en perjuicio del trabajador está aludiendo a las normas sobre protección de datos de carácter personal[40], en particular, al artículo 5 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, de acuerdo con el cual "los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1 f) del Reglamento (UE) 2016/679"[41], destacando que "la obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable".

Quedan, en definitiva, proscritas las vigilancias médicas indiscriminadas, injustificadas o generalizadas para cualquier caso o actividad[42], aun cuando, funcionando como una especie de excepción a la

[39] Sobre estas cuestiones, entre otros, PEDROSA ALQUÉZAR, S. I.: *La vigilancia de la salud en el ámbito laboral. Regulación legal, límites y cuestiones problemáticas*, Madrid (CES), 2005, pág. 120 y ss.; ARIAS DOMÍNGUEZ, A. y RUBIO SÁNCHEZ, F.: *El derecho de los trabajadores a su intimidad*, Pamplona (Thomson/Aranzadi), 2006, pág. 123 y ss. o FERNÁNDEZ-COSTALES MUÑIZ, J.: *La vigilancia de la salud de los trabajadores*, León (Junta de Castilla y León/Eolas), 2009, pág. 95 y ss.

[40] FERNÁNDEZ-COSTALES MUÑIZ, J.: *Prevención de Riesgos Laborales y empresa: obligaciones y responsabilidades*, Pamplona (Aranzadi), 2019, págs 143-144.

[41] Sobre esta cuestión en el Reglamento europeo, PEDROSA ALQUÉZAR, S. I.: "Vigilancia de la salud laboral y protección de datos", *Revista del Ministerio de Empleo y Seguridad Social*, núm. 137, 2018, pág. 166 y ss.

[42] SÁNCHEZ CUBEL, M. D.: *Todo sobre la nueva Ley de Prevención de Riesgos Laborales*, Barcelona (Praxis), 1996, pág. 89.

excepción, no cabe olvidar la necesidad del consentimiento[43] expreso del trabajador o que una Ley, por razones de interés general, permita el tratamiento de estos datos especialmente sensibles, tal y como establece el artículo 9.2 del RGPD y su trasposición en España a través del artículo 9.2 LOPDP, que destaca cómo "los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad… En particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte".

Además, el artículo 9.2.h) del Reglamento admite la recogida y tratamiento de datos con fines de "medicina preventiva o laboral" y "evaluación de la capacidad laboral del trabajador", sin perjuicio de que hayan de respetarse las garantías y límites pertinentes en relación con los datos que se pretenden obtener y su posible uso posterior.

La determinación del sujeto responsable del fichero que integre las obligaciones relativas a la salud "requiere la previa determinación del sujeto de quién deba predicarse la obligación de mantener la información relativa a la salud, así como la extensión de la misma", siendo posible diferenciar al menos tres hipótesis distintas: "el personal médico que practica las medidas de vigilancia, el empresario sobre el que recae la obligación legal de mantener la información derivada de la vigilancia de la salud y, en fin, la existencia de servicios de prevención internos o externos encargados de la vigilancia de la salud"[44].

---

[43] Sobre la materia, GOÑI SEIN, J. L.: "Vulneración de derechos fundamentales en el trabajo mediante instrumentos informáticos, de comunicación y archivo de datos", en AA.VV. (ALARCÓN CARACUEL, M. R. y ESTEBAN LEGARRETA, R., Coords.): *Nuevas tecnologías de la información y la comunicación y Derecho del Trabajo*, Albacete (Bomarzo), 2004, pág. 55 y ss.

[44] MARTÍNEZ FONS, D.: *La vigilancia de la salud de los trabajadores en la Ley de Prevención de Riesgos Laborales*, cit., págs. 110 y ss.

En este sentido, cabe destacar cómo la nueva normativa obliga a que los responsables y encargados determinen "las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa" (arts. 24 y 25 RGPD y 28 LOPDP).

Todos los datos extraídos del cumplimiento del deber empresarial de garantizar la salud deben ser almacenados en ficheros de la empresa, quedando condicionado su mantenimiento en ellos a su utilidad y, consecuentemente, a su periódica actualización. Es más, el empresario debe elaborar y conservar a disposición de la autoridad competente la documentación por la que acredite que efectivamente cumple con el deber de control de la salud de los trabajadores y las conclusiones que se deriven de los reconocimientos médicos practicados.

Así, el cumplimiento de lo previsto demanda al titular de la organización empresarial realizar un acopio documental que, en ciertos casos, dependiendo de la índole de la actividad empresarial, puede resultar ingente, y para su organización resultará de todo punto necesaria su acumulación en ficheros, de los cuales es responsable precisamente el empresario, aunque, paradójicamente, no tiene derecho al acceso a la totalidad del contenido de los mismos[45]. No cabe olvidar, en definitiva, que uno de los principios fundamentales de un adecuado sistema de tratamiento de datos viene dado por conseguir un "escrupuloso respeto a la confidencialidad de los mismos"[46] en tanto en cuanto esta forma parte fundamental e inescindible del derecho a la intimidad de la persona.

Cabe señalar también la importancia del principio de veracidad, el cual viene a exigir que los datos de carácter personal almacenados sean

---

[45] PRADAS MONTILLA, R.: "Empresas y protección de datos de carácter personal", *Actualidad Laboral*, T. I, 2003, pág. 73.

[46] PEDROSA ALQUÉZAR, S. I.: *La vigilancia de la salud en el ámbito laboral. Regulación legal, límites y cuestiones problemáticas*, cit., pág. 119.

exactos y estén actualizados, de forma tal que el trabajador no se vea lesionado en su posición jurídica en tanto la empresa pueda tomar decisiones partiendo de datos inexactos o desactualizados que, incluso, puedan ir en detrimento de la propia salud. Ello permitirá hacer uso de los derechos de rectificación o cancelación regulados en los artículos 14 y 15 LOPDP.

No obstante, si los datos resultaren pertinentes para otro fin compatible (art. 6.4 LOPDP) y resulten útiles al empresario para la organización y dirección de la prestación laboral en la unidad productiva, deberá permitirse su mantenimiento[47], previa notificación o petición de consentimiento respecto a esta nueva finalidad a cual serán destinados, habida cuenta de que obstaculizar con garantías "excesivamente formalistas" una actividad empresarial cada vez más irremediablemente obligada al uso de sistemas informáticos no ofrece a día de hoy una lógica clara, pues resultaría absurdo la exigencia de cancelación de una serie de datos que ya se poseen y se necesitan para un nuevo fin en tanto significaría obligar a una segunda recogida de los mismos, sin que tal circunstancia redunde en una mayor garantía de los derechos del trabajador[48].

Estos principios y derechos implican que los datos no podrán ser mantenidos por tiempo ilimitado[49], siendo el principio de conservación limitada otro de los aplicables a la protección de datos y a la vigilancia de la salud, de acuerdo con el cual los pormenores referentes al control médico únicamente permanecerán en los ficheros por el tiempo

[47] Sobre la conservación y custodia de la historia clínica, con carácter general, AYERRA LAZCANO, J. M.ª.: "Regulación general de la historia clínica", *Derecho y Salud*, Vol. 11, 2003, págs. 29 y ss.

[48] En tal sentido, aunque no en el ámbito estricto de los datos de salud, FERNÁNDEZ VILLAZÓN, L. A.: "Tratamiento automatizado de datos personales en los procesos de selección de trabajadores", *Relaciones Laborales*, T. I, 1994, pág. 537.

[49] En torno a la materia, destacando las distintas legislaciones autonómicas a este respecto, o haciendo notar cuestiones como los plazos de una posible reclamación en vía civil o penal por actuaciones médicas, ÁLVAREZ CIVANTOS, O. J.: *Normas para la implantación de una eficaz protección de datos de carácter personal en empresas y entidades*, Granada (Comares), 2002, págs. 261 y ss.

necesario para el cumplimiento de los fines para los cuales fueron en su momento recabados. Así, ante los resultados de un nuevo examen habrá de determinarse cuáles mantienen su validez respecto a los anteriores para contribuir a una eficaz protección, de forma tal que si algún dato carece ya de utilidad deberá ser cancelado[50].

De tal manera, parece evidente que ante determinados supuestos, como que el trabajador cambie de empresa o cuando tras un proceso de selección no haya sido aceptado para formar parte de la misma, el fin para el cual las informaciones fueron recogidas desaparece, careciendo de sentido su mantenimiento en poder de la unidad productiva, resultando lo contrario en todo caso una intolerable apropiación perpetua e indebida de amplios aspectos y facetas de la vida personal del sujeto[51].

El artículo 18.1 CE impide las injerencias "arbitrarias o ilegales" en la intimidad. De tal premisa cabe deducir cómo el derecho a la intimidad personal será vulnerado cuando la intromisión en el ámbito propio y reservado del sujeto no sea acorde con la Ley, no sea eficazmente consentida o, aún autorizada, subvierta los términos y el alcance para el que se otorgó el consentimiento, quebrando la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida. La ley impone, por tanto, no solo la confidencialidad de los datos recabados y análisis realizados en los reconocimientos médicos, sino también su realización en la forma y con los medios que no lleguen a suponer una intrusión fuera de contexto en la vida privada e íntima del trabajador.

En cualquier caso, y con todo, al tener que entregar las conclusiones que tengan que ver con el correcto desarrollo de las funciones en materia preventiva, la confidencialidad de la información puede correr riesgos que resultan difícilmente evitables. Que un dato tenga el

[50] PEDROSA ALQUÉZAR, S. I.: *La vigilancia de la salud en el ámbito laboral. Regulación legal, límites y cuestiones problemáticas*, cit., págs. 168-169.

[51] MURILLO DE LA CUEVA, P. L.: "Informática y protección de datos personales (Estudio sobre la Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal)", *Cuadernos y Debates*, núm. 43, 1993, pág. 69.

carácter de confidencial significa su "reservabilidad", su mantenimiento en secreto frente a personas que no tienen interés legítimo alguno en su conocimiento, de forma tal que dicha privacidad debe ser interpretada de forma restrictiva y siempre funcionarizada directa e imprescindiblemente a la prevención.

El artículo 22 LPRL, al margen de establecer el principio de confidencialidad, lo modula también tomando en consideración la articulación de la documentación como resultados o como conclusiones de las pruebas practicadas, dando a los primeros una máxima confidencialidad, mientras las segundas ven mermado ese blindaje en virtud del tipo de datos que incorporan y la mayor cantidad de sujetos a los cuales se les comunican, aun cuando no deben en caso alguno trascender más allá de la Administración sanitaria, la empresa o los sujetos con responsabilidades en materia preventiva.

La información médica de carácter personal plasmada en los resultados de la vigilancia de la salud incluye (destacando así la amplia acepción que el término posee, aun cuando no todos los autores lo hayan considerado de tal manera), además de información sobre la salud que tiene que ver con el puesto de trabajo, datos que no poseen relación directa con la prestación de servicios pero que han surgido en la práctica del examen de salud. Referencia terminológica, en definitiva, orientada a unos resultados que, al pertenecer a la esfera íntima del trabajador, resultarán únicamente accesibles al personal médico o autoridades sanitarias que han desarrollado las distintas pruebas enmarcadas en el proceso de vigilancia de la salud, quienes deberán guardar secreto[52] respecto al contenido de los resultados frente al resto de personas con alguna relación con las tareas preventivas de vigilancia de la salud y, por supuesto, frente a terceros, excepción hecha del supuesto de que la no revelación de esos datos pudiera suponer un perjuicio para la salud de otros trabajadores o terceras personas relacionadas con la empresa o que por imperativo legal se establezca lo contrario.

[52] Al respecto, TOLOSA TRIBIÑO, C.: "El secreto profesional de los médicos en la Ley de Prevención de Riesgos Laborales", *Relaciones Laborales*, núm. 20, 1997, pág. 125 y ss.

Cuestión distinta es que, partiendo de tal información, resulte necesario extraer unas conclusiones relativas exclusivamente a la aptitud (o no) del empleado en relación con el desempeño de las obligaciones que su puesto de trabajo implica o con la posible necesidad de introducir cambios o mejoras preventivas y protectoras. Estas conclusiones se elaborarán utilizando, pero no incorporando, lo más destacado de la información médica, evitando facilitar información de índole médica o clínica o reflejar el problema de salud concreto padecido por un trabajador.

Respecto a las mismas el deber de confidencialidad aparece algo más relajado, en tanto que serán comunicadas al empresario y a ellas tendrán acceso las personas y órganos con responsabilidad en materia de prevención con objeto de que puedan desarrollar correctamente sus funciones, o lo que es lo mismo, delegados de prevención, comité de Seguridad y Salud y la representación unitaria y sindical de los trabajadores, quienes aparecen igualmente sometidos al deber de confidencialidad.

Esta obligación no solo atañe a estos y a los profesionales médicos, sino también al resto de profesionales y trabajadores del ámbito sanitario que participan en la asistencia del paciente. Así, bajo el paraguas de la confidencialidad se obliga también a sujetos tales como administrativos, documentalistas, informáticos, etc. que pueden tener acceso a datos de salud de los pacientes[53].

El acceso de los representantes de los trabajadores a datos sanitarios, debido a la sensibilidad y naturaleza de los mismos, parece hacer conveniente que los datos sean oportunamente disociados. Respecto a esta facultad de la que disfrutan los delegados de prevención de conocer y analizar los daños producidos en la salud e integridad física de los trabajadores del artículo 39.2 LPRL, al venir situados los objetivos en analizar las causas y proponer medidas preventivas oportunas, y aun

[53] SÁNCHEZ CARO, JAVIER Y ABELLÁN-GARCÍA SÁNCHEZ, FERNANDO: *Derechos y deberes de los pacientes (Ley 41/2002, de 14 de noviembre: consentimiento informado, historia clínica, intimidad e instrucciones previas)*, Granada (Comares), 2003, pág. 41 y ss.

cuando no faltan autores que opinan que tal disposición legal habilita en todo caso al tratamiento de datos personales de los trabajadores afectados, cabe destacar que no siempre será necesario conocer los datos personales del operario, aun cuando es posible que, en ocasiones, sea relevante identificar las condiciones particulares del sujeto para llevar a cabo de la manera más adecuada la tarea preventiva.

2.2. La anonimización de datos personales

En cualquier caso, y dada la excesiva implicación de una amplia pluralidad de sujetos con legitimidad en materia preventiva lo más razonable resulta mantener en el anonimato la identidad concreta del trabajador respecto al cual trascienden determinados datos médicos, de forma tal que únicamente se ofrezca el conocimiento de aspectos que permitan localizar el riesgo en el sistema organizativo de la empresa, utilizando para ello datos cifrados mediante claves codificadas o el envío de manera separada de los datos personales y de salud de los trabajadores impidiendo así la asociación de ambos.

En esta línea, el recurso que permite aminorar los riesgos y garantiza la seguridad en la utilización masiva de datos es la anonimización[54], que no es otra cosa, tal y como señala el Considerando 26 Reglamento 2016/679, que el vaciado de contenido personal de los datos denominados personales. Para anonimizar un dato debe vaciarse a este de todo aquel contenido que lo conecte con el individuo al cual pertenece, de forma tal que no pueda utilizarse para identificar a una persona física a través del conjunto de medios que puedan ser razonablemente utilizados por el responsable del tratamiento de datos o por terceros. Así, entendiendo que el estado anónimo ha de garantizarse de manera tan permanentemente como el borrado, la anonimización implicará una desidentificación sólida e irreversible.

[54] COHEN, I.; AMARASINGAHM, R.; SHAH, A.; XIE, B. y LO, B.: "The legal and ethical concerns that arise from using complex predictive analytics in health care", *Health Affairs*, vol. 33, núm. 7, 2014, pág. 1139 y ss.

La anonimización consistía tradicionalmente en un proceso de dos fases principales. La primera despojaba a los conjuntos de datos de todos los rasgos identificadores personales (nombre, dirección, número de Seguridad Social,…). La segunda modificaba o eliminaba otras categorías de datos que podían actuar como identificadores en un contexto concreto. En este punto existe una dicotomía entre los datos de carácter personal, sujetos a las normas de protección de datos, y los datos ya anonimizados, habida cuenta de que una vez esto ha ocurrido "y los individuos ya no son identificables, la normativa de protección de datos no se aplica"[55].

Así, en un principio, la anonimización aseguraba la privacidad. Sin embargo, las fisuras que presenta esta técnica han alertado a la comunidad científica y a los juristas de las amenazas que sufre la información privada de los sujetos que han cedido sus datos a determinadas plataformas tecnológicas, pues, no en vano, de la mano del big data la creciente cantidad de información almacenada de millones de usuarios de internet facilita la reidentificación de las personas a las que pertenecen los datos en cuestión, aun cuando estos han sido anonimizados[56], lo que evidencia el peligro de que se produzcan accesos indeseados y no consentidos, así como usos diferentes, incluso fraudulentos, de aquellos para los cuales tales datos se han cedido o almacenado, con la consiguiente pérdida de la intimidad del afectado.

Por ello, este proceso de anonimización es un proceso crítico para las autoridades de protección de datos y las agencias creadas en la materia, en tanto en cuanto existen evidencias suficientes "que demuestran que los avances tecnológicos y la posibilidad de combinar diferentes

[55] GIL GONZÁLEZ, E.: *Big data, privacidad y protección de datos*, Madrid (Agencia Española de Protección de Datos/Boletín Oficial del Estado), 2016, pág. 83, quien señala cómo "de este modo, el resultado anulaba lo mejor de ambos lados: los datos continuaban siendo útiles, y podían ser analizados, compartidos o puestos a disposición del público al tiempo que los individuos no podían ser identificados, y por lo tanto se protegía su privacidad".

[56] Sobre esta cuestión, analizando los riesgos y el control de los datos MAYER-SCHÖENBERG, V. y CUKIER, K.: *Big Data. A revolution that will transform how we live, work and think*, cit., pág. 150 y ss.

datos puede conllevar la identificación de un consumidor, ordenador o dispositivo, incluso si estos datos por sí mismo no constituyen datos de identificación personal. Es más, no solo es posible reidentificar datos que no son identificadores personales a través de medios diversos, sino que las empresas tienen fuertes incentivos para hacerlo"[57].

La densidad del aspecto de protección de datos y ciberseguridad en la medicina digital impide que se pueda desarrollar en este trabajo un análisis en profundidad de la cuestión. Sin embargo, conviene hacer una breve reflexión respecto de un eventual acceso por parte de terceros especialmente interesados en estos datos del paciente, que, en un primer momento anonimizados, permitan ser desanonimizados, pudiendo reconectarlos con el sujeto al que pertenecen, y es que tal y como algún autor ha alertado es un hecho que "lo que el médico sabe también lo pueden saber –o intentar saber– terceros"[58].

A pesar de que el avance de las nuevas tecnologías permitiría, siempre y cuando fueran adoptadas las medidas precisas para garantizar la integridad y confidencialidad de los datos, la comunicación de los resultados a través del correo electrónico o de una página de internet facilitando al trabajador su acceso a través de una clave, el sobre cerrado y sellado por el servicio de prevención con la referencia expresa de confidencial parece el mejor sistema para garantizar dicha confidencialidad, siendo los mismos remitidos directamente al interesado y no a la empresa, circunstancia que generaría el riesgo de la filtración o el conocimiento de los datos por terceros no autorizados o no deseados.

---

[57] FEDERAL TRADE COMMISION: *Protecting consumer privacy in an era of rapid change. Recommendations for bussinesses and policymakers*, Washington (FEDERAL TRADE COMMISION), 2012, pág. 20.

[58] MORLA GONZÁLEZ, M.: "Medicamentos digitales. La autonomía del paciente a debate", *Revista Internacional de Éticas aplicadas*, núm. 29, 2019, pág. 129, pág. 129.

2.3. El tratamiento de datos y el acceso a los ficheros y documentación

Los avances tecnológicos y las labores de gestión y administración han obligado a que personal no sanitario pueda acceder y acceda a documentación clínica, ya sea para desarrollar sus tareas administrativas, ya para el mantenimiento de bases de datos en las que se alberga información de carácter médico. Ello ha dado lugar al denominado secreto médico derivado, configurado como un deber de sigilo a respetar por el personal no sanitario, que surge motivado por la complejidad administrativa y técnica existente en la actualidad en relación con la Medicina. Dicho personal posee la capacidad de acceso a información confidencial, quedando así obligado al secreto correspondiente, y, desde luego, siempre justificado dicho acceso por el ejercicio de sus legítimas funciones.

En este sentido, la labor del personal informático se debe centrar en asegurar una garantía sobre la correcta utilización de la información clínica. El informático tiene el deber de no acceder a datos que no requieren su conocimiento, puesto que "pese a tener la posibilidad de acceso en la medida que controla los propios sistemas informáticos no debe de hacer uso de esta prerrogativa"[59].

Las compañías informáticas y tecnológicas han venido desarrollado y desarrollan múltiples, variadas y diferentes aplicaciones y dispositivos en el ámbito de la salud con igualmente distintos usos y fines, lo que les obliga a "procurar que su servicio sea efectivo y óptimo. Para ello, el acceso a información sensible del paciente, usuario de sus servicios, se convierte entonces en un factor esencial para fines tales

[59] "La labor del personal informático se enmarca dentro del desarrollo de la actividad dirigida a garantizar que los datos contenidos en los sistemas de tratamiento de la información clínica de los pacientes sean utilizados de forma correcta. En ocasiones pueden producirse pérdidas de información accidentales, debiendo el informático proceder a la recuperación de dicha información, es en este momento, donde pueden darse casos en que tenga conocimiento de datos sobre la salud de determinadas personas". DE LORENZO Y MONTERO, RICARDO: "El secreto médico derivado", *Redacción Médica*, Núm. 1848, 2013, https://www.delorenzoabogados.es/blog/?p=52&idioma=eng.

como identificar eventuales fallos en sus dispositivos, desarrollar mejoras y llevar a cabo un control de calidad sobre sus servicios"[60]. En el eventual caso de que las empresas desarrolladoras de aplicaciones y dispositivos tuvieran acceso a datos de salud del paciente "se verán entonces sometidas a los deberes de confidencialidad que el secreto médico derivado descarga sobre ellas en aras de garantizar esa protección a la intimidad… cuya configuración… ha ido evolucionando en paralelo al avance de las nuevas tecnologías"[61].

Además, resulta preciso tener en cuenta, en términos de seguridad, que la tecnología no constituye un medio infalible, es más, la realidad nos muestra continuamente que puede fallar y lo hace, de forma tal que depositar elevados índices de confianza y dependencia en los productos médico-tecnológicos utilizados por los profesionales, conlleva riesgos y una serie de dilemas éticos y jurídicos de no poca importancia[62], y no solo en relación a la eventual responsabilidad en la que incurriría el médico ante el fallo del dispositivo que esté utilizando para tratar a su paciente[63], sino también en relación al acceso por parte de terceros a sus datos de salud, que tienen la categoría de especialmente protegidos (art. 9.1 reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016) o ante eventuales amenazas de ciberseguridad[64].

La Comisión Europea ha destacado los beneficios sociales que proporcionan estas aplicaciones, pero al mismo tiempo ha sido consciente de sus particularidades y de la tipología de datos que tratan y, en

---

[60] COHEN, I.; AMARASINGAHM, R.; SHAH, A.; XIE, B. y LO, B.: "The legal and ethical concerns that arise from using complex predictive analytics in health care", cit., pág. 1139 y ss.

[61] MORLA GONZÁLEZ, M.: "Medicamentos digitales. La autonomía del paciente a debate", cit., pág. 128.

[62] GIOTA, K. y KLEFTARAS, G.: "Mental health apps: innovations, risks and ethical considerations", *E-Health Telecommunications Systems and Networks*, núm. 3, 2014, págs. 19-23.

[63] COHEN, I.; AMARASINGAHM, R.; SHAH, A.; XIE, B. y LO, B.: "The legal and ethical concerns that arise from using complex predictive analytics in health care", *Health Affairs*, vol. 33, núm. 7, 2014, pág. 1139 y ss.

[64] MORLA GONZÁLEZ, M.: "Medicamentos digitales. La autonomía del paciente a debate", cit., pág. 128.

consecuencia, de la protección que debe otorgárseles, por lo que, sobre estas bases, ha estado elaborando un código de conducta europeo sobre privacidad en aplicaciones móviles de salud, en aras de proteger el debido cumplimiento de la protección de datos y de promover las buenas prácticas tanto de desarrolladores de aplicaciones como de los usuarios de Apps de salud.

Los principios en los que se basa el código de conducta no son más que un reflejo de aquellos incluidos explícitamente en el Reglamento 2016/679 de protección de datos dirigido especialmente a los desarrolladores de aplicaciones, habida cuenta de que son estos quienes en el diseño de las mismas deben garantizar el pleno respeto a los principios de privacidad desde el primer momento, pues la constante necesidad de mejora y mantenimiento de los dispositivos médico-tecnológicos necesita de al menos la información anonimizada como parte de la investigación en el ámbito de la medicina digital, y que para una mejora más cualificada de los dispositivos, sea posible el acceso a una información identificable[65].

En fin, la realidad es que quien posee la información será quien pueda suministrarla y, en tal sentido, el personal sanitario deberá integrar y delimitar el contenido de las conclusiones de los reconocimientos en cada caso concreto en función de los límites y condicionantes expuestos, de forma que será su conciencia en los términos de la deontología de su disciplina profesional la que deberá asegurar que los informes finales aparezcan delimitados en los estrictos términos impuestos legalmente.

La Recomendación 171 de la OIT, sobre los servicios de salud en el trabajo, constituye un buen ejemplo en cuanto a la fijación de este elemento interpretativo a utilizar en las conclusiones, habida cuenta de que en su artículo 16 destaca como "al término de un examen médico prescrito para determinar la aptitud de un trabajador para un puesto de

[65] Sobre la materia, KLUGMAN, C.; DUNN, L.; SCHWARTZ, J. y COHEN, I.: "The ethics of smart pills and sefl-acting devices: autonomy, truth-telling, and trust at the dawn of digital medicine", *American Journal of Bioethics*, vol. 18, núm. 9, 2017, pág. 1 y ss.

trabajo que entraña exposición a un riesgo determinado, el médico que lo haya realizado debería comunicar sus conclusiones por escrito al trabajador y al empleador. Por otra parte, esta comunicación no debería contener indicación alguna de índole médica; según los casos, podría indicar que el trabajador es apto para el puesto de trabajo previsto o bien especificar los tipos de trabajo y las condiciones de trabajo que le estén contraindicados, temporal o permanentemente, desde el punto de vista médico".

Por otra parte, y del mismo modo, el personal administrativo de un centro sanitario, puede, siempre en el ejercicio de sus funciones inherentes a su cargo, acceder a otro tipo de información confidencial relacionada con los pacientes, como puede ser la facturación por los servicios prestados, la gestión del sistema de citas para especialistas, etc, datos de los cuales podría llegar a deducirse con un mínimo conocimiento el tipo de enfermedad padecida, o si se está siguiendo un tratamiento en virtud del número de visitas o revisiones realizadas. Debe destacarse claramente que también en tales supuestos se mantiene el deber de secreto frente a tales informaciones y datos para el personal no sanitario, circunstancia evidentemente igual protegida por la regulación en materia de protección de datos[66].

[66] DE LORENZO Y MONTERO, RICARDO: "El secreto médico derivado", *Redacción Médica*, Núm. 1848, 2013, https://www.delorenzoabogados.es/blog/?p=52&idioma=eng.

BIBLIOGRAFÍA

AA.VV.: *Industria conectada* 4.0. *La transformación digital de la industria española*, Madrid (Ministerio de Industria), 2015.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS: *La protección de datos en las relaciones laborales*, Madrid (Agencia Española de Protección de Datos), 2021.

ALEMÁN PÁEZ, F.: "El derecho de desconexión digital. Una aproximación conceptual, crítica y contextualizadora al hilo de la Loi Travail n.º 2016-1088", *Trabajo y Derecho. Nueva revista de actualidad y relaciones laborales*, núm. 30, 2017.

ÁLVAREZ CIVANTOS, O. J.: *Normas para la implantación de una eficaz protección de datos de carácter personal en empresas y entidades*, Granada (Comares), 2002.

ÁLVAREZ CUESTA, H.: *El futuro del trabajo vs. el trabajo del futuro*, A Coruña (Colex), 2017.

ARIAS DOMÍNGUEZ, A. y RUBIO SÁNCHEZ, F.: *El derecho de los trabajadores a su intimidad*, Pamplona (Thomson/Aranzadi), 2006.

AYERRA LAZCANO, J. M.ª.: "Regulación general de la historia clínica", *Derecho y Salud*, Vol. 11, 2003.

BORRAJO DACRUZ, E.: "El impacto de tecnologías y medios de información en el Derecho del Trabajo", en AA.VV.: *Implicaciones socio-jurídicas de las tecnologías de la información: encuentros 1980-1990: los juristas ante la revolución informática*, Madrid (CITEMA), 1991.

COHEN, I.; AMARASINGAHM, R.; SHAH, A.; XIE, B. y LO, B.: "The legal and ethical concerns that arise from using complex predictive analytics in health care", *Health Affairs*, vol. 33, núm. 7, 2014.

CRUZ VILLALÓN, J. "El impacto de la digitalización sobre los derechos fundamentales laborales", en AA.VV. (RODRÍGUEZ-PIÑERO ROYO, M. y TODOLÍ SIGNES, A., Dirs.): *Vigilancia y control en el Derecho del Trabajo digital*, Pamplona (Aranzadi), 2020.

DE LORENZO Y MONTERO, RICARDO: "El secreto médico derivado", *Redacción Médica*, Núm. 1848, 2013, https://www.delorenzoabogados.es/blog/?p=52&idioma=eng.

DE MIGUEL SÁNCHEZ, N.: "Investigación y protección de datos de carácter personal: una aproximación a la Ley 14/2007, de 3 de julio, de investigación biomédica", *Revista Española de Protección de Datos*, núm. 1, 2006.

DE MIGUEL BERIAIN, I. y MORLA GONZÁLEZ, M.: "Digital pills for mental diseases: an ethical and social analysis of the issues behind the concept", *Journal of Law and the Biosciences*, agosto 2020.

DÍEZ-PICAZO, L.: *Experiencias jurídicas y teoría del Derecho*, 3.ª ed., Barcelona (Ariel), 1993.

FEDERAL TRADE COMMISION: *Protecting consumer privacy in an era of rapid change. Recommendations for bussinesses and policymakers*, Washington (FEDERAL TRADE COMMISION), 2012.

FERNÁNDEZ COSTALES, J.: "La aplicación y la incidencia de la informática en el ámbito del Derecho Civil", *Revista General de Legislación y Jurisprudencia*, núm.4, 1985.

FERNÁNDEZ DOMÍNGUEZ, J. J. y RODRÍGUEZ ESCANCIANO, S.: *Utilización y control de datos laborales automatizados*, Madrid (Agencia de Protección de Datos), 1997.

FERNÁNDEZ LÓPEZ, J. M.: "El derecho fundamental a la protección de datos personales. Obligaciones que derivan para el personal sanitario", *Derecho y Salud*, Número extraordinario del XI Congreso de Derecho y Salud, 2003.

FERNÁNDEZ VILLAZÓN, L. A.: "Tratamiento automatizado de datos personales en los procesos de selección de trabajadores", *Relaciones Laborales*, T. I, 1994.

FERNÁNDEZ-COSTALES MUÑIZ, J.: *La vigilancia de la salud de los trabajadores*, León (Junta de Castilla y León/Eolas), 2009.

– *Prevención de Riesgos Laborales y empresa: obligaciones y responsabilidades*, Pamplona (Aranzadi), 2019.

GARCÍA MURCIA, J. y RODRÍGUEZ CARDO, I. A.: "La protección de datos personales en el ámbito del trabajo: una aproximación desde el nuevo marco normativo", *Nueva Revista Española de Derecho del Trabajo*, núm. 216, 2019.

GIL GONZÁLEZ, E.: *Big data, privacidad y protección de datos*, Madrid (Agencia Española de Protección de Datos/Boletín Oficial del Estado), 2016.

GIOTA, K. y KLEFTARAS, G.: "Mental health apps: innovations, risks and ethical considerations", *E-Health Telecommunications Systems and Networks*, núm. 3, 2014.

GOÑI SEIN, J. L.: "Vulneración de derechos fundamentales en el trabajo mediante instrumentos informáticos, de comunicación y archivo de datos", en AA.VV. (ALARCÓN CARACUEL, M. R. y ESTEBAN LEGARRETA, R., Coords.): *Nuevas tecnologías de la información y la comunicación y Derecho del Trabajo*, Albacete (Bomarzo), 2004.

GOÑI SEIN, J. L.: "Flexibilidad y revisión del ámbito del Derecho del Trabajo", en AA.VV. (RIVERO LAMAS, J., Coord.): *La flexibilidad laboral en España*, Zaragoza (Instituto de Relaciones Laborales), 1993.

HEREDERO HIGUERAS, M.: "La protección de datos de salud informatizados en la Ley Orgánica 5/1992, de 29 de octubre", *Derecho y Salud*, Vol. 2, 1994.

KLUGMAN, C.; DUNN, L.; SCHWARTZ, J. y COHEN, I.: "The ethics of smart pills and sefl-acting devices: autonomy, truth-telling, and trust at the dawn of digital medicine", *American Journal of Bioethics*, vol. 18, núm. 9, 2017.

LUCAS MURILLO DE LA CUEVA, P.: "El tratamiento jurídico de los documentos y registros sanitarios informatizados y no informatizados", en AA.VV.: *Información y documentación clínica (Actas del Seminario Conjunto sobre Información y Documentación Clínica celebrado en Madrid los días 22 y 23 de septiembre de 1997), Vol. II*, Madrid (CGPJ/MSC), 1997.

LUJÁN ALCARAZ, J.: "Uso y control en la empresa de los medios informáticos de comunicación", *Aranzadi Social*, T. II, 2005.

MARTÍNEZ FONS, D.: *La vigilancia de la salud de los trabajadores en la Ley de Prevención de Riesgos Laborales*, Valencia (Tirant lo Blanch), 2002.

MAYER-SCHÖENBERG, V. y CUKIER, K.: *Big Data. A revolution that will transform how we live, work and think*, Boston/Nueva York (Eamon Dolan Book/Mariner Books/Houghton Mifflin Harcourt), 2013, (en version traducida: *Big Data. La revolución de los datos masivos*, Madrid (Turner), 2013).

MORLA GONZÁLEZ, M.: "Medicamentos digitales. La autonomía del paciente a debate", *Revista Internacional de Éticas aplicadas*, núm. 29, 2019.

MURILLO DE LA CUEVA, P. L.: "Informática y protección de datos personales (Estudio sobre la Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal)", *Cuadernos y Debates*, núm. 43, 1993.

PEDROSA ALQUÉZAR, S. I.: *La vigilancia de la salud en el ámbito laboral. Regulación legal, límites y cuestiones problemáticas*, Madrid (CES), 2005.

– "Vigilancia de la salud laboral y protección de datos", *Revista del Ministerio de Empleo y Seguridad Social*, núm. 137, 2018.

PRADAS MONTILLA, R.: "Empresas y protección de datos de carácter personal", *Actualidad Laboral*, T. I, 2003.

PRECIADO DOMÈNECH, C. H.: *El Derecho a la Protección de Datos en el contrato de trabajo. Adaptado al nuevo Reglamento 679/2016, de 27 de abril*, Pamplona, (Aranzadi), 2017, pág. 29 y ss. o BLÁZQUEZ AGUDO, E. M.ª.: *Aplicación práctica de la protección de datos en las relaciones laborales*, Madrid (CISS), 2018.

RODRÍGUEZ ESCANCIANO, S.: "La intimidad del trabajador en el uso de diagnósticos médicos informatizados", *Revista Española de Derecho del Trabajo*, núm. 101, 2000.

– "La potencialidad lesiva de la informática sobre los derechos de los trabajadores", en *Revista Española de Protección de Datos*, núm. 2, 2007.

– "El tratamiento de datos sensibles vinculados a la Prevención de Riesgos Laborales", *Revista Jurídica de la Universidad de León*, núm. 5, 2018.

SÁNCHEZ CARO, JAVIER Y ABELLÁN-GARCÍA SÁNCHEZ, FERNANDO: *Derechos y deberes de los pacientes (Ley 41/2002, de 14 de noviembre: consentimiento informado, historia clínica, intimidad e instrucciones previas)*, Granada (Comares), 2003.

SÁNCHEZ CUBEL, M. D.: *Todo sobre la nueva Ley de Prevención de Riesgos Laborales*, Barcelona (Praxis), 1996.

SÁNCHEZ-CARO, J. y ABELLÁN, F.: *Telemedicina y protección de datos sanitarios. Aspectos legales y éticos*, Granada (Comares), 2002.

TARODO SORIA, S.: *Libertad de conciencia y derechos del usuario de los servicios sanitarios*, Bilbao (Universidad del País Vasco), 2005.

TASCÓN LÓPEZ, R.: "Sobre la ejecución procesal de las obligaciones derivadas de la legislación sobre protección de datos personales; en este caso, eliminar los datos relativos a los diagnósticos médicos de los trabajadores de un archivo empresarial sobre absentismo con baja médica (Comentario a la STCo 153/2004, de 20 de septiembre)", *Revista Española de Protección de Datos*, núm. 2, 2007.

TOLOSA TRIBIÑO, C.: "El secreto profesional de los médicos en la Ley de Prevención de Riesgos Laborales", *Relaciones Laborales*, núm. 20, 1997.

Avaliação de conhecimentos a distância no ensino superior português: processos de monitorização e sua conformidade com o RGPD[1]

Saul A. N. Ferreira Leite[2]

Resumo: Os meios digitais eram já uma presença constante no quotidiano dos estudantes quando, em abril de 2020, a pandemia por COVID-19 lhe conferiu especial importância. As instituições de ensino superior socorreram-se dessa via para prosseguir com as atividades letivas em plena pandemia, abrindo portas à utilização de soluções para monitorização da avaliação a distância, que algumas acabariam efetivamente por adotar.

O presente estudo propõe-se a seguir uma proposta de classificação dessas soluções identificando, em cada caso, as suas funcionalidades, os dados pessoais tratados, os fundamentos de licitude admissíveis e a necessidade de realização de uma avaliação de impacto sobre a proteção dos dados (AIPD).

Palavras-chave: *RGPD, AIPD, monitorização eletrónica, avaliação a distância.*

Abstract: Digital communication used to be a constant presence in students' daily lives when, in April 2020, the COVID-19 pandemic gave it a particular important role. Higher education institutions started using

[1] **Declaração de princípio:** A presente reflexão resulta do trabalho desenvolvido em sede académica, sob orientação dos Professores Doutores Nuno David e Francisco Pereira Coutinho, não vinculando a posição institucional da CNPD – embora muito se agradeça todo o apoio e ensinamentos transmitidos pela Professora Doutora Filipa Urbano Calvão.

[2] Mestre em Engenharia de Telecomunicações e Informática pelo Iscte – Instituto Universitário de Lisboa. Consultor da Comissão Nacional de Proteção de Dados.

this means to continue the learning activities, opening the door to distance assessment monitoring solutions, which some have started to adopt.

This study intends to follow an already existent e-proctoring tools classification to identify, case by case, the functionalities, the processed personal data, the admissible lawfulness of processing and the need to carry out a data protection impact assessment (DPIA).

Keywords: *GDPR, DPIA, e-proctoring, remote assessment.*

1. Introdução

As aplicações informáticas que se propõem a monitorizar um processo de avaliação de conhecimentos a distância captaram, nos últimos anos e de forma tendencialmente global, a atenção dos estabelecimentos de ensino em geral e de ensino superior em particular.

Para tanto, muito contribuíram as restrições à circulação de pessoas e a suspensão das atividades de ensino e de avaliação presenciais, impostas pelos Estados um pouco por todo o mundo, aspirando conter a propagação da pandemia por COVID-19. Nesse contexto, as referidas medidas foram primeiramente aplicadas em Portugal no período decorrido entre 14 de março e 15 de maio de 2020[3], e mais tarde por declaração do estado de emergência e suas sucessivas renovações, que vigorou entre 9 de novembro de 2020 e 30 de abril de 2021[4]. As restrições acabariam ainda por se fazer sentir com a declaração do estado de calamidade[5] que vigorou entre 1 e 30 de maio de 2021.

[3] Início e fim determinados pela publicação do Decreto-Lei n.º 10-A/2020, de 13 de março, e do Decreto-Lei n.º 20-H/2020, de 14 de maio, respetivamente.

[4] Através da publicação do Decreto do Presidente da República n.º 51-U/2020, de 6 de novembro, e sucessivas renovações, cf. informação disponível em: <*https://www.parlamento.pt/Paginas/estado-emergencia.aspx*>.

[5] O estado de calamidade foi declarado através da publicação da Resolução do Conselho de Ministros n.º 45-C/2021, de 30 de abril, alterada pelas Resoluções do Conselho de Ministros n.ºs 46-C/2021, de 6 de maio, e 52-A/2021, de 11 de maio, tendo sido prolongado até 30 de maio, por publicação da Resolução do Conselho de Ministros n.º 59-B/2021, de 14 de maio.

O direito ao ensino – constitucionalmente previsto[6] – levou a que as instituições de ensino superior optassem pelos meios que garantissem a continuidade das atividades letivas, necessariamente a distância, equacionando alternativas ao tradicional regime de avaliação.

A colocação em prática de um regime de avaliação a distância sempre suscitaria questões do foro e, ainda, relativas à sua eficácia, mas também, relativamente ao processo de monitorização dos alunos, uma cuidada ponderação sobre o risco de ingerência nos seus direitos e liberdades fundamentais dos alunos, devido à sua monitorização

A este propósito, em abril de 2020, a Fundação para a Ciência e a Tecnologia (FCT), através da Unidade de Computação Científica (FCCN), iniciou junto da comunidade académica um projeto-piloto de sistemas de avaliação a distância – Piloto SAR[7] – para avaliar a experiência de utilização em ambiente de testes (provas de avaliação fictícias) relativamente a quatro soluções comerciais de monitorização a distância[8]. O projeto terminaria em julho do mesmo ano, concluindo[9] essencialmente que as soluções comerciais em geral, e particularmente as que foram testadas, não apresentavam àquela data o nível de qualidade e maturidade suficientes para a sua utilização em larga escala, nem respondiam às especificidades do sistema de ensino superior português. Num *webinar*[10] realizado a 22 de maio de 2020, organizado em parceria pela *MetaRed Portugal*[11] e a FCT, no qual intervieram, entre outros, os responsáveis universitários pela gestão das aplicações do Piloto SAR, destacou-se uma clara preocupação com o nível de intrusão de algumas das aplicações testadas, bem como a necessidade de conduzir uma

[6] Art.º 74.º da Constituição da República Portuguesa.

[7] Disponível em <*https://www.fccn.pt/noticias/fct-projeta-a-utilizacao-de-sistemas-de-avaliacao-remota-no-ensino-superior*>.

[8] Foram disponibilizadas as soluções '*ProctorExam', 'TestWe', 'Exam.net'* e '*Respondus'*, respetivamente geridas pela Universidade de Lisboa, Instituto Politécnico de Bragança, Universidade de Trás-os-Montes e Alto Douro e Universidade de Aveiro.

[9] RIBEIRO, Rui, CABRAL, Pedro e GOMES, João, "Relatório Final – Sistemas de Avaliação Remota", FCT, 2020.

[10] Disponível em: <*https://www.youtube.com/watch?v=FS4Ci_BwBUA*>.

[11] Associação de instituições públicas e privadas, de ensino superior.

adequada análise dos respetivos tratamentos de dados à luz do Regulamento Geral sobre a Proteção de Dados (RGPD).

Se o ótimo é inimigo do bom, a pressa é inimiga da perfeição, nos diria, mais não fosse, a sabedoria popular. Não obstante, no ano letivo seguinte, em que o ensino superior foi sobretudo caracterizado por um regime misto no qual as aulas decorriam simultaneamente em modo presencial[12] e a distância, algumas instituições de ensino superior portuguesas determinaram[13] a adoção de um regime de avaliação de conhecimentos a distância, em alguns casos obrigatório.

Não tardaria, contudo, à semelhança do que aconteceu noutros países[14], que os visados se insurgissem[15] contra a realização das provas através de específicos *softwares,* por entenderem estar em causa a violação do RGPD, da Lei n.º 58/2019, de 8 de agosto, e das orientações

---

[12] Por vigorarem exceções ao dever geral de recolhimento domiciliário e à proibição de circulação na via pública em concelhos de risco elevado, sempre que em causa estivessem deslocações às instituições de ensino superior.

[13] Por via da publicação do Despacho Reitoral n.º 8/2021, 21 de janeiro, (disponível em: <*https://gdoc.uevora.pt/695399*>), a Universidade de Évora determinou a suspensão imediata das atividades de avaliação presenciais e a adoção do modelo online, sempre que a tipologia das unidades curriculares/curso o permitisse. A decisão ocorreu após publicação do Comunicado do Conselho de Ministros de 21 de janeiro de 2021, que determinou a suspensão das atividades letivas e não letivas, a partir de 22 de janeiro e pelo período de 15 dias.

[O] Despacho n.º 21/2021, de 17 de março, da Diretora da Faculdade de Direito da Universidade de Lisboa, determinou que os exames escritos da época de recurso do 1.º semestre da licenciatura e do Mestrado em Direito e Prática Jurídica seriam realizados com recurso a meios de avaliação a distância e, se possível, com o apoio de um programa de controlo de realização das provas. Após contestação dos alunos, foi o mesmo posteriormente alterado pelo Despacho n.º 24/2021, de 25 de março.

[14] Em vários Estados dos Estados Unidos da América (EUA) ("Students are pushing back against proctoring surveillance apps", EFF, disponível em: <*https://www.eff.org/deeplinks/2020/09/students-are-pushing-back-against-proctoring-surveillance-apps*>), em França ("À l'université Paris 8, la télé surveillance des examens est jugée trop intrusive", Le Figaro, disponível em: <*https://etudiant.lefigaro.fr/article/a-l-universite-paris-8-la-tele-surveillance-des-examens-est-jugee-trop-intrusive_a0b940b4-811d-11ed-b9f4-d826a205a5b5*>), entre outros.

[15] (Em linha) Disponível em: <*https://www.jn.pt/nacional/software-usado-na-avaliacao--guarda-sons-e-imagens-de-universitarios-do-minho–13455740.html*>; e <*https://www.publico.pt/2021/03/25/p3/noticia/faculdade-direito-queria-gravar-movimento-som-exames-estudantes-contestaram-provas-voltam-presenciais-1955939*>.

da Comissão Nacional de proteção de Dados (CNPD)[16] relativas ao ensino a distância.

Nesta senda, viria a CNPD deliberar[17] sobre a utilização das aplicações *'Respondus'* (*'Lockdown Browser'* e *'Respondus Monitor'*), por uma universidade portuguesa, entendendo que no concreto caso o tratamento de dados era suscetível de violar os princípios da licitude, finalidade, da minimização dos dados e da proporcionalidade – art.º 5.º, n.º 1, alíneas *a), b)* e *c)*, do RGPD – e, ainda, que a empresa *Respondus, Inc*, recolhia amostras das gravações de áudio e vídeo para os seus próprios fins, sem que fosse obtido o consentimento dos alunos (p. 6). Concluiu, ainda, que os dados dos estudantes eram armazenados nos EUA, sem a adoção de medidas suplementares que permitissem garantir um nível de proteção essencialmente equivalente ao assegurado na União Europeia (p. 6v.).

Um pouco por toda a Europa verificaram-se episódios semelhantes, embora com desfechos variados.

Em setembro de 2021, também aquela Autoridade para a proteção de dados pessoais italiana, *Garante per la Protezione dei Dati Personali* (GPDP), aplicou à Universidade *Luigi Bocconi*, em Milão, uma coima no valor de 200.000 euros por entender que não estavam reunidas as condições de licitude para o tratamento de dados, nomeadamente de categorias especiais de dados, durante a utilização de um sistema para monitorização dos alunos. Na mesma deliberação[18] assinalou, ainda, a falta de informação aos titulares dos dados, a não observância da proteção dos dados desde a conceção e por defeito, a ausência de medidas apropriadas à mitigação

---

[16] Designadamente, das 'Orientações sobre a utilização de tecnologias de suporte ao ensino à distância' e 'Orientações sobre avaliação à distância nos estabelecimentos de ensino superior' (respetivamente disponíveis em: <*https://www.cnpd.pt/media/1encswse/orientacoes_tecnologias_de_suporte_ao_ensino_a_distancia.pdf*> e <*https://www.cnpd.pt/media/0mwfxdcp/orientacoes_avaliacao_distancia_ensino_superior.pdf*>).

[17] "Deliberação/2021/662", CNPD, disponível em: <*https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121887*>.

[18] "Ordinanza ingiunzione nei confronti di Università Commerciale 'Luigi Bocconi' di Milano – 16 settembre 2021", GPDP, disponível em: <*https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9703988*>.

dos riscos e a violação do princípio geral das transferências (art.º 44.º, em consonância com os Considerandos n.º 101 e 102, do RGPD).

Num outro caso[19], na sequência das averiguações por si iniciadas, em 30 de abril de 2020, a Autoridade de Proteção de Dados dinamarquesa (*Datatilsynet*) decidiu a favor da Universidade de Tecnologias de Informação de Copenhaga (ITU), que se socorreu do *software ProctorExam* para monitorizar os alunos de uma certa unidade curricular[20], através de um processo de avaliação a distância. Entendeu a Autoridade que foi realizada uma avaliação correta e documentada da necessidade de recurso àquela solução, que gravou o áudio e vídeo de 330 examinandos, bem como o conteúdo dos seus monitores, revelando-se a menos intrusiva face às circunstâncias. Considerou, ainda, que os alunos foram devidamente informados sobre o tratamento de dados – que considerou lícito, nos termos da alínea *e)* do n.º 1 do art.º 6 do RGPD – e que a Universidade adotou as medidas de segurança técnicas e organizativas adequadas, no cumprimento do RGPD e da lei nacional de proteção de dados. Não se pronunciou, contudo, quanto ao facto de a Universidade alegadamente recolher alegadamente o consentimento dos alunos para aquele tratamento de dados, mas sem o qual não poderiam realizar o exame ou, ainda, sobre as transferências internacionais de dados efetuadas efetuadas no âmbito da utilização daquela solução comercial.

Atendendo à retrospetiva traçada, o presente estudo propõe-se a seguir um modelo para a categorização das soluções de avaliação a distância, por forma a melhor enquadrar as respetivas características e funcionalidade de cada uma s. De seguida, irão analisar-se os fundamentos de licitude elegíveis em cada tratamento de dados, concluindo-se quanto à necessidade de realização da avaliação de impacto sobre a proteção dos dados.

---

[19] "Universitets brug af tilsynsprogram ved online eksamen", Datatilsynet, disponível em: <*https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/jan/universitets-brug-af-tilsynsprogram-ved-online-eksamen*>.

[20] *Algoritmos e Estruturas de Dados*, por se tratar de uma prova em que as respostas corretas seriam idênticas, sem necessidade de desenvolvimento ou demonstração de resultados, exigindo-se que os alunos não comunicassem entre si.

2. Considerações prévias

O regime jurídico dos graus e diplomas do ensino superior, aprovado pelo Decreto-Lei n.º 74/2006, de 24 de março[21], prevê na sua redação atual, através das alíneas *e)* dos art.ºs 14.º e 26.º, que os regimes de avaliação de conhecimentos, respetivamente para o ciclo de estudos conducente ao grau de licenciado e de mestre, são aprovados pelo órgão legal e estatutariamente competente de cada estabelecimento de ensino superior.

No que concerne à modalidade de ensino superior a distância, o Decreto-Lei n.º 133/2019, de 3 de setembro, estabelece um quadro de princípios e regras de acreditação, organização e funcionamento das instituições de ensino superior que atuam sob esse modelo de ensino, delegando nas mesmas a definição das metodologias do processo de avaliação, que pode ser presencial, ou através de plataformas tecnológicas que assegurem a sua fiabilidade (cf. n.º 1 do art.º 14.º).

As instituições de ensino superior encontram-se, portanto, legitimadas para que possam optar, se assim o entenderem, por um regime de avaliação de conhecimentos a distância, desde que observem o cumprimento das respetivas normas e regulamentos de avaliação, sem prejuízo dos atos de supervisão e de (re)acreditação dos seus ciclos de estudos, designadamente pela Agência de Avaliação e Acreditação do Ensino Superior (A3ES)[22].

3. Soluções de monitorização: categorias e funcionalidades

As ferramentas que se propõem à monitorização da avaliação a distância fazem uso dos recursos do dispositivo do avaliado, entre os quais

[21] Alterado pelos Decretos-Leis n.ºs 107/2008, de 25 de junho, 230/2009, de 14 de setembro, 115/2013, de 7 de agosto, 63/2016, de 13 de setembro, 65/2018, de 16 de agosto e 27/2021, de 16 de abril.

[22] Criada pelo Decreto-Lei n.º 369/2007, de 5 de novembro.

se incluem a *webcam*, o microfone e a ligação à internet, podendo ser essencialmente enquadradas nas seguintes categorias[23], sem prejuízo da possibilidade da sua combinação entre si:

I. Monitorização em tempo real, com recurso a um ou mais avaliadores remotamente ligados, nos quais são delegadas as tarefas de verificação da identidade dos alunos e sua monitorização durante o período de realização da prova;

II. Monitorização com recurso à gravação de vídeo e, opcionalmente, também de áudio, através da qual se gravam os alunos durante o período de realização da prova. As gravações são posteriormente analisadas, geralmente por docentes, ou por terceiros contratados para o efeito;

III. Monitorização automática, na qual se procede à gravação dos avaliados durante a prova de avaliação. As gravações são automaticamente processadas por um sistema de análise de áudio e vídeo, para deteção e classificação de comportamentos suscetíveis de constituírem fraude académica.

As principais funcionalidades[24] disponibilizadas pelas soluções comerciais de monitorização são:

• Integração com sistemas de apoio ao ensino LMS (*learning management systems*), de onde se destacam as plataformas *Moodle*, *Blackboard* e *Canvas*. As provas de avaliação são criadas diretamente na plataforma de ensino, bem como a configuração da monitorização pretendida (*e.g.* gravar apenas vídeo, gravar áudio e vídeo, definir avisos prévios ao início da gravação, solicitar um documento de identificação);

---

[23] O'REILLY, Gordon e CREAGH, John, "A categorization of Online Proctoring", *Proceedings of Global Learn-Global Conference on Learning and Technology*, 2016, pp. 542-552.

[24] ARNÒ, Simone, GALASSI, Alessandra, TOMMASI, Marco e SAGGINO Aristide, "State--of-the-Art of Commercial Proctoring Systems and Their Use in Academic Online Exams", *International Journal of Distance Education Technologies*, Volume 19, Issue 2, April-June 2021, doi: 10.4018/IJDET.20210401.oa3.

• Autenticação/validação automática da identidade do aluno. Apesar do termo se encontrar cunhado em várias soluções, em muitas delas corresponde a um mero automatismo para solicitar e armazenar automaticamente o resultado da captura fotográfica de um documento de identificação exibido pelo aluno*(1). Como alternativa, ou complemento, poderá ser solicitada a validação de um código remetido para o endereço de correio eletrónico (institucional) do aluno, ou através da validação de uma conta de utilizador (nome e respetiva palavra-passe). Algumas soluções permitem, no entanto, uma verificação fiel do conceito de autenticação/verificação (biométrica), comparando, através do reconhecimento facial, um modelo (*template)* biométrico do aluno (previamente armazenado), com um outro que seja construído a partir de uma fotografia captada naquele momento. De igual modo, embora sem casos conhecidos, seria possível usar o mesmo princípio para o reconhecimento da voz do aluno, da sua impressão digital, íris, ou outros dados biométricos;

• Compatibilidade com dispositivos móveis iOS e/ou Android[25], enquanto meios complementares à monitorização do aluno e do espaço físico em que o mesmo se encontra;

• Restrição ao navegador *web* (*browser lockdown*)*(2), geralmente colocando-o em modo de 'ecrã-inteiro', e de específicas funcionalidades*(3) como a abertura de novos separadores, acesso a outras páginas *web* ou impressão de conteúdos;

• Restrição à execução de aplicações que não se revelem necessárias para realização da prova*(4), bem como de funcionalidades do sistema operativo (SO) e respetivos atalhos (*e.g.* copiar/colar, opções do botão direito do rato, fotografia de ecrã/*screenshot*)*(5);

• Deteção e restrição da tecnologia de virtualização*(6), evitando que o aluno execute outros sistemas operativos sobre aquele que proporciona a camada de virtualização (cf. Figura 1);

[25] Sistemas operativos para dispositivos móveis, respetivamente da *Apple* e da *Open Handset Alliance*.

• Gravação e/ou transmissão em tempo real de áudio e de vídeo do examinando. Possibilidade, consoante as aplicações, de sinalização de comportamentos suspeitos e dos respetivos instantes temporais, baseada na análise de movimentos com recurso à tecnologia de Inteligência Artificial;

• Procedimento automático, antes de se iniciar a prova de avaliação, para solicitar ao aluno que efetue uma rotação de 360.º com sua *webcam,* gravando um vídeo do local e das condições em que o exame será iniciado*(7);

• Gravação e/ou transmissão em tempo real, do conteúdo do monitor do examinando*(8);

• Captura e armazenamento do tráfego *web* gerado pelas aplicações, em ambos os sentidos (cliente/servidor e vice-versa)*(9);

• Restrição geográfica dos locais admissíveis para a realização do exame (*e.g.* via GPS);

• Transcrição de eventuais discursos captados pelo microfone;

• Término automático do exame, caso a solução considere (com certo grau de probabilidade) que o aluno adotou um comportamento classificado fraudulento;

• Comunicação em tempo real (*live chat*), entre vigilante e examinando.

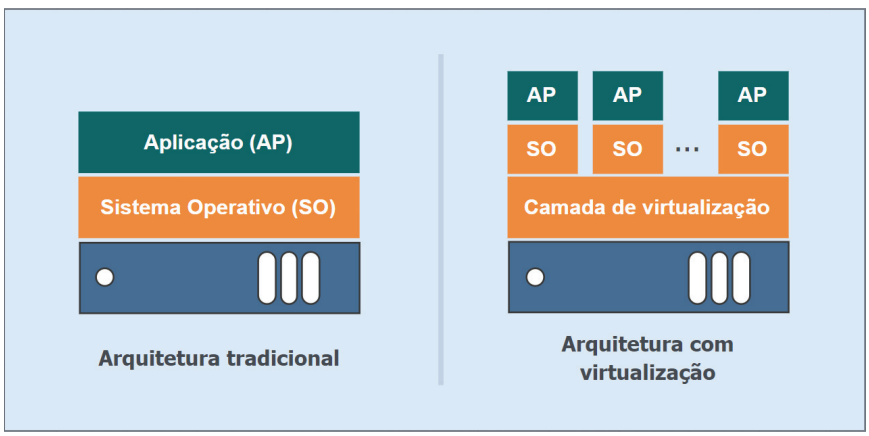

Figura 1 – Arquitetura tradicional e com virtualização.

É possível combinar a monitorização em tempo real com a monitorização automática, verificando-se, numa base contínua, a identidade do examinando e os seus comportamentos. Determinadas soluções, ao detetarem um comportamento suspeito (*e.g.* se o aluno tapar a boca com a mão) notificam de imediato o examinador que, através de um canal de comunicação (*live chat*), tem a possibilidade de alertar ou dar instruções ao aluno.

3.1. Exemplos de ferramentas e respetivas particularidades

Para observar as funcionalidades presentes em cada categoria de monitorização, analisaram-se sete ferramentas comerciais: *ExamNet, ProctorExam e Respondus,* – testadas no Piloto SAR[26] – *Jitsi, Colibri, Safe Exam Browser (SEB)* e *WISEflow* – pela sua ampla utilização e relevância para o estudo.

A informação relativa a cada uma das soluções foi verificada entre janeiro e fevereiro de 2023, através dos respetivos sítios *webe*, nos casos em que existiam, nos fóruns e *blogs* oficiais. Realça-se contudo, que à exceção das ferramentas de código aberto (*open source software*) *Jitsi* e SEB – cujo código não foi alvo de análise –, a informação disponibilizada sobre os específicos tratamentos de dados das várias funcionalidades das restantes soluções é praticamente inexistente ou fornecida de forma dispersa e, ainda assim, considerada pouco clara.

- *Jitsi*

Trata-se de uma plataforma *web* para realização de videoconferências. Pese embora exista uma aplicação para dispositivos móveis e que proporciona uma melhor experiência de utilização, é possível utilizar a solução em qualquer dispositivo sem necessidade da sua instalação, bastando para tanto aceder ao sítio[27] *web* do projeto, através de um navegador.

[26] Exclui-se da análise a solução francesa *TestWe*, por ser manifestamente insuficiente a informação publicamente disponível em: <*https://testwe.eu/pt*>.

[27] Disponível em: <*https://meet.jit.si*>.

A solução é disponibilizada pela empresa norte americana *8x8 Inc.*, de forma gratuita, porém, sem qualquer suporte ou garantia de serviço. O acesso ao código-fonte[28] é livre.

A solução trata os seguintes dados dos utilizadores: endereço IP, nome da sala virtual, conteúdos partilhados durante a sessão e número de contacto telefónico caso a ligação áudio seja estabelecida por via de chamada telefónica. De acordo com a informação disponibilizada, os conteúdos partilhados são apenas armazenados pelo tempo estritamente necessário (no caso das mensagens escritas até que a sessão de videoconferência termine; armazenamento da gravação da sessão, quando a mesma é ativada e até que esta seja totalmente transferida pelo utilizador)[29].

A plataforma permite efetuar uma videoconferência entre múltiplos participantes, que podem partilhar simultaneamente o conteúdo do seu monitor e o vídeo captado pela sua *webcam*. Paralelamente, pode ser efetuada a ligação através de outro dispositivo, o que permite obter imagens do aluno de outra perspetiva.

De acordo com a 'Política de Privacidade'[30], os dados tratados podem ser partilhados com entidades terceiras: "*We may disclose your personal information to the following categories of recipients: to any competent law enforcement body, regulatory, government agency, court or other third party where we believe disclosure is necessary (i) as a matter of applicable law or regulation, (ii) to exercise, establish or defend our legal rights, or (iii) to protect your vital interests or those of any other person*".

- Colibri

É uma solução da FCT/FCCN[31] baseada na aplicação de videoconferência – norte americana – Zoom[32], permitindo a sua integração com

[28] Código aplicacional que, após compilado, dá origem à aplicação tal como a conhecemos.

[29] Informação disponível em: <*https://jitsi.org/meet-jit-si-privacy*>, [15 jan. 2023].

[30] "*Who does 8x8 share my personal information with?*", disponível em: <*https://www.8x8.com/terms-and-conditions/privacy-policy*>, [15 jan. 2023].

[31] Informação disponível em: <*https://ajuda.colibri.fccn.pt/sobre*>.

[32] Disponível em: <*https://zoom.us*>.

a plataforma de ensino *Moodle*. Foi inicialmente disponibilizado para permitir a realização de aulas e reuniões a distância. Após a conclusão do Piloto SAR foi também adotada, por diversas universidades, para monitorizar em tempo real[33] a avaliação dos alunos e, ainda, para a realização de provas públicas por videoconferência[34].

Por ser uma solução essencialmente pensada para a transmissão de conhecimento, a sua aplicação na monitorização da avaliação a distância apresenta certas limitações, mas também algumas vantagens face às demais. Enquanto que através do *Jitsi* é possível efetuar, na mesma sala virtual, a partilha simultânea da câmara e do conteúdo do monitor de todos os intervenientes, permitindo que a mesma pessoa possa vigiar vários alunos, no Colibri a partilha do monitor apenas pode ser efetuada por uma pessoa, em cada momento. No entanto, esta solução oferece a possibilidade de integração com o serviço de autenticação federada RCTSaai[35].

Embora o aluno necessite de instalar a aplicação *Zoom*, esta é atualmente disponibilizada para os sistemas operativos mais comuns, incluindo para dispositivos móveis, que podem ser utilizados de forma complementar. De acordo com a informação disponibilizada através do sítio *web*[36] e no Manual do Utilizador[37], o Colibri permite a gravação das sessões em *cloud,* sem especificar qual, aparentando essa escolha

[33] Utilizado pela Universidade de Coimbra (cf. informação disponível em: <*https://www.uc.pt/aerop/avaliacao_remota*>) e pela Universidade de Évora, que aconselhou os docentes a realizar as avaliações *online,* em tempo real, através do módulo do *Moodle* '*Safe Exam Browser*', com vigilância *Zoom/Colibri* por telemóvel, sem gravação (cf. Despacho reitoral n.º 8/2021, disponível em: <*https://gdoc.uevora.pt/695399*>).

[34] Cf. informação relativa à Universidade do Minho, disponível em: <*https://www.uminho.pt/PT/Teletrabalho/Paginas/ColibriProvasPublicas.aspx*>.

[35] A Rede Ciência Tecnologia e Sociedade (RCTSaai) é uma infraestrutura global de autenticação e autorização, através de uma conta institucional, destinando-se a alunos, docentes e funcionários das instituições aderentes (cf. informação disponível em: <*https://confluence.fccn.pt/display/RCTSAAI/RCTSaai*>).

[36] Disponível em: <*https://ajuda.colibri.fccn.pt/objetivo*>*,* [15 jan. 2023].

[37] 'Gravação das reuniões' (p.12), disponível em: <*https://videoconf-colibri.fccn.pt/assets/tutorial_colibri.pdf*>.

ser delegada na *Zoom Video Communications, Inc.*[38]. Os vídeos ficam disponíveis em *cloud* pelo período de 10 dias, durante o qual podem ser transferidas para o Portal Educast[39].

Ao utilizar a aplicação, sempre que os utilizadores se encontrem autenticados, são tratados os seguintes dados[40]: endereço IP, endereço de acesso à sala virtual[41], nome do utilizador, endereço de *e-mail*, relação entre o utilizador e a instituição de ensino (opcional), perfil do utilizador e conteúdos que o mesmo possa adicionar, modificar ou remover.

- *Safe Exam Browser (SEB)*

É um navegador *web* de características particulares, que permite definir e aplicar restrições à sua utilização, nomeadamente para realização de provas de avaliação (*e.g.* confinamento ao navegador/*browser lockdown,* inibição de certas funcionalidades do sistema operativo como a abertura de determinadas aplicações). A definição das restrições é geralmente comunicada por via da integração com um sistema LMS, de apoio ao ensino. É necessário que o navegador seja instalado no dispositivo do aluno, sendo este compatível com sistemas operativos Windows, macOS e iOS.

---

[38] De acordo com os termos de utilização do Colibri, disponíveis em: <*https://ajuda.colibri.fccn.pt/condicoes-de-uso*> [4 fev. 2023], que mais não são do que a transposição dos termos de utilização da ferramenta *Zoom,* à data de 20 de agosto de 2020 (quando a versão atual, no sítio *web* da *Zoom,* é de 30 de dezembro de 2022), refere o ponto 3, relativo ao 'Uso dos serviços e suas responsabilidades', o seguinte: "O anfitrião pode escolher gravar reuniões e *webinars* da *Zoom*. Ao usar os Serviços, você dá consentimento à *Zoom* para armazenar gravações de toda e qualquer reunião ou *webinar* da *Zoom* em que você ingressar, caso sejam armazenadas em nossos sistemas.". Relembrando que a *Zoom Video Communications, Inc.*, enquanto detentora do produto *Zoom,* é uma empresa norte-americana, parece insuficiente a informação prestada pela FCT aos utilizadores da ferramenta, nomeadamente quanto ao local e às condições de armazenamento dos vídeos gravados, não só na *cloud* mas também no Portal Educast.

[39] Repositório de vídeos educativos nacionais e sua disponibilização aos alunos através da internet (disponível em: <*https://help.educast.fccn.pt/?page_id=372*>, [15 jan. 2023]).

[40] De acordo com a informação disponível em: <*https://ajuda.colibri.fccn.pt/termos-e-condicoes*>, [15 jan. 2023].

[41] Pode ser um dado pessoal se, para acesso à mesma sala virtual, forem enviados diferentes endereços consoante o utilizador final, permitindo relacionar um utilizador com o endereço que lhe foi disponibilizado.

O SEB permite também a integração (opcional) com as aplicações *Jitsi* e *Zoom*, conferindo assim uma componente de monitorização visual do aluno.

Segundo a informação publicada no sítio *web*[42], não existe recolha de dados pessoais pela aplicação: "*SafeExamBrowser (SEB) doesn't send any personal information to any centralized server and is not connected to any web analytics, user tracking or clickstream analytics service.*".

- *WISEflow*

Permite que os utilizadores se autentiquem na aplicação através da criação de uma conta, que pode ser criada por via da integração com vários serviços de autenticação federada, entre os quais o eduGAIN[43].

Requer que o utilizador instale um *plugin* no navegador *web Google Chrome,* permitindo a restrição de funcionalidades do navegador e do sistema operativo.

No início de cada prova de avaliação é tirada uma fotografia ao aluno, que vai sendo comparada com outras fotografias, posteriormente capturadas durante a realização da prova, em momentos aleatórios. Nas provas seguintes, não só são comparadas as novas fotografias que aí sejam capturadas, como também se as compara com aquelas que tenham sido captadas em provas anteriores, e que estão disponíveis pelo período de tempo definido pelo responsável pelo tratamento.

- *Exam.net*

É uma solução através da qual se podem criar as provas de avaliação, permitindo a correção de certo tipo de questões de forma automatizada. Possui, aquilo a que designa de três modos de segurança: no primeiro o aluno só pode realizar o teste através do *Safe Exam Browser,* com as

[42] Disponível em: <*https://safeexambrowser.org/about_overview_en.html#details*>.

[43] Serviço de autenticação disponibilizado a estudantes, investigadores e docentes das instituições de ensino aderentes. Disponível em: <*https://www.fccn.pt/noticias/edugain-conectar-o-mundo*>.

restrições que tenham sido definidas pela instituição de ensino; no segundo, o aluno pode recorrer a um qualquer navegador *web* para realização da prova; e no terceiro, apesar de se permitir a utilização de outros navegadores, é dada preferência, de forma automática, ao SEB.

Para aceder ao exame os alunos não necessitam de criar uma conta *ExamNet*, bastando a introdução de um código que lhes é previamente remetido.

São referidas outras funcionalidades da solução, sem especificar que informação é recolhida acerca do aluno, ou do seu dispositivo: "Também temos deteção de fraude em *background*, que ocorre a um nível mais profundo nos nossos servidores. Isso permite-nos detetar discretamente e informar docentes de suspeita de fraude tal como o uso de *software* especial, ecrãs divididos, *hacking* à integridade do nosso código (ou do ambiente) e procuramos a utilização de máquinas virtuais e soluções de ambiente de trabalho remotas. A nossa equipa monitoriza e afina frequentemente os módulos de deteção de fraude, acompanhando o que acontece no mundo real."[44].

- *Respondus (Monitor* e *LockDown Browser)*

É uma solução composta pelas vertentes de análise (*Monitor)* e de restrição de funcionalidades (*LockDown Browser*). Permite ativar funcionalidades de monitorização em função do tipo de prova[45]:

a) Avaliação na sala de aula, em modo *online,* sem necessidade de recorrer à utilização de *webcams*. O docente fica incumbido de vigiar os alunos presencialmente, enquanto a componente *LockDown Browser* restringe o ambiente da prova àquele navegador, validando o acesso à prova por via de palavra-passe.

b) Avaliação a distância com monitorização automática, através das componentes *LockDown Browser* e *Monitor.* A primeira confere as capacidades anteriormente descritas, enquanto que a segunda guia o

[44] Disponível em: <*https://exam.net/pt/cheat*>, [15 jan. 2023].

[45] Disponível em: <*https://web.respondus.com/wp-content/uploads/2021/03/RespondusMonitor_Scenarios.pdf*>.

aluno na verificação das condições de ligação à *internet* e de funcionamento da *webcam*, bem como na verificação da sua identidade[*(1)]. Após a prova, o docente verifica os resultados fornecidos pela ferramenta, que assinala os instantes temporais das práticas suscetíveis de constituírem fraude, disponibilizando o vídeo respetivo[46].

c) Avaliação em tempo real, sem gravação ou deteção automática de comportamentos suspeitos, na qual o aluno realiza a prova a distância, com recurso à componente *LockDown Browser*. É monitorizado pelo docente, através de uma sessão de videoconferência com recurso às ferramentas *Zoom*, *Teams ou Meet*.

d) Avaliação que combina, simultaneamente, alunos em regime presencial e a distância. Os métodos de monitorização aplicados são, respetivamente, os descritos nas alíneas *a)* e *c)*.

Existe uma funcionalidade designada *Photo on File*, que permite às instituições de ensino carregar fotografias dos alunos, ou dos respetivos documentos de identificação[47]. O propósito é o de permitir identificar quem realiza o exame. No entanto, não é referido se a comparação pode ser automatizada, envolvendo o tratamento de dados biométricos.[*(10)]

De acordo com a política de tratamento de dados[48], a *Respondus, Inc.* tem como subcontratantes a *Amazon Web Services, Inc.*, para prestação do serviço de armazenamento de dados, e a *PayPal* para o processamento de pagamentos, reservando-se o direito de alterar a lista de subcontratantes, em qualquer momento, bastando que reflita as alterações no sítio *web* por si indicado[49]. No ponto 2.3, relativo às transferências internacionais de dados, é dado a conhecer que os dados são tratados fora do Espaço Económico Europeu (incluindo o seu

[46] Motivo, pelo qual, se considera suportar a monitorização com recurso à gravação de vídeo.

[47] Disponível em: <*https://support.respondus.com/hc/en-us/articles/4409607197211-What-is-the-Photo-on-File-feature-that-appears-in-the-instructor-s-video-review-section-*>.

[48] Disponível em: <*https://web.respondus.com/data-processing*>.

[49] Disponível em: <*https://web.respondus.com/privacy/subprocessors*>.

armazenamento), cabendo ao responsável pelo tratamento a tarefa de recolher, junto dos titulares, o respetivo consentimento. O ponto 2.4, relativo às medidas de segurança, menciona a utilização de técnicas de pseudonimização e de cifra, mas não de anonimização dos dados, e sem que referira a que dados ou em que medida são aplicadas as técnicas mencionadas.

Os vídeos gravados pela solução são geralmente armazenados por um período de cinco anos, a partir da data da sua gravação, a menos que o responsável pelo tratamento solicite um prazo de conservação diferente[50].

- *ProctorExam*

Entre o período de realização do Piloto SAR e a atualidade, a solução passou de uma infraestrutura no centro de dados do responsável pelo tratamento (*on-premises*) para um modelo de computação na nuvem (*cloud computing*), socorrendo-se dos serviços prestados pelos subcontratantes *Amazon Web Services* e *Google Cloud.*

Para utilizar a solução é necessário que o aluno instale um *plugin*[51] específico para o navegador *Google Chrome.*

Segundo o sítio *web* da solução[52], são geralmente tratados os seguintes dados do examinando: nome; endereço de *e-mail;* número de estudante ou outro número de identificação pseudonimizado; vídeos e outros dados relativos à gravação do conteúdo do monitor e por via da *webcam* (incluindo da câmara do telemóvel quando utilizado como dispositivo secundário); rosto do estudante e ambiente envolvente; e identificação da instituição de ensino. Na secção '*Data we collect automatically when you use ProctorExam'*, é referida a 'possibilidade' de tratamento de informação relativa ao navegador *web*, sistema operativo

[50] Disponível em: <*https://support.respondus.com/hc/en-us/articles/4409595425307-How-long-is-video-kept-What-if-we-need-a-longer-period-*>.

[51] Disponível em: <*https://chrome.google.com/webstore/detail/proctorexam-screen-sharin/digojkgonhgmnohbapdfjllpnmjmdhpg*>.

[52] Informação disponível em: <*https://proctorexam.com/privacy-and-data-security*>, [12 jan. 2023].

e do endereço IP[53] do examinando, como que não constituindo, também ela, dados pessoais.

A tabela seguinte relaciona as características e funcionalidades das soluções descritas, em função da(s) sua(s) categoria(s) de monitorização.

Características e Funcionalidades			Jitsi	Colibri	SEB	WISEflow	ExamNet	Respondus	ProctorExam
Gerais	Infraestrutura		local/*cloud*	*cloud*	*local*	*cloud*	*cloud*	*cloud*	*cloud*
	Subcontratantes		✓	✓		✓	✓	✓	✓
	Integração LMS		✓	✓	✓	✓	✓	✓	✓
	Conversação *(live chat)*		✓	✓			✓		
	Instalação p*lugin web*					✓			✓
	Instalação aplicação			✓	✓		✓	✓	
	Open Source		✓		✓				
	Sede da empresa		EUA	PT/EUA	Suíça	Dinamarca	Suécia	EUA	Países Baixos
Autenticação	Documento de identificação	*(1)						✓	✓
	Reconhecimento facial					✓		✓	
	Padrão de escrita							✓	
	Por videoconferência		✓	✓	✓		✓	✓	
	Foto em ficheiro	*(10)						✓	
Restrição	Ao navegador *web*	*(2)			✓	✓	✓	✓	
	Opções do navegador *web*	*(3)			✓	✓	✓	✓	✓
	Execução de aplicações	*(4)			✓	✓	✓	✓	
	Funcionalidades do SO	*(5)			✓	✓	✓	✓	
	Virtualização	*(6)			✓	✓	✓	✓	
Monitorização	**Monitorização em tempo real**		✓	✓	✓		✓	✓	✓
	Gravação áudio/vídeo		✓	✓				✓	✓
	Monitorização automática					✓		✓	
	Meio envolvente	*(7)						✓	✓
	Monitor do aluno	(8)	✓	✓					
	Captura do tráfego *web*	*(9)							
	Suporta *webcam* secundária		✓	✓					✓
Compatível	MS Windows	Desktop	✓	✓	✓	✓	✓	✓	✓
	Linux	Desktop	✓	✓					✓
	macOS	Desktop	✓	✓	✓	✓	✓	✓	✓
	Android	Móvel	✓	✓					✓
	iOS	Móvel	✓	✓	✓	✓	✓		✓

Tabela 1 – Características e funcionalidades das soluções de monitorização descritas, em função da sua categoria.

[53] No Acórdão do TJEU, relativo ao processo C-582/14 (*Patrick Breyer v Bundesrepublik Deutschland*), o Tribunal reconheceu que sob certas circunstâncias, um endereço de IP dinâmico é um dado pessoal, mesmo quando a informação adicional, que permite a identificação do titular, se encontra na posse do provedor de serviços/*internet service provider* (ISP). As circunstâncias a que se refere o Tribunal correspondem à possibilidade de se combinar informação adicional que permita identificar o titular dos dados, o que se verifica neste caso.

A necessidade de instalação de uma aplicação no dispositivo do aluno e/ou de um *plugin* para o navegador *web* é, geralmente, um requisito transversal às soluções dos três modelos de monitorização. Pela sua capacidade de funcionamento através das funcionalidades dos navegadores *web*, o projeto *Jitsi* é uma exceção à regra, permitindo a monitorização em tempo real e/ou com recurso à gravação, sem necessidade de qualquer instalação[54] pelo aluno.

As soluções que requerem a instalação de uma aplicação, visam sobretudo a compatibilidade com sistemas operativos *Microsoft Windows* e *Apple macOS.* Por esse motivo, haverá que salvaguardar que da sua utilização não resultam ónus para os alunos, nomeadamente relativos aos custos de licenciamento e de instalação de um sistema compatível, quando estes possuam um outro[55].

De um modo geral, com especial predominância nas soluções que conferem monitorização automática, observa-se uma elevada adesão a serviços prestados por terceiros. Este facto, tem essencialmente que ver com duas ordens de razão:

- Por um lado, a tendência natural de migração para um modelo de computação na nuvem[56], por aí se encontrar resposta ao elevado consumo – mas também variável – de recursos computacionais, que a tecnologia de Inteligência Artificial tanto exige. A adesão à computação em nuvem permitiu, ainda, centralizar a infraestrutura de suporte à respetiva solução, contribuindo para a abstração de um conjunto de tarefas complexas de gestão e manutenção, não só da infraestrutura de suporte como da própria solução. A disponibilidade das soluções e sua resiliência a falhas passou a ser praticamente inabalável, enquanto que o responsável pelo tratamento passou (apenas) a configurar os mecanismos de segurança que pretende conferir a cada prova de avaliação.

[54] Tipicamente os sistemas operativos incluem já um navegador *web*.

[55] Pelo menos nos casos em que a opção pela avaliação a distância não tenha partido do próprio aluno. Mas, ainda que fosse essa a sua vontade, seria expectável que o aluno fosse informado, *a priori,* dos exatos termos de funcionamento da solução, de onde se incluem os requisitos da sua instalação.

[56] Que pode ser total, ou híbrido (migração de apenas parte dos serviços).

• Por outro lado, a disponibilização no mercado de funcionalidades de eficácia comprovada e de grande utilidade na automatização da monitorização, permitindo reduzir drasticamente o esforço de desenvolvimento e manutenção das soluções. São disso exemplo as funcionalidades de reconhecimento facial e de voz, ou a transcrição de discursos, disponibilizadas pela *Amazon Web Services* (AWS)[57].

As soluções de monitorização automática implicam o tratamento de dados biométricos por recorrerem, entre outras, a técnicas de reconhecimento facial, as quais implicam riscos acrescidos para os direitos dos titulares dos dados[58].

A informação disponibilizada pela generalidade das soluções nos respetivos sítios *web* é, geralmente, insuficiente para que responsável pelo tratamento (*a priori*) ou titulares dos dados (*a posteriori*), conheçam com rigor as técnicas e os dados tratados por determinada solução, no seu modelo base de funcionamento (*i.e.* sem a implementação de requisitos impostos).

A decisão de subcontratação impõe que se estabeleça uma negociação entre as partes que, no entanto, pelo facto de algumas soluções serem altamente dependentes de determinadas tecnologias, ou de serviços de terceiros, dificultam em muito certas intenções de alteração ao funcionamento da solução.

A ausência de medidas de proteção de dados desde a conceção poderá igualmente ter consequências diretas nas medidas de proteção de dados por defeito, que o responsável pretenda conferir[59].

---

[57] "How the cloud can help educational institutions with grading, assessments, and admissions", *AWS Public Sector Blog,* (em linha), disponível em: <*https://aws.amazon.com/blogs/publicsector/how-cloud-can-help-educational-institutions-grading-assessments-admissions*>.

[58] Cf. ponto 73 das Diretrizes 3/2019 do CEPD, sobre tratamento de dados pessoais através de dispositivos de vídeo (em linha), disponível em: <*https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_pt.pdf*>.

[59] Naquela que foi a intenção de adotar a solução *Respondus,* por parte de uma instituição de ensino superior portuguesa que, contudo, não pretendia a captação de som, viu-se a mesma obrigada a criar manuais para instruir os alunos a desativar o microfone, através do respetivo sistema operativo. Esta medida resultou de uma manifesta ausência de medidas de proteção dos dados desde a conceção e, por consequência, por defeito. É, ainda, um exemplo daquilo que não foi possível ultrapassar por via de um suposto processo de negociação de subcontratação.

Parte desses dados não são sequer percecionados, pelos subcontratantes, enquanto dados pessoais, apesar da sua combinação permitir a identificação de uma pessoa[60]. Não obstante, importará referir que é ao responsável pelo tratamento que cabe assegurar-se de que o tratamento é realizado em conformidade com o RGPD (cf. art.º 24.º do mesmo diploma), a quem compete, também, despojar-se de quaisquer dúvidas ou incertezas antes de adotar uma determinada solução de monitorização.

4. Fundamentos de licitude para o tratamento de dados pessoais

As soluções de monitorização são tão atraentes quanto melhor se revele a sua eficácia na prevenção e deteção de fraude académica. A opção por soluções de monitorização automática, por implicar o tratamento de dados biométricos, carece de especial atenção no momento da sua fundamentação.

No que respeita aos fundamentos jurídicos para o tratamento de dados pelos diferentes modelos de monitorização, analisaremos conjuntamente a monitorização em tempo real e com recurso à gravação de vídeo, e em secção própria a monitorização automática.

4.1. Tratamento de dados nos processos de monitorização não automáticos

Para o tratamento de dados associado aos modelos de monitorização em tempo real e com recurso à gravação de vídeo perfilam-se, à partida, as alíneas *a)*, *e)* ou *f)* do n.º 1 do art.º 6.º do RGPD[61].

[60] Vide considerações, anteriormente tecidas, acerca da solução *ProctorExam.*

[61] Respetivamente: se o titular dos dados tiver dado consentimento para o tratamento dos seus dados pessoais, para a(s) finalidade(s) em causa; se o tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; ou se o tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, a menos que prevaleçam os interesses ou direitos e liberdades fundamentais do titular dos dados.

Em qualquer das hipóteses, teria o responsável pelo tratamento de adotar as medidas técnicas e organizativas necessárias para mitigar os riscos associados à gravação não autorizada e ao acesso indevido às gravações autorizadas, que necessitariam de ter associado um prazo de conservação previamente estabelecido[62] A par da obrigatoriedade do cumprimento dos restantes princípios relativos ao tratamento de dados, entende-se que seria útil a aprovação de um código de conduta e de um manual de procedimentos destinados aos vigilantes, contribuindo assim para uma atividade idónea e limitada às finalidades do tratamento dos dados[63].

4.1.1. Consentimento do titular dos dados

Remetendo-nos ao fundamento jurídico previsto na alínea *a)* do n.º 1 do art.º 6.º do RGPD, entende-se que o consentimento do aluno (que se supõe maior de idade) afigura-se condição suficiente para o tratamento dos dados desde que prestado nas condições do disposto no ponto 11 do art.º 4.º do RGPD, na sua redação atual[64], bem como cumpridos os princípios relativos ao tratamento de dados pessoais (art.º 5.º, *ibid*.).

Note-se, no entanto, que o Considerando n.º 43, do RGPD, classifica de improvável a livre vontade do titular, sempre que se verifique um manifesto desequilíbrio entre o titular dos dados e o responsável pelo seu tratamento, designadamente quando este se trate de uma autoridade pública. Um consentimento efetivamente livre implicaria sempre que fosse dada ao aluno a possibilidade de realizar a mesma prova em regime presencial, o que poderia não ser imediatamente praticável, num contexto em que vigorassem restrições aos direitos dos cidadãos (*e.g.* durante a pandemia por COVID-19).

---

[62] Cf. n.º 1 do art.º 24.º do RGPD, relativo à responsabilidade do responsável pelo tratamento. Alíneas *e)* e *f)*, n.º 1 do art.º 5.º do RGPD, relativas ao princípio da limitação da conservação e ao princípio da integridade e confidencialidade dos dados, respetivamente.

[63] Respetivamente, art.º 5.º e n.º 2 do art.º 24.º, ambos do RGPD.

[64] A segunda retificação ao Regulamento Geral sobre a Proteção de Dados, publicada no jornal oficial da União a 4 de março de 2021, substitui a expressão «explícita» por «inequívoca».

Por esse motivo, de acordo com as Diretrizes n.º 5/2020 do CEPD (pontos 16 e 17)[65], relativas ao consentimento na aceção do Regulamento 2016/679, o tratamento de dados baseado na alínea *e)* do n.º 1 do art.º 6 do RGPD parece ser, neste tipo de casos, o mais apropriado. É o que se analisa em seguida.

4.1.2. Tratamento por motivos de interesse público

Os interesses prosseguidos pelas entidades públicas correspondem aos interesses públicos determinados por lei[66].

No caso das instituições públicas de ensino superior ministrado a distância, prevê o disposto no art.º 14.º do Decreto-Lei n.º 133/2019, de 3 de setembro, que cabe a estas "definir metodologias de avaliação formativa e sumativa que integrem avaliações presenciais ou através de plataformas tecnológicas, que assegurem a fiabilidade da avaliação desenvolvida".

No que concerne às restantes instituições públicas de ensino superior, prevê o Decreto-Lei n.º 74/2006, de 24 de março, na sua redação atual, que os regimes de avaliação de conhecimentos são aprovados pelo órgão legal e estatutariamente competente do respetivo estabelecimento de ensino. Desta forma, seria suficiente contemplar os modelos de avaliação em tempo real e/ou com recurso à gravação nas respetivas normas e regulamentos de avaliação, bem como a publicação do respetivo despacho reitoral de homologação[67].

---

[65] Disponível em: <*https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pt.pdf*>.

[66] Regime jurídico das instituições de ensino superior, aprovado pela Lei n.º 62/2007, de 10 de setembro.

[67] Vide exemplos em nota de rodapé n.º 33 e 34.

4.1.3. Tratamento por motivo de interesses legítimos do responsável

O segundo parágrafo[68] do n.º 1 do art.º 6.º do RGPD veda às autoridades públicas, na prossecução das suas atribuições, a possibilidade de fundamentar o tratamento de dados com base na alínea *f)* do primeiro parágrafo, *ibidem*.

As instituições privadas de ensino superior regem-se pelo direito privado, em tudo o que não for legalmente contrariado[69]. A alínea *f)* do n.º 1 do art.º 6.º do RGPD é assim uma opção válida para este tipo de instituições que, contudo, sempre teriam que demonstrar a impossibilidade de realizar a avaliação por outra via, que não envolvesse o tratamento de dados pessoais em medida que ultrapassasse a da avaliação presencial. É, pois, o que se retira da conjunção dos três primeiros princípios do RGPD[70] relativos ao tratamento de dados pessoais, *i.e.,* revestir o tratamento de um caráter de necessidade, circunscrito ao mínimo indispensável para prossecução das finalidades (que devem ser lícitas) e limitado ao tratamento de dados adequados, pertinentes e necessários a essas mesmas finalidades.

Por outro lado, seria condição *sine qua non* a realização de um teste de adequação do qual não resultasse que os interesses, direitos e liberdades dos titulares dos dados não prevaleceriam sobre os interesses legítimos do responsável pelo tratamento.

Quanto às fundações públicas sujeitas a um regime de direito privado, fundamentou a CNPD o seu ponto de vista na Deliberação/2021/662 (pontos 46 a 50). Daí se retira que, às fundações que tenham por

---

[68] Apesar de não ser relevante para este caso, note-se que a versão portuguesa do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho é a única que refere no segundo parágrafo do art.º 6.º (*in fine*), a expressão "por via eletrónica", presumindo-se tratar de uma gralha. *Nova Legislação de Proteção de Dados*, CNPD, dez. 2019, depósito legal n.º 466370/20.

[69] Cf. n.º 4 do art.º 9.º da Lei n.º 62/2007 (Regime jurídico das instituições de ensino superior).

[70] Alíneas *a)*, *b)* e *c)* do n.º 1 do art.º 5.º do RGPD, respetivamente: licitude, lealdade e transparência; limitação das finalidades e; minimização dos dados.

missão a manifesta prossecução do interesse público, estará, em princípio, vedada a invocação de interesses legítimos.

4.2. Monitorização automática e o tratamento de dados biométricos

A monitorização automática está geralmente associada à utilização de técnicas de reconhecimento facial para validação da identidade do aluno, implicando, por esse motivo, o tratamento de dados biométricos[71]. De uma análise ao Considerando n.º 51 do RGPD, *prima facie*, resultará o entendimento de que o tratamento de fotografias constitui um tratamento de categorias especiais[72] de dados pessoais, sempre que "processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular", sendo abrangidas pela definição de dados biométricos.

Segundo o entendimento de A. Barreto Menezes Cordeiro, os Considerandos não podem ser utilizados para diminuir ou aumentar o alcance da lei, sendo o seu único propósito o de explicar os preceitos legais e os motivos que os sustentam. Nesse sentido, sendo perentório o n.º 1 do art.º 9 do RGPD na proibição de tratamento dados biométricos "para identificar uma pessoa de forma inequívoca", o Considerando n.º 51 mais não vem do que esclarecer que essa proibição abrange tanto as técnicas de identificação como de autenticação/verificação biométricas.

[71] Dados biométricos, segundo a alínea *14)* do art.º 4.º do RGPD, "são dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos."

[72] Que, de acordo com n.º 1 do art.º 9.º do RGPD, inclui os "dados biométricos para identificar uma pessoa de forma inequívoca".

Para clarificar a diferença entre os conceitos, atente-se no Parecer n.º 3/2012 do WP29[73] (p.6)[74] sobre a evolução das tecnologias biométricas, de onde se extrai, sobre a identificação biométrica:

"[a] identificação de uma pessoa por um sistema biométrico consiste, em regra, no processo de comparação de dados biométricos dessa pessoa (obtidos no momento da identificação) com um determinado número de modelos biométricos armazenados numa base de dados (ou seja, um processo de correspondência «um para muitos»)".

A definição anterior encontra-se em linha com a posição da Comissão Europeia patente no Livro Branco sobre a Inteligência Artificial (p.24)[75], no qual se expõe que a "identificação significa que o modelo da imagem facial de uma pessoa é comparado com muitos outros modelos armazenados numa base de dados para saber se a imagem dessa pessoa se encontra armazenada nessa base de dados".

O conceito parece, assim, estar associado ao processo de comparação de um determinado modelo (*template*) biométrico de uma pessoa desconhecida, ou para a qual não se sabe se estará registada na base de dados, daí resultando a necessidade de comparação com os vários modelos biométricos que constituem a base de dados (*e.g.* leitores biométricos para controlo de assiduidade ou de acesso a instalações).

Relativamente à verificação (ou autenticação) biométrica, refere o no Parecer n.º 3/2012 do WP29, o seguinte:

"[a] verificação de uma pessoa por parte de um sistema biométrico consiste, em regra, no processo de comparação de dados biométricos dessa pessoa (obtidos no momento da identificação) com um único

[73] Grupo de trabalho previsto pelo art.º 29.º da Diretiva 95/46/CE, para dar orientações gerais na clarificação da legislação em matéria de proteção de dados. Lidou com as questões relativas à proteção de dados pessoais e à privacidade até 25 de maio de 2018, data de em que a Diretiva 95/46/CE foi revogada pela execução do RGPD e o WP29 substituído pelo Comité Europeu para a Proteção de Dados (EDPB, na versão inglesa).

[74] Disponível em: <*https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf*>.

[75] Disponível em: <*https://op.europa.eu/pt/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1*>.

modelo biométrico armazenado num dispositivo (ou seja, um processo de correspondência «um para um»)".

O Livro Branco sobre a Inteligência Artificial descreve o mesmo conceito como a "comparação de dois modelos biométricos, que geralmente se pressupõe pertencerem à mesma pessoa (…) para determinar se a pessoa que aparece nas duas imagens é a mesma", dando como exemplo o controlo automatizado de fronteira nos aeroportos.

A título de exemplo, considere-se o processo de verificação existente nos *smartphones* e que permite criar um modelo biométrico com base em fotografias do seu proprietário. Posteriormente, é possível ao proprietário desbloquear o equipamento se, da verificação entre a fotografia tirada naquele momento e o modelo biométrico previamente criado, resultar uma relação de correspondência.

De referir, ainda, que diversas soluções de monitorização automática garantem a validação da identidade do aluno não só através de técnicas de reconhecimento facial, como também por via do tratamento de outros dados biométricos. Aí se enquadrará a análise do padrão de escrita do aluno, ou dos seus dados comportamentais, que contribuem igualmente para o grau de sucesso da sua identificação de forma inequívoca.

Relembrar, também, que essa identificação ocorre não só no momento que antecede a prova, mas também durante o período da sua realização, no qual são capturadas novas amostras, que por sua vez poderão ter a dupla finalidade de servir uma comparação imediata ou, a partir delas, se aperfeiçoar ou criar novos modelos biométricos para futuras comparações (cf. sucede com a solução *Wiseflow*).

Pelos motivos expostos, as soluções de monitorização automática terão de ser abordadas na perspetiva do tratamento de categorias especiais de dados pessoais, exigindo-se, nesse contexto, a verificação de uma das exceções previstas no n.º 2 do art.º 9.º do RGPD, que permita o levantamento da proibição prevista no n.º 1 do mesmo artigo e diploma.

4.2.1. Consentimento explícito do titular dos dados

O consentimento explícito do titular dos dados é a possibilidade prevista pela alínea *a)* do n.º 2 do art.º 9.º do RGPD, salvo se o direito da União ou do Estado-Membro previr que a proibição do tratamento dos dados não possa ser levantada. Não parece ser esse o caso, atenta a Lei n.º 58/2019, de 8 de agosto, e tendo em conta que o público alvo serão alunos do ensino superior, supondo-se maiores de idade.

O consentimento do aluno afigura-se condição suficiente para o tratamento dos seus dados biométricos, desde que seja livre, específico, informado e inequívoco, na aceção do disposto no ponto 11 do art.º 4.º do RGPD, mas também ele explícito, atendendo ao tratamento de categorias especiais de dados pessoais, e desde que cumpridos os princípios relativos ao tratamento de dados pessoais (art.º 5.º do mesmo diploma).

No entanto, para que o consentimento seja efetivamente livre, sendo essa uma condição essencial para que se considere válido, o ponto 3 das Diretrizes 05/2020 refere que "o consentimento só pode constituir fundamento jurídico adequado se, ao titular dos dados, for oferecido controlo e uma verdadeira opção de aceitar ou recusar os termos propostos ou recusá-los sem ser prejudicado".

Tendo em conta que o aluno não se encontra numa posição de paridade em relação ao estabelecimento de ensino que frequenta, o seu consentimento só será efetivamente livre[76] se, à luz dos Considerandos n.º 42 (*in fine*) e 43 do RGPD, lhe for concedida a possibilidade de realizar a mesma prova de avaliação sem se sujeitar a tais medidas de controlo. Assim, seria válida a alternativa de realização da atividade de avaliação em regime presencial, ou outra forma, desde que não implicasse o tratamento de dados biométricos, e praticada em iguais circunstâncias de dificuldade, sem que optando por uma dessas soluções resultassem consequência negativas para o aluno.

[76] De acordo com o ponto 13 das Diretrizes 05/2020 do CEPD, "[o] elemento «livre» implica uma verdadeira escolha e controlo para os titulares dos dados. Regra geral, o RGPD prevê que se o titular dos dados não puder exercer uma verdadeira escolha, se sentir coagido a dar o consentimento ou sofrer consequências negativas caso não consinta, então o consentimento não é válido".

4.2.2. Tratamento por motivos de interesse público

O levantamento da proibição do tratamento de dados biométricos poderá ainda acontecer nas condições a que se refere a alínea *g)* do n.º 2 do art.º 9.º do RGPD. No entanto, o fundamento referido não só requer a existência de interesse público, como o classifica de 'importante', característica que não lhe está associada em qualquer outra disposição do RGPD, vincando assim um atributo que alça uma especial necessidade de proteção dos dados tratados.

Atento o disposto no art.º 14.º do Decreto-Lei n.º 74/2006, de 24 de março, tal norma, que define a autonomia do respetivo órgão legal e estatutariamente competente para aprovar o regime de avaliação de conhecimentos não será condição suficiente para permitir a utilização de técnicas de reconhecimento facial nos processos de avaliação, não obstante a natureza do interesse prosseguido.

Pelo facto de o tratamento incidir sobre categorias especiais de dados pessoais, sendo suscetível de provocar maior risco de ingerência nos direitos fundamentais[77] dos alunos, será necessário que se encontre legalmente estatuído em que medida e circunstâncias, sem esquecer as salvaguardas adequadas, se poderá identificar os estudantes com recurso aos seus dados biométricos (Considerando n.º 52 do RGPD).

Ao verificar-se a situação anteriormente descrita, seria igualmente expectável a regulamentação (*e.g.* através da publicação de uma Portaria), das especificidades (da utilização) a que se referem as Orientações sobre Reconhecimento Facial[78] do Comité Consultivo[79] da

[77] Incluindo, mas não limitado ao respeito pela vida privada e familiar e ao direito à proteção de dados pessoais (respetivamente, art.º 7.º e 8.º da Carta dos Direitos Fundamentais da UE), de acordo com as considerações da Agência dos Direitos Fundamentais da União Europeia sobre a tecnologia de reconhecimento facial. Não se tratando de direitos absolutos, poderão os mesmos ser sujeitos a interferências devidamente justificadas, desde que não comprometam os valores fundamentais e inalienáveis desses direitos.

[78] "*Guidelines on facial recognition*", Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), 2021. Disponível em: <*https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html*>.

[79] Previsto no Capítulo V (parágrafos 85 a 87) da Convenção 108, de 1981.

Convenção 108[80], tendo em conta que o Estado Português aderiu à referida Convenção em 14 de maio de 1981, ratificando-a em 2 de setembro de 1993. A partir de 1 de janeiro de 1994 passou a mesma a ser executada na ordem jurídica nacional.

O tratamento dos dados por motivos de interesse público parece ser, aliás, o caminho adequado, quando em causa esteja a restrição de direitos fundamentais dos titulares, uma vez que o Considerando n.º 52 do RGPD prevê que a derrogação possa ser feita por motivos de ordem sanitária, incluindo de saúde pública – como se verificou em abril de 2020 e nos tempos que se seguiram. Ainda assim, haveria que criar o referido diploma em respeito pelos princípios da necessidade e proporcionalidade, sem esquecer as salvaguardas adequadas, submetendo-o ao parecer prévio da CNPD (embora não vinculativo), no âmbito das suas atribuições e competências.

5. Da necessidade de realizar uma AIPD

A realização de uma avaliação de impacto sobre a proteção de dados (AIPD)[81] permite ao responsável pelo tratamento – em princípio a instituição de ensino, a menos que essa responsabilidade seja (explicitamente) partilhada – não só avaliar os riscos que o tratamento é suscetível de gerar, como ainda, o auxilia na gestão desses riscos, permitindo avaliar e garantir a necessidade e a proporcionalidade do tratamento dos dados. Tem, portanto, uma dupla finalidade.

Exige-se a realização de uma AIPD sempre que um tratamento – em particular se utilizar novas tecnologias, e atendendo à sua natureza, âmbito, contexto e finalidade – seja suscetível de implicar um elevado

[80] Convenção para a Proteção de Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, *European Treaty Series* n.º 108, pp. 7-8, *in fine*. Disponível em: <*https://rm.coe.int/16800ca434*>.

[81] Cujo conteúdo mínimo se encontra descrito no n.º 7 do art.º 35.º do RGPD.

risco para os direitos e liberdades dos titulares[82]. A realização de AIPD é obrigatória, mas não limitada, aos casos em que se verifique o tratamento de categorias especiais de dados em grande escala[83].

5.1. Tratamento de dados nos processos de monitorização não automática

Ainda que possa não se entender obrigatória a realização de AIPD nos tratamentos de dados prosseguidos pelos métodos de monitorização em tempo real e com recurso à gravação, a opção pela sua efetiva realização irá favorecer, em primeiro lugar, o responsável pelo tratamento, ao muni-lo dos dados necessários a atestar a conformidade do tratamento e, por último, os titulares dos dados e a defesa dos seus direitos e liberdades.

Nessa análise devem versar as conclusões sobre os riscos associados à utilização de determinada solução comercial (ou desenvolvida pela própria instituição), e as medidas adotadas para mitigar esses mesmos riscos.

Note-se, porém, que se os tratamentos anteriores forem prosseguidos sob determinadas circunstâncias, poderão efetivamente requerer a realização de uma AIPD. É, pois, essa a responsabilidade do responsável pelo tratamento. A título de exemplo tome-se um caso de monitorização com recurso à gravação que envolva transferências internacionais de dados para o território de um país terceiro que não assegure um nível de proteção de dados adequado, nomeadamente para o armazenamento dos vídeos. Deverão ser adotadas salvaguardas adicionais (*e.g.* cifra das comunicações e dos dados armazenados) para garantir um nível de proteção dos dados essencialmente equivalente ao da União Europeia[84], sendo óbvia, nesse caso, a necessidade de realizar uma AIPD.

---

[82] Cf. n.º 1 do art.º 35.º do RGPD.

[83] Cf. alínea *b)* do n.º 3 do art.º 35.º do RGPD.

[84] Por referência ao Acórdão do TJUE, de 16 de julho de 2020, no processo C-311/18 (Acórdão *Schrems II*).

Nos casos em que a instituição de ensino determina aos alunos a instalação de específicas aplicações nos seus dispositivos, pois então esta terá necessariamente a responsabilidade de fazer o que estiver ao seu alcance para garantir que essas aplicações sejam seguras, não só naquele momento, como em utilizações futuras. Parece assim razoável, sem prejuízo de outras garantias ou intervenientes, a delegação de responsabilidade no subcontratante e contratualmente assumida, para que este realize os testes necessários à segurança da aplicação, numa base contínua, dando deles conhecimento ao responsável pelo tratamento ainda que de forma sumária, fazendo assim prova da sua efetiva realização. O responsável pelo tratamento poderá também ter necessidade de intervir diretamente no seu sistema (LMS), se dele depender assegurar que o aluno tem instalada a última versão da solução adotada para realização da prova. Não faria sentido que, por um lado se corrigissem os problemas de segurança encontrados e que, por outro, se continuasse a permitir a utilização de versões obsoletas e inseguras[85].

A comercialização no mercado negro, de soluções 'chave na mão' para aceder remotamente a dispositivos vulneráveis é uma realidade[86] atual, sendo inclusive utilizada por instituições governamentais de vários países.

Durante o processo de avaliação da necessidade de realização de uma AIPD, deve igualmente ter-se em conta as cláusulas contratuais associadas à prestação de serviços e às políticas de utilização dos mesmos. Embora muito se louve a iniciativa da FCT em disponibilizar a solução Colibri para coadjuvar, primeiro, o ensino a distância, e mais tarde a realização de provas de avaliação, não pode deixar de aqui se referir que poderia a mesma ter ido mais além na definição contratual dos já aqui referidos 'Termos de Utilização' do Colibri/Zoom,

[85] Falhas de segurança detetadas no Google Chrome (2650 milhões de utilizadores) e Zoom: <*https://www.wired.co.uk/article/google-chrome-windows-zoom-critical-update*>, <*https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=+Google+Chrome*>, <*https://explore.zoom.us/en/trust/security/security-bulletin*>.

[86] PERLROTH, Nicole, *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race,* Bloomsbury Publishing, 2021.

destacando-se, desta vez, a secção 15 relativa à 'Ausência de Garantias'[87] e a secção 17, relativa 'Limitação de Responsabilidade'[88], das quais resultam abstratas garantias para os utilizadores finais do serviço – alunos e docentes –, mas também para as instituições de ensino enquanto responsáveis pelo tratamento dos dados.

Recorde-se, ainda, que nos casos em que não é clara a necessidade de realização de uma AIPD, o Grupo de Trabalho do art.º 29 recomenda a sua realização[89].

5.2. Tratamento de dados no processo de monitorização automática

Se nos modelos de monitorização anteriormente referidos se admite a discussão da obrigatoriedade de realização de AIPD, não parece que o mesmo se aplique aos tratamentos de dados sob o processo de monitorização automática. Independentemente de determinada solução dispor de um maior ou menor número de funcionalidades, a utilização de novas tecnologias[90], *prima facie*, será suscetível de implicar um elevado risco para os direitos e liberdades dos titulares dos dados.

---

[87] De onde se retira: "(…) a utilização dos serviços é exclusivamente por sua conta e risco. Qualquer material e/ou dados baixados ou de outra forma obtidos pela utilização dos serviços são por seu próprio critério e risco. Você será o único responsável por qualquer dano que possa decorrer da utilização dos serviços. Todo o risco decorrente da utilização ou desempenho dos serviços recai sobre você. A Zoom não assume qualquer responsabilidade pela retenção de qualquer informação de usuário ou comunicação entre usuários. A Zoom não pode garantir e não promete qualquer resultado específico da utilização dos serviços. A utilização é por seu próprio risco.", cf. consulta em 4 de fevereiro de 2023, (em linha) disponível em: <*https://ajuda.colibri.fccn.pt/condicoes-de-uso*>.

[88] De onde se retira "Na extensão máxima permitida pela lei aplicável, em nenhum caso a Zoom ou suas afiliadas, fornecedores ou revendedores serão responsáveis por quaisquer danos especiais, incidentais, indiretos, punitivos ou consequenciais (…)", terminando do seguinte modo "Como alguns estados e jurisdições não permitem a exclusão ou limitação de responsabilidade, a limitação acima pode não se aplicar a você.". Disponível em: <*https://ajuda.colibri.fccn.pt/condicoes-de-uso*>, [4 fev. 2023].

[89] Cf. (p.9 *in fine*) Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679. Disponível em: <*https://www.cnpd.pt/media/f0ide5i0/aipd_wp248rev-01_pt.pdf*>.

[90] Cf. n.º 1 do art.º 35.º do RGPD.

Poderia essa avaliação estar dispensada, caso se verificasse uma das exceções previstas pelo n.º 5, ou pelo n.º 10, do art.º 35.º do RGPD. No entanto, estando implicado o tratamento de categorias especiais de dados pessoais, automaticamente se exclui o n.º 10, já que o mesmo incide sobre específicos fundamentos de licitude previstos no n.º 1 do art.º 6, e não no n.º 2 do art.º 9.º, conforme seria necessário para levantar a proibição daquele tratamento.

Por outro lado, pelo facto de não ter a CNPD publicado a lista (opcional) a que se refere o n.º 5 do art.º 35.º, relativa aos tipos de operações de tratamento para os quais não é obrigatória a realização de uma AIPD, se exclui também eventual exceção que ali pudesse estar prevista e ser aplicável ao caso em análise.

A utilização de soluções de monitorização automática, das quais resulte uma decisão de anular uma prova de avaliação tendo por base um tratamento automatizado, com recurso a definição de perfis, sempre obrigaria à realização de AIPD de acordo com a alínea *a)* do n.º 3 do art.º 35.º do RGPD. Mas, ainda que assim não se entendesse, ou se a decisão final de anular um exame fosse delegada no respetivo docente, após a sua análise, haveria que consultar a lista a que se refere o n.º 4 do art.º 35.º do RGPD, relativa aos tratamentos de dados pessoais sujeitos à realização de AIPD[91] e que se materializa no Regulamento 798/2018. Da sua análise e apreciação dos números 2, 5, 7 e 9 resultaria a clarividência da necessidade de realização de AIPD.

Tendo em conta a reflexão efetuada, resumem-se, de seguida, para cada uma das categorias de monitorização, os fundamentos de licitude adequados ao tratamento de dados e a necessidade de se realizar uma AIPD.

[91] Aprovada pelo Regulamento 798/2018, disponível em: <*https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121818*>.

Soluções de Monitorização	Fundamentos de licitude admissíveis	AIPD
Em tempo real	Alínea *a)* ou *e)* do n.º 1 do art.º 6.º do RGPD *(com as devidas anotações)* Ou Alínea *f)* do n.º 1 do art.º 6.º do RGPD *(se em causa estiverem instituições privadas)*	Recomendada
Recurso a gravação	*idem*	*idem*
Automática	Alínea *e)* do n.º 1 do art.º 6.º do RGPD, conjugada com a alínea *g)* do n.º 2 do art.º 9.º do mesmo diploma *(com as devidas anotações)* Ou Alínea *a)* do n.º 1 do art.º 6.º do RGPD, conjugada com a alínea *a)* do n.º 2 do art.º 9.º do mesmo diploma *(com as devidas anotações)*	Obrigatória

Tabela 2 – Relação dos fundamentos de licitude elegíveis e necessidade de realizar AIPD, consoante o tipo de monitorização

6. Conclusão

De forma geral, considera-se escassa a informação disponibilizada, nos sítios *web* das soluções comerciais, que contribua de forma útil para a perceção integral do respetivo modelo de funcionamento e dos dados suscetíveis de serem tratados. Tal facto não favorece nem as instituições de ensino, no momento da procura por soluções capazes de responder às suas necessidades, nem a tranquilidade dos alunos, quando procuram

informação após se verem confrontados com a necessidade de utilizar uma determinada solução comercial.

Realça-se, assim, a especial importância em disponibilizar, de forma pública ou reservada (*e.g.* restrita à comunidade académica visada), integral ou parcialmente, a AIPD que o responsável pelo tratamento tenha eventualmente realizado.

Ademais, determinadas soluções de monitorização possuem uma variedade de funcionalidades, cuja a opção pela sua utilização fará variar o grau de ingerência nos direitos e liberdades dos titulares dos dados. Nessa medida, têm as instituições de ensino, enquanto responsável pelo tratamento, a obrigação de verificar e demonstrar que o tratamento de dados pessoais que realizam, respeita os princípios e as regras legalmente aplicáveis, em matéria de proteção dos dados[92].

Por outro lado, apesar de se terrem elencado os possíveis fundamentos de licitude, para o tratamento de dados prosseguido por cada uma das três categorias de monitorização, compete a cada instituição de ensino avaliar e demonstrar que o concreto tratamento é, de facto, necessário, por não existirem, ou não serem efetivamente viáveis, outros métodos de avaliação menos intrusivos da privacidade dos titulares dos dados. Tal, aplica-se, não só na prossecução dos interesses (públicos) da instituição de ensino, mas também nas situações em que o titular dá o seu consentimento para tratamento dos seus dados.

Em suma, e de acordo com as Orientações da CNPD[93], "importa avaliar o tratamento à luz dos princípios da minimização dos dados pessoais e da proporcionalidade, nas vertentes da adequação, necessidade e proibição do excesso[94]". Não seria, portanto, razoável que, por via do recurso à monitorização da avaliação a distância, pretendesse o responsável pelo tratamento assegurar adicionais garantias, face às observadas no regime de avaliação presencial.

---

[92] Nos termos do n.º 2 do art.º 5.º e n.º 1 do art.º 24.º, ambos do RGPD.

[93] "Orientações sobre avaliação à distância nos estabelecimentos de ensino superior" (p.4, *in fine*), disponível em: <*https://www.cnpd.pt/media/0mwfxdcp/orientacoes_avaliacao_distancia_ensino_superior.pdf*>.

[94] Cf. alínea *c)* do n.º 1 do art.º 5.º do RGPD.

Nesse sentido, a monitorização em tempo real (sem gravação de áudio ou vídeo) parece ser o modelo que mais se aproxima da vigilância em regime presencial e, ainda, aquele que representa menor risco de ingerência nos direitos e liberdades dos titulares. A sua combinação com uma ferramenta de características semelhantes às que são conferidas pelo SEB, que é também de código aberto e por esse motivo mais transparente, é uma possibilidade indubitavelmente menos intrusiva face às soluções de monitorização automática. Por outro lado, permite igualmente o emparelhamento de um dispositivo secundário, que possibilita a captação, de outra perspetiva, do local em que o aluno realiza o exame, perfilando-se como alternativa adequada à captação de som.

O responsável pelo tratamento tem, de facto, uma panóplia de opções e efetiva liberdade de escolha, permitindo-lhe configurar um ambiente fiável para efeitos de avaliação a distância, em função das suas reais necessidades e do respeito pela privacidade dos titulares dos dados.

Da responsabilidade civil pelo tratamento desconforme de dados pessoais

Daniel Bessa de Melo[1]

Resumo: O presente artigo visa explorar a temática da responsabilidade civil das entidades responsáveis pelo processamento e tratamento de dados pessoais, sobretudo à luz do art. 82.º do Regulamento Geral de Proteção de Dados e da sua articulação com as normas internas. Tratar-se-á em especial da responsabilidade civil do encarregado de proteção de dados.

Palavras-chave: *proteção de dados; responsabilidade civil; RGPD; encarregado de proteção de dados.*

Abstract: This article tackles the issue of civil liability of entities responsible for data protection compliance, mainly regarding article 82nd of the General Data Protection Regulation and its articulation with internal rules. Importance shall be given to the civil liability of the data protection officer.

Keywords*: data protection; civil liability; GDPR; data protection officer.*

[1] Advogado. Licenciado em Direito pela Faculdade de Direito da Universidade do Porto. Mestre em Ciências Jurídico-Civilísticas pela Faculdade de Direito da Universidade do Porto. dbm@sociedadeadvogados.eu / danielbessamelo@gmail.com

1. Introdução

O Direito da Proteção de Dados representa ainda um domínio negligenciado na literatura jurídica e, até à revolução coperniciana operada pelo RGPD, traduzia algo de desconhecido na doutrina portuguesa[2]. Não surpreende que poucos tenham sido os contributos a respeito da responsabilidade civil no contexto do tratamento de dados pessoais. Dada ainda a exiguidade das decisões jurisprudenciais, tanto a nível nacional como transnacional, é patente que laboramos essencialmente no desconhecido – mas este desconhecimento convida-nos à originalidade, à antecipação de querelas e a bebermos dos contributos comparatísticos, sabido, aliás, como nos confrontamos com um sistema normativo que ultrapassa a latitude do ordenamento jurídico português.

2. A natureza dos interesses infringidos pelo tratamento desconforme de dados pessoais

Escusado será aqui referir que nem todo o prejuízo é passível de ser ressarcido nem toda a afetação de interesses despoleta *ipso facto* uma situação de responsabilidade[3]. Incumbe ao legislador delimitar o círculo de interesses protegidos através das normas de responsabilidade civil, decalcando dessa forma o perímetro do dano normativamente relevante. Entre nós, e considerando apenas a responsabilidade aquiliana, tal perímetro é dado pelo art. 483.º, n.º 1, do Código Civil, e consiste ou na preterição de um direito absoluto ou na violação de uma disposição legal destinada a proteger interesses alheios.

---

[2] MENEZES CORDEIRO, António Barreto, "A Autonomia da Função de Encarregado de Proteção de Dados e a Independência do Exercício da Advocacia", *Revista da Ordem dos Advogados*, Ano 78, Vol. I/II, 2018, pág. 18.

[3] *Vide* SALVI, Cesare, "Danno" in AA.VV., *Digesto delle Discipline Privatistiche – Sezione Civile*, Vol. V, 4.a ed., UTET, Torino, 1998, pág. 64.

Considerando as opções fundamentais traçadas pelo nosso legislador, não nos deparamos com nenhuma dificuldade na mobilização dos instrumentos comuns de responsabilidade civil. O direito à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à sua livre circulação, declarado propósito do Regulamento Geral de Proteção de Dados (art. 1.º, n.º 1)[4], assume a morfologia de um direito fundamental[5]. O fundamento último desse direito ao controlo da divulgação e utilização de dados pessoais, considerado como corolário do direito à autodeterminação informativa, descobre-se na tutela da dignidade humana e do livre desenvolvimento da personalidade[6], conforme explicado pelo Tribunal Constitucional Alemão[7]. A maioria da literatura tende, no entanto, a pugnar por uma via mais restrita, descortinando o fundamento da proteção de dados na tutela da *privacy*, a qual representaria a "fase mais recente" da evolução do direito à privacidade[8].

Independentemente de qual seja a resposta preferível, o que não incumbe aqui aflorar nem releva para o escopo deste estudo, apenas importa referir que o direito à proteção de dados pessoais, mesmo a

---

[4] Na ausência de indicação em sentido contrário, todos os artigos citados pertencem ao Regulamento Geral de Proteção de Dados, doravante designado apenas por RGPD. Sobre os principais objetivos da reforma do Direito da Proteção de Dados, RÜCKER, Daniel, e KUGLER, Tobias, *New European General Data Protection Regulation*, Hart, Oxford, 2018, pp. 1-4.

[5] MENEZES CORDEIRO, António Barreto, "A Autonomia da Função de Encarregado de Proteção de Dados e a Independência do Exercício da Advocacia", *cit*., pág. 19. A proteção de dados pessoais, explica MIRANDA BARBOSA, Mafalda, "Proteção de Dados e Direitos de Personalidade", *Ab Instantia*, Ano V, n.º 7, Almedina, Coimbra, 2017, pág. 32, releva em vários planos para a tutela da pessoa humana: salvaguarda a identidade do sujeito, obviando à divulgação de dados que possam levar a uma usurpação ou à desvirtuação da verdade pessoal do sujeito; garante a não divulgação de elementos que poderão servir de base a comportamentos discriminatórios; defende a privacidade do sujeito. O direito à privacidade e à proteção de dados vêm incluídos respetivamente nos arts. 7.º e 8.º da Carta de Direitos Fundamentais da União Europeia. A inclusão desses direitos no catálogo de direitos fundamentais não significa que eles atribuam uma proteção ilimitada (RÜCKER, Daniel, e KUGLER, Tobias, *New European General Data Protection Regulation*, *cit*., pág. 5).

[6] TITO, Karenina Carvalho, "A Figura do Encarregado de Proteção de Dados no Regulamento Geral sobre a Proteção de Dados da União Europeia", *Revista Jurídica Luso-Brasileira*, Ano 7, n.º 4, 2021, pág. 993.

[7] LYNSKEY, Orla, *The Foundations of EU Data Protection Law*, Oxford University Press, Oxford, 2015, pp. 94-95.

[8] Cfr. *idem*, pp. 101-103.

encarar-se como um direito autónomo em vez de uma declinação do conteúdo de outro direito[9], é uma posição absolutamente protegida *ex vi* art. 483.º, n.º 1, do Código Civil[10]. A afetação desse direito constitui, portanto, o agente na prática de um facto ilícito.

3. Análise da responsabilidade aquiliana pelo tratamento desconforme de dados pessoais

3.1. O art. 82.º do RGPD e a sua sobreposição às estruturas internas de imputação delitual

O RGPD fornece-nos uma norma especial de responsabilidade civil extracontratual – de acordo com o art. 82.º, qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do RGPD tem direito a receber uma indemnização do responsável ou do subcontratante[11] pelos danos sofridos. Este preceito concretiza o princípio amplamente conhecido de que *ubi ius, ibi remedium*: havendo um direito à proteção e resguardo de dados pessoais, a sua afetação não pode deixar de constituir o agente em responsabilidade pelos danos provocados[12]. Nas palavras de ZANFIR-FORTUNA, "*data protection is a rather privileged field in that the Regulation that governs it specifically enshrines not only a general right to an effective judicial remedy, but also a specific right to receive compensation for the damage suffered as a result of a breach of the Regulation's provisions*"[13].

---

[9] Acerca desta posição, *idem*, pp. 103-104.

[10] MIRANDA BARBOSA, Mafalda, "Proteção de Dados e Direitos de Personalidade", *cit*., pp. 44-45.

[11] Acerca destes conceitos, MENEZES CORDEIRO, António Barreto, "Da Responsabilidade Civil pelo Tratamento de Dados Pessoais", *cit*., pp. 48-50, RÜCKER, Daniel, e KUGLER, Tobias, *New European General Data Protection Regulation*, *cit*., pp. 23 e ss., e MIRANDA BARBOSA, Mafalda, "Data Controllers e Data Processors", *Revista de Direito Comercial*, 2018, pp. 433 e ss..

[12] ZANFIR-FORTUNA, Gabriela, Anotação ao art. 82.º, *in* KUNER, Christopher, BYGRAVE, Lee A., e DOCKSEY, Christopher (coord.), *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford University Press, Oxford, 2020, pág. 1162.

[13] *Idem*, pág. 1163.

Nesta conformidade, eliminando qualquer discricionariedade dos Estados-Membros na implementação (ou não) de um direito indemnizatório pelo tratamento desconforme de dados pessoais, o supramencionado art. 82.º dispõe de eficácia imediata "*and creates an EU-wide individual cause of action for any person that feels wronged with regard to processing of personal data falling under the GDPR, to initiate remedial actions in civil courts*"[14]. Regressando à latitude do ordenamento luso, é certo que o surgimento do crédito indemnizatório sempre decorreria das regras gerais de responsabilidade aquiliana (arts. 483.º e ss., do Código Civil), verificado como o direito à proteção e não divulgação de dados pessoais consubstancia um direito absoluto. O art. 82.º, incorporado no nosso sistema *ex vi* a cláusula de receção do art. 8.º, n.º 4, da Constituição da República Portuguesa, deve ser visto como uma norma especial de responsabilidade civil extracontratual[15] que, dotada de força normativa superior, derroga potenciais normas internas que com ela conflituam[16]. Nos aspetos não regulados pelo art. 82.º serão subsidiariamente aplicáveis os preceitos gerais de responsabilidade civil.

3.2. A ilicitude

Retomando a análise do preceito do art. 82.º, verificamos que o cerne da ilicitude não reside propriamente na afetação de um direito absoluto, como sempre seria o direito ao adequado tratamento de dados

[14] *Idem*, pp. 1163-1164. No sentido de o art. 82.º atribuir diretamente uma causa de pedir para uma pretensão indemnizatória sem qualquer intermediação do Direito interno, KNETSCH, Jonas, "The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases", *European Journal of Privacy Law & Technologies*, Giappichelli, Torino, 2020, pág. 66.

[15] Em sentido próximo, ZANFIR-FORTUNA, Gabriela, Anotação ao art. 82.º, *cit*., pág. 1168.

[16] Assim sucedeu, por exemplo, na Alemanha, cuja Lei de Proteção de Dados não permitia uma indemnização por danos imateriais (*idem*, pág. 1175).

pessoais, mas antes na preterição das normas do RGPD[17]. Analisando cuidadosamente a letra da norma, e numa formulação que não se pode considerar acidental, a responsabilidade prevista no art. 82.º é, essencialmente, uma responsabilidade pela violação, não de direitos, mas de disposições destinadas a regular o tratamento de dados pessoais, as quais podem (e devem) ser configuradas como normas de proteção[18]. Seria ocioso uma excursão geral por esta modalidade de ilicitude. Apenas alguns aspetos merecem ser recordados: o conteúdo de ilicitude já não é matizado pela violação de um direito absoluto, mas pela quebra do comando previsto na norma de proteção[19]; o círculo de interesses protegidos ultrapassa aqueles atribuídos pelo mecanismo do direito absoluto, permitindo-se assim uma tutela de interesses puramente patrimoniais[20].

O aparente contraste entre o conteúdo do art. 82.º, n.ºs 1 e 2, tem sido destacado pela doutrina, porquanto da leitura do n.º 2 afigura-se *prima facie* que nem todas as violações do RGPD constituem o sujeito em responsabilidade civil, mas somente as que sejam cometidas na decorrência de tratamento de dados. Deve-se, porém, em sintonia com a lição de MENEZES CORDEIRO, adotar uma interpretação extensiva no sentido de o art. 82.º abranger "tratamentos ilícitos, bem como violações de direitos, de obrigações ou de proibições legais que estejam

---

[17] Defendendo uma interpretação extensiva, VOIGT, Paul, e VON DEM BUSSCHE, Axel, *The EU General Data Protection Regulation*, Springer, Cham, 2017, pág. 205, entendem que a noção de *infringement of the GDPR* deverá abarcar não só o RGPD propriamente dito, mas também as normas dos Estados-Membros concretizadoras dos princípios estipulados no RGPD ou presentes em atos delegados e de execução adotados nos termos do RGPD. Cfr., no mesmo sentido, MENEZES CORDEIRO, António Barreto, "Da Responsabilidade Civil pelo Tratamento de Dados Pessoais", *in* MIRANDA BARBOSA, Mafalda, ROSENVALD, Nelson, e MUNIZ, Francisco (coord.), *Novos Desafios de Responsabilidade Civil*, IJFDUC, Coimbra, 2019, pág. 42, e RÜCKER, Daniel, e KUGLER, Tobias, *New European General Data Protection Regulation*, *cit*., pág. 192.

[18] No sentido de as normas previstas no RGPD poderem ser encaradas enquanto disposições legais de proteção de interesses alheios, MIRANDA BARBOSA, Mafalda, "Proteção de Dados e Direitos de Personalidade", *cit*., pág. 45.

[19] MIRANDA BARBOSA, Mafalda, *Lições de Responsabilidade Civil*, Princípia, Cascais, 2017, pág. 173.

[20] *Idem*, pág. 171.

indiretamente relacionadas com as atividades desenvolvidas pelos responsáveis e pelos subcontratantes"[21]. Há ainda quem questione se, diante a formulação do art. 5.º, n.º 2, não se estabeleceu uma inversão do ónus de demonstração da desconformidade com o RGPD, alijando sobre o responsável pelo tratamento de dados a tarefa de provar que não cometeu nenhuma infração à legislação de proteção de dados, ou se, pelo contrário, a obrigação contida no art. 5.º, n.º 2, circunscreve-se apenas às relações entre o responsável e as autoridades de supervisão e não pode, como tal, ser manietada por um lesado em ação indemnizatória[22]. Afigura-se-nos ser esta última a melhor interpretação, já que de outra forma criar-se-ia uma injustificável distorção de regime entre a responsabilidade do responsável e a do subcontratante[23], o que minaria o sentido unificante do próprio art. 82.º.

3.3. A culpa (ou a sua desnecessidade). As causas de isenção de responsabilidade

Nem todos os sistemas de responsabilidade civil autonomizam a culpa da ilicitude. O legislador luso no encalço do homólogo alemão seguiu essa via, enunciando separadamente dois momentos de imputação delitual. Diverso é o sistema francês, em que a noção de *faute* absorve a ilicitude e a culpa[24]. A existência de diversos modelos de imputação explica as diferentes interpretações de que o art. 82.º tem sido objeto.

---

[21] MENEZES CORDEIRO, António Barreto, "Da Responsabilidade Civil pelo Tratamento de Dados Pessoais", *cit*., pág. 42.

[22] Cfr., com discussão, BAKHOUM, Mor et al., *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, Springer, Berlin, 2018, pp. 323-324.

[23] Isto porque, conforme entendimento pacífico, o disposto no art. 5.º, n.º 2, não se aplica ao subcontratante (cfr. NISSIM, Jenai, "Accountability and the Role of the Data Protection Officer", *in* CAREY, Peter, *Data Protection*, 5.a ed., Oxford University Press, Oxford, 2018, pág. 224).

[24] Acerca dos vários modelos de responsabilidade civil, MIRANDA BARBOSA, Mafalda, *Lições de Responsabilidade Civil*, *cit*., pp. 87 e ss..

Efetivamente, na literatura estrangeira entende-se que tal preceito dispensa de todo qualquer elemento de censurabilidade[25], encerrando assim uma disposição de responsabilidade objetiva – ou seja, bastaria a mera verificação de um processamento desconforme de dados para se gerar um crédito indemnizatório a favor do sujeito lesado na medida do dano sofrido.

Diversamente, MIRANDA BARBOSA esclarece que o RGPD limita-se a inverter o ónus de prova da culpa, presumindo a sua existência a partir do momento em que se constata a violação das obrigações impostas pela legislação de proteção de dados[26]. Tal inversão coaduna-se com algumas das implicações dogmáticas que a modalidade de ilicitude acolhida primariamente pelo art. 82.º – a violação de disposições legais de proteção – convoca. Constitui um lugar-comum na doutrina a posição de que as normas de proteção permitem uma antecipação do juízo da culpa, que passa a ter por referencial não a lesão de um direito absoluto, mas a violação do conteúdo prescritivo de uma norma. Como dificilmente se concebem causas de incumprimento não culposo (inexigibilidade) dessas determinações legais, admite-se genericamente uma inversão do ónus da prova da culpa[27].

Mesmo que não se admita sem mais uma inversão do *onus probandi*, atendendo à circunstância de o lesado geralmente não ter informação detalhada quanto ao modo de atuação ou à organização interna do responsável pelo tratamento de dados ou do subcontratante, deve-se reputar ser suficiente, para preencher tal ónus, uma "submissão plausível dos factos" (*plausible submission of the facts*), recaindo

---

25 ZANFIR-FORTUNA, Gabriela, Anotação ao art. 82.º, *cit*., pág. 1176.

26 MIRANDA BARBOSA, Mafalda, "Proteção de Dados e Direitos de Personalidade", *cit*., pág. 44; também da Autora, "Data Controllers e Data Processors", *cit*., pág. 432. No mesmo sentido, PIMENTA COELHO, Cristina, Anotação ao Art. 82.º, *in* SOUSA PINHEIRO, Alexandre (coord.), *Comentário ao Regulamento Geral de Proteção de Dados*, Almedina, Coimbra, 2018, pág. 636. Em sentido mais amplo, referindo haver uma dupla presunção de ilicitude e de culpa, MENEZES CORDEIRO, António Barreto, "Da Responsabilidade Civil pelo Tratamento de Dados Pessoais", *cit*., pág. 52.

27 Cfr. MIRANDA BARBOSA, Mafalda, *Lições de Responsabilidade Civil*, *cit*., pp. 175-178.

subsequentemente sobre o agente o ónus de afastar definitivamente tal primeira aparência de um juízo de censurabilidade[28].

O art. 82.º, n.º 3, prevê uma isenção de responsabilidade sempre que o responsável pelo tratamento de dados ou o subcontratante lograrem demonstrar não serem de alguma forma responsáveis pelo evento danoso. A disposição, na realidade, encerra uma simples logomaquia, já que a realizar-se tal demonstração é evidente que nunca nenhuma responsabilidade lhes poderia ser assacada. Em todo o caso, a doutrina tem sido particularmente exigente quanto ao circunstancialismo fáctico que possa determinar uma isenção de responsabilidade: "*even the smallest involvement in the event giving rise to the damage will give rise to liability*"[29]; "*involvement in the damaging act itself is not required*"[30]. Nem mesmo o acesso ilegítimo por terceiros a uma base de dados através de meios altamente sofisticados afasta automaticamente a responsabilidade do responsável pelo tratamento de dados ou do subcontratante, ainda que estes hajam observado escrupulosamente o RGPD.

Há quem entenda que uma atuação do subcontratante contrária ou fora do círculo de atribuições e funções dadas pelo responsável isenta este de qualquer responsabilidade pelos danos causados[31]. Cremos que não se deve ser tão perentório. O subcontratante apenas tem acesso aos dados pessoais porque o responsável, no contexto da relação contratual e/ou comercial que os une (cfr. art. 28.º, n.º 3), fornece-os. Ninguém assume o risco do dolo de outrem, mas uma condução negligente de dados pessoais da parte do subcontratante leva-nos a indagar de uma eventual *culpa in eligendo* do responsável pelo tratamento de dados.

---

28 VOIGT, Paul, e VON DEM BUSSCHE, Axel, *The EU General Data Protection Regulation*, *cit*., pág. 207.

29 *Idem*, pág. 208.

30 RÜCKER, Daniel, e KUGLER, Tobias, *New European General Data Protection Regulation*, *cit*., pág. 192.

31 ZANFIR-FORTUNA, Gabriela, Anotação ao art. 82.º, *cit*., pág. 1176.

3.4. O dano

Entre os danos passíveis de serem ressarcidos *ex vi* art. 82.º encontram-se, assim colocando termo à discórdia quanto à sua indemnizabilidade neste contexto[32], os danos morais (referidos no RGPD como "danos imateriais"), de que são exemplo os decorrentes de discriminação social, de *stress* psicológico ou da afetação do livre desenvolvimento da personalidade[33]. Atribuindo primazia à função preventiva da responsabilidade civil, o Tribunal de Justiça da União Europeia tem considerado que a indemnização arbitrada deverá ser generosa o suficiente para, indo além do imposto pelo princípio da integral reparação do dano[34], produzir um efeito de *deterrence*[35]; e que a indemnização apenas pode englobar uma função punitiva se o Direito nacional em concreto aplicável conhecer esse tipo de sanção para situações similares[36].

3.5. O nexo de causalidade

Em consonância com as regras gerais, a responsabilidade civil por violação das regras e princípios do RGPD depende do desvelar de um nexo de causalidade entre tal violação e os danos produzidos na esfera do lesado. O conceito de causalidade, enquanto categoria eivada de

---

[32] BAKHOUM, Mor et al., *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, *cit*., pág. 320.

[33] VOIGT, Paul, e VON DEM BUSSCHE, Axel, *The EU General Data Protection Regulation*, *cit*., pág. 205. Para exemplos de danos materiais e imateriais, MENEZES CORDEIRO, António Barreto, "Da Responsabilidade Civil pelo Tratamento de Dados Pessoais", *cit*., pp. 44-45.

[34] *Idem*, pág. 43, e KNETSCH, Jonas, "The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases", *cit*., pág. 67.

[35] VOIGT, Paul, e VON DEM BUSSCHE, Axel, *The EU General Data Protection Regulation*, *cit*., pp. 205-206.

[36] MENEZES CORDEIRO, António Barreto, "Da Responsabilidade Civil pelo Tratamento de Dados Pessoais", *cit*., pág. 44. Escusado será referir que o Direito português não admite os *punitive damages*: cfr., por todos, MIRANDA BARBOSA, Mafalda, *Lições de Responsabilidade Civil*, *cit*., pp. 54 e ss..

considerações ético-normativas[37], deverá ser interpretado em sentido lato de forma a dar-se provimento aos objetivos que o RGPD visa desempenhar[38].

3.6. Os titulares de crédito indemnizatório

Quanto à titularidade da pretensão indemnizatória, o art. 82.º, n.º 1, refere-se a "qualquer pessoa que tenha sofrido danos". O RGPD, embora poderia tê-lo feito, não restringe subjetivamente o crédito indemnizatório aos titulares dos dados pessoais que não foram geridos corretamente[39]. Terceiros de alguma forma prejudicados pelo tratamento desconforme de dados pessoais poderão peticionar uma indemnização nas condições estipuladas pelo art. 82.º. A circunstância de o art. 82.º, n.º 4, *in fine*, referir-se ao "fim de assegurar a efetiva indemnização *do titular dos dados*" (itálico nosso) deve ser encarada como uma formulação meramente acidental que não tem por efeito a restrição do escopo subjetivo desta norma[40].

Desta forma, poderão reclamar uma indemnização ao abrigo do art. 82.º quer os titulares de dados pessoais incorretamente processados como eventuais terceiros que hajam igualmente, por força desse tratamento desconforme, sofrido um prejuízo na sua esfera jurídica, uma vez verificado um nexo de causalidade adequada entre o dano sofrido por esses terceiros e a violação das normas de proteção de dados[41].

---

[37] Acerca da superação do nexo de causalidade enquanto mera questão-de-facto e a descoberta da sua intencionalidade normativa, *idem*, pp. 265 e ss..

[38] MENEZES CORDEIRO, António Barreto, "Da Responsabilidade Civil pelo Tratamento de Dados Pessoais", *cit*., pág. 45.

[39] Sobre as interpretações possíveis do art. 82.º, *idem*, pp. 46-48.

[40] Assim, BAKHOUM, Mor et al., *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, *cit*., oág. 322.

[41] VOIGT, Paul, e VON DEM BUSSCHE, Axel, *The EU General Data Protection Regulation*, *cit*., pág. 206.

Em princípio, as pessoas coletivas cairão fora da copa do art. 82.º[42]. Afigura-se-nos, contudo, que nada impede que estas sustentem a sua pretensão indemnizatória nas normas gerais de responsabilidade civil.

3.7. Os sujeitos responsáveis

O art. 82.º, diminuindo a importância da qualificação dos sujeitos envolvidos para efeitos de alocação do dano[43], delimita os agentes prevaricadores ao responsável pelo tratamento de dados e ao subcontratante. Outras entidades – inclusive o próprio encarregado de proteção de dados, doravante designado por EPD – que hajam atuado em desconformidade com as obrigações impostas pelo RGPD e/ou hajam preterido o direito absoluto à autodeterminação informacional, embora não possam ser acionados ao abrigo do art. 82.º, poderão sê-lo ao abrigo das normas internas de responsabilidade civil[44].

O art. 82.º, n.º 2, faz incidir sobre o responsável pelo tratamento de dados o dever de indemnizar desde que esteja envolvido num tratamento que viole o RGPD, nomeadamente pela preterição das "obrigações de cuidado" atualmente expressas no art. 24.º, n.º 1[45]. Como se densifica na doutrina, "[o] sistema não exige que o responsável assuma um

---

[42] MENEZES CORDEIRO, António Barreto, "Da Responsabilidade Civil pelo Tratamento de Dados Pessoais", *cit*., pág. 82, conquanto não defenda essa posição "em absoluto" e realce ser necessário analisar a *case law* que se produzirá para se poder aquilatar das vantagens e desvantagens da exclusão de pessoas coletivas do art. 82.º.

[43] BAKHOUM, Mor et al., *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, *cit*., pág. 320.

[44] MENEZES CORDEIRO, António Barreto, "Da Responsabilidade Civil pelo Tratamento de Dados Pessoais", *cit*., pág. 48. No mesmo sentido, refere MIRANDA BARBOSA, Mafalda, "Data Controllers e Data Processors", *cit*., pág. 485, que "[ainda] que o terceiro não esteja, em concreto, vinculado pelos deveres impostos pelos diversos preceitos do regulamento geral de proteção de dados, sempre haveremos que afirmar que ele pode ser responsabilizado, no quadro da responsabilidade extracontratual, por violação de direitos de natureza absoluta". Mas no sentido da exclusão da responsabilidade direta dos trabalhadores que estejam autorizados a tratar de dados pessoais, PIMENTA COELHO, Cristina, Anotação ao Art. 82.º, *cit*., pág. 635.

[45] Assim, o Acórdão do Tribunal da Relação de Lisboa de 08.07.2021, proc. n.º 174/20.4T8PDL.L1-6. Contudo, no aresto invocaram-se normas de Direito interno, como a violação do art. 486.º, n.º 1, do Código Civil, não se tendo sequer feito alusão ao art. 82.º.

papel nuclear na produção dos danos causados, nem sequer decisivo. Na prática, o responsável pelo tratamento poderá ser responsabilizado mesmo não tendo causado qualquer dano ao sujeito lesado. Assim, a transmissão lícita de dados para um terceiro que os processa de modo ilícito, bem como a receção de dados obtidos ilicitamente, sem o seu conhecimento diligente, podem sustentar a responsabilidade do responsável pelo tratamento"[46].

Por seu turno, o RGPD circunscreve a responsabilidade do subcontratante aos cenários de *(i)* violação de obrigações decorrentes do RGPD que lhe sejam especificamente dirigidas (cfr., nomeadamente, os arts. 28.º, 29.º, 32.º, 37.º e 38.º) e *(ii)* incumprimento das instruções lícitas recebidas por parte do responsável pelo tratamento de dados. Não sendo o subcontratante um autómato, ele não deverá seguir as instruções do responsável pelo tratamento de dados que configurem práticas atentatórias das obrigações específicas que sobre si incidem, sob pena de poder ser responsabilizado nos termos acima explanados[47]. Ademais, fora dos meandros do art. 82.º, não repugna que o contrato celebrado entre o responsável e o subcontratante tenha uma eficácia protetora do titular de dados pessoais[48], permitindo a este reclamar uma indemnização fundada na preterição de deveres laterais cujo regime se assimilará ao da responsabilidade contratual. A tal não obsta a possível indeterminabilidade do sujeito titular de dados pessoais, requisito esse – o da cognoscibilidade do círculo de terceiros reflexamente tutelados pelo contrato – que a doutrina e jurisprudência alemãs têm sapientemente superado[49] (como superado se encontra o vetusto requisito de que credor contratual e terceiro protegido devam perseguir o mesmo

[46] MENEZES CORDEIRO, António Barreto, "Da Responsabilidade Civil pelo Tratamento de Dados Pessoais", *cit*., pág. 50.

[47] *Idem*, pág. 51.

[48] Admite-o, por exemplo, MIRANDA BARBOSA, Mafalda, "Proteção de Dados e Direitos de Personalidade", *cit*., pp. 46-47.

[49] Mais que saber se o terceiro protegido encontra-se pessoalmente relacionado com o credor, importa aquilatar em que circunstâncias os interesses objetivos envolvidos permitem inferir que as partes contratuais implicitamente estipularam um *duty of care* perante terceiros (MARKESINIS, Basel, *German Law of Torts*, 4.a ed., Hart Publishing, Oxford/Portland/Oregon, pág. 63).

interesse[50]).

4. A responsabilidade contratual do responsável pelo tratamento de dados

O art. 82.º cuida de uma situação de responsabilidade extracontratual. Contudo, a operacionalidade de uma responsabilidade fundada no incumprimento contratual, a determinar à luz das disposições de Direito interno[51], não deve ser imediatamente arredada. Se bem que o direito à proteção de dados mereça autonomamente a chancela a tutela aquiliana, não se pode excluir os casos, frequentes, em que o tratamento desconforme de dados pessoais consubstancia um incumprimento das obrigações emergentes de uma relação contratual entretecida com o titular desses dados[52] ou, ainda, uma inobservância dos deveres laterais de proteção que a relação obrigacional complexa convoca (art. 762.º, n.º 2, do Código Civil)[53].

Em tais cenários verifica-se um concurso objetivo de fontes de

---

[50] BASEDOW, Jürgen, e WURMNEST, Wolfgang, *Third-Party Liability of Classification Societies*, Springer, Berlin/Heidelberg, 2005, pp. 48-49.

[51] No sentido de o art. 82.º não excluir a intervenção de normas internas de responsabilidade civil, VOIGT, Paul, e VON DEM BUSSCHE, Axel, *The EU General Data Protection Regulation*, *cit*., pág. 206.

[52] RÜCKER, Daniel, e KUGLER, Tobias, *New European General Data Protection Regulation*, *cit*., pág. 193.

[53] Nesta hipótese de preterição de deveres acessórios de conduta, a responsabilidade situar-se-á numa terceira via entre o polo aquiliano e obrigacional, embora com tendencial assimilação ao regime desta (MIRANDA BARBOSA, Mafalda, "Proteção de Dados e Direitos de Personalidade", *cit*., pág. 46), aplicando-se-lhe nomeadamente o princípio da ressarcibilidade dos danos puramente patrimoniais, a regra da inversão do ónus da prova da culpa (art. 799.º, n.º 1, do Código Civil) e a regra da responsabilidade por atos de auxiliares (art. 800.º do Código Civil); assim, PINTO OLIVEIRA, Nuno Manuel, "Tópicos sobre a Distinção entre a Responsabilidade Contratual e a Responsabilidade Extracontratual", *in* AA.VV., *Estudos em Comemoração dos 20 Anos da Escola de Direito da Universidade do Minho*, Coimbra Editora, Coimbra, 2014, pág. 526. Cfr., por todos, MOTA PINTO, Carlos Alberto, *Cessão da Posição Contratual*, reimp., Almedina, Coimbra, 2003, pp. 337 e ss., e CARNEIRO DA FRADA, Manuel A., *Contrato e Deveres de Protecção*, Coimbra Editora, Coimbra, 1994, pp. 155 e ss..

responsabilidade civil, já que a lesão perpetrada é subsumível tanto aos antros do inadimplemento como do delito. Tal concurso, conforme o entendimento que nos parece acertado[54], deverá ser resolvido através da consunção da responsabilidade aquiliana, conjunto de normas aplicáveis ao indiferenciado contacto social, pela responsabilidade obrigacional, teleologicamente orientada a disciplinar o fenómeno imputacional ocorrido no contexto de uma relação contratual. Esta posição implica, verdadeiramente, que o art. 82.º só se aplique onde não se possa divisar uma responsabilidade pelo incumprimento contratual.

5. A responsabilidade civil do Encarregado de Proteção de Dados.

5.1. Caracterização geral

Em termos sinópticos, pode-se entender por EPD a pessoa (singular ou coletiva) nomeada pelo responsável pelo tratamento de dados ou pelo subcontratante para, no âmbito da sua atividade, desenvolver funções de fiscalização e de *compliance*, assegurando a conformidade da atuação daquelas entidades com as regras e princípios plasmados no RGPD. Embora a génese do EPD remonte à Diretiva n.º 95/46/CE, de 25 de Outubro, é o RGPD que, nas condições contempladas pelo seu

[54] ALMEIDA COSTA, Mário Júlio, *Direito das Obrigações*, 12.a ed., Almedina, Coimbra, 2009, pp. 552-553. Diversamente, considerando que pela celebração de um contrato as partes não pretenderam a renúncia à tutela geral e, como tal, o lesado poderá livremente optar (e não construir um regime híbrido, como pretende, atendendo à "intencionalidade problemática" do caso, MIRANDA BARBOSA, Mafalda, *Lições de Responsabilidade Civil*, *cit*., pág. 20) entre as duas espécies de responsabilidade, ÁLVARO DIAS, João, *Procriação Assistida e Responsabilidade Civil*, Coimbra Editora, Coimbra, 1996, pp. 228 e ss., e GRAÇA TRIGO, Maria, *Responsabilidade Civil Delitual por Facto de Terceiro*, Coimbra Editora, Coimbra, 2009, pág. 26. Em Itália, no sentido da solução da livre escolha de responsabilidades, cfr. SALVI, Cesare, *La Responsabilità Civile*, 2.a ed., Giuffrè, Milano, 2005, pp. 13-14, e SCHLESINGER, Piero, e TORRENTE, Andrea, *Manuale di Diritto Privato*, 24.a ed., Giuffrè, Milano, 2019, pp. 960-961.

art. 37.º, obriga à sua designação[55]. Mesmo fora dessas hipóteses de designação obrigatória, o EPD pode ser nomeadamente voluntariamente[56], nada justificando, por conseguinte, qualquer diversidade de estatuto (e, ao que nos importa) de responsabilidade[57].

Uma vez verificadas quaisquer das situações elencadas no art. 37.º, n.º 1[58], surge na esfera jurídica do responsável pelo tratamento de dados ou do subcontratante a obrigação de designação de um EPD. Tal obrigação, incidindo autonomamente sobre cada uma das referidas entidades[59], não carece de qualquer estímulo exterior, nomeadamente da parte das autoridades de supervisão[60], devendo ser imediatamente observada. A escolha do EPD poderá coenvolver uma culpar *in elegindo* do responsável ou do subcontratante, sempre que aquele não desempenhar as suas funções com a diligência e zelo devidos. Tal responsabilidade será uma mera consequência do princípio da autorregulação em

---

[55] Sobre a evolução histórica da figura, MENEZES CORDEIRO, António Barreto, "A Autonomia da Função de Encarregado de Proteção de Dados e a Independência do Exercício da Advocacia", *cit*., pp. 20-22. Antes do RGPD, a obrigatoriedade de designação de um EPD encontrava-se na Lei de Proteção de Dados alemã (VOIGT, Paul, e VON DEM BUSSCHE, Axel, *The EU General Data Protection Regulation*, *cit*., pág. 53).

[56] MENEZES CORDEIRO, António Barreto, "A Autonomia da Função de Encarregado de Proteção de Dados e a Independência do Exercício da Advocacia", *cit*., pág. 23.

[57] Explicam VOIGT, Paul, e VON DEM BUSSCHE, Axel, *The EU General Data Protection Regulation*, *cit*., pág. 56, que "*the voluntary DPO will have to comply with the regulations of the GDPR and assume all statutory responsibilities of this position*". Ainda no sentido da equiparação geral de estatuto entre o EPD de nomeação obrigatória e de nomeação facultativa, ROCHA ANDRADE, Rodrigo, "Da Responsabilidade do Encarregado de Proteção de Dados", *Fórum de Proteção de Dados*, n.º 7, 2020, pág. 29, nota 15.

[58] Cfr., por todos, RÜCKER, Daniel, e KUGLER, Tobias, *New European General Data Protection Regulation*, *cit*., pp. 175 e ss..

[59] SZAŁOWSKI, Ryszard, "Data Protection Officer in the Light on the Provisions of the General Data Protection Regulation", *Ius Novum*, n.º 4, 2018, pág. 116, RÜCKER, Daniel, e KUGLER, Tobias, *New European General Data Protection Regulation*, *cit*., pág. 175, e PEREIRA DUARTE, Diogo, Anotação ao Art. 37.º, *in* MENEZES CORDEIRO, António Barreto (coord.), *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, Almedina, Coimbra, 2021, pág. 292.

[60] MENEZES CORDEIRO, António Barreto, "A Autonomia da Função de Encarregado de Proteção de Dados e a Independência do Exercício da Advocacia", *cit*., pág. 23.

matéria de proteção de dados[61], de que é também declinação a obrigatoriedade de o responsável pelo tratamento de dados implementar as medidas técnicas e organizacionais destinadas a assegurar a *compliance* com o RGPD.

O art. 37.º, n.º 5, configura o EPD como um profissional qualificadíssimo, dotado de conhecimentos especializados no domínio do Direito e da proteção de dados[62] (isto muito embora o RGPD, numa solução a carecer de revisão, não imponha que o EPD seja um licenciado em Direito[63]). Importará também que o EPD, atento o significado das funções que desempenha – a principal das quais é assegurar o cumprimento das regras e princípios previstos no RGPD[64] – e da sua instrumentalização à tutela de direitos de personalidade, apresente integridade pessoal e profissional[65]. Caso o EPD nomeado não se assimilar, à data da sua designação, ao padrão gizado pelo legislador, ficando aquém dele, tal desconformidade será tida em consideração para se aferir da eventual responsabilidade da entidade que o designou.

---

[61] Mencionando que o RGPD atribui aos responsáveis e subcontratantes a "*responsabilidade* de autorregularem as suas actividades", *idem*, pág. 31. Também assim, no sentido da consagração de um "princípio de autorresponsabilização dos Responsáveis pelo Tratamento e do Subcontratantes", ROCHA ANDRADE, Rodrigo, "Da Responsabilidade do Encarregado de Proteção de Dados", *cit*., pp. 25-26. Cfr., ainda, MUIÀ, Pier Paolo, *Il Nuovo Codice della Privacy*, Maggioli, Santarcangelo di Romagna, 2019, pp. 47-48.

[62] TITO, Karenina Carvalho, "A Figura do Encarregado de Proteção de Dados no Regulamento Geral sobre a Proteção de Dados da União Europeia", *cit*., pp. 1004-1005.

[63] SZAŁOWSKI, Ryszard, "Data Protection Officer in the Light on the Provisions of the General Data Protection Regulation", *cit*., pág. 125, e PEREIRA DUARTE, Diogo, Anotação ao Art. 37.º, *cit*., pág. 293.

[64] TITO, Karenina Carvalho, "A Figura do Encarregado de Proteção de Dados no Regulamento Geral sobre a Proteção de Dados da União Europeia", *cit*., pág. 1009.

[65] MENEZES CORDEIRO, António Barreto, "A Autonomia da Função de Encarregado de Proteção de Dados e a Independência do Exercício da Advocacia", *cit*., pág. 28, e NISSIM, Jenai, "Accountability and the Role of the Data Protection Officer", *cit*., pág. 233. Cfr., ainda, VOIGT, Paul, e VON DEM BUSSCHE, Axel, *The EU General Data Protection Regulation*, *cit*., pp. 56-57.

5.2. O EPD como comissário. O problema da relação de comissão

O art. 37.º, n.º 6, do RGPD, refere que o EPD pode integrar ou não a estrutura interna do responsável ou do subcontratante: quer dizer, pode desempenhar as suas funções com base num contrato de trabalho subordinado ou num contrato de prestação de serviços[66]. A morfologia desse vínculo tem implicações ao nível da responsabilidade civil. Caso o EPD for um trabalhador interno do responsável pelo tratamento de dados ou do subcontratante, e na medida em que a relação de trabalho subordinado encerra uma relação de comissão (cfr. art. 1152.º do Código Civil)[67], estes – a título extracontratual – responderão objetivamente na qualidade de comitente pelos atos por aquele praticados (art. 500.º do Código Civil)[68].

A circunstância da função de EPD se caracterizar "por uma marcada independência em face das entidades designadoras"[69], de que é corolário a proibição de os responsáveis e subcontratantes instruírem o EPD no exercício das suas funções (art. 38.º, n.º 3), não preclude a

---

[66] VOIGT, Paul, e VON DEM BUSSCHE, Axel, *The EU General Data Protection Regulation*, *cit*., pág. 57, e PEREIRA DUARTE, Diogo, Anotação ao Art. 37.º, *cit*., pág. 294.

[67] GRAÇA TRIGO, Maria, Anotação ao Art. 500.º, *in* BRANDÃO PROENÇA, José Carlos (coord.), *Comentário ao Código Civil. Direito das Obrigações. Das Obrigações em Geral*, Universidade Católica Editora, Lisboa, 2018, pág. 386, embora com a advertência de que a noção de subordinação para efeitos do art. 500.º do Código excede a de subordinação jurídica para efeitos de uma relação de trabalho, e ALMEIDA COSTA, Mário Júlio, *Direito das Obrigações*, *cit*., pág. 617. No Direito francês, em igual sentido, TERRÉ, François, e SIMLER, Philippe, *Droit Civil. Les Obligations*, 12.a ed., Dalloz, Paris, 2019, pp. 1126-1127.

[68] No sentido de que a independência do EPD não obvia a que este se encontre sob a direção da entidade nomeadora, donde surgirá uma relação de comissão, ROCHA ANDRADE, Rodrigo, "Da Responsabilidade do Encarregado de Proteção de Dados", *cit*., pp. 37-38. Bem assim, para ALVAREZ RIGAUDIAS, Cecilia, e SPINA, Alessandro, Anotação ao Art. 38.º, *in* KUNER, Christopher, BYGRAVE, Lee A., e DOCKSEY, Christopher (coord.), *The EU General Data Protection Regulation (GDPR). A Commentary*, *cit*., pág. 707, o facto de ser sobre o responsável pelo tratamento de dados que recai a obrigação de demonstrar a conformidade com o RGPD não isenta o EPD da sua responsabilidade enquanto "*employee or contractor of the controller or processor, as in the case of any other employee or contractor*".

[69] MENEZES CORDEIRO, António Barreto, "A Autonomia da Função de Encarregado de Proteção de Dados e a Independência do Exercício da Advocacia", *cit*., pág. 30.

eventual verificação de uma relação de comissão[70] e a subsequente responsabilidade da entidade que o nomeou. Admiti-lo seria esvaziar de sentido as cautelas que o RGPD estabelece quanto às qualidades profissionais e pessoais do EPD. A independência do EPD visa apenas assegurar que realize a sua fiscalização de forma livre e isenta[71], prevenindo que seja influenciado negativamente pelo responsável ou subcontratante[72]. De resto, e sem prejuízo das demais especificidades do seu estatuto, o EPD interno encontra-se sob a direção e autoridade da entidade que o designa. Aliás, veja-se que é condição do cabal cumprimento das funções cometidas ao EPD que este integre a estrutura e o organograma da entidade que o designou – em suma, que participe como agente ativo no *decision making*. O próprio EPD, importa notar, não tem quaisquer posições de fiscalização sobre a entidade que o designa[73], nem muito menos dispõe autonomamente de poderes decisórios[74], exercendo antes uma tarefa de aconselhamento. Como se observa em anotação ao art. 38.º, "[*it*] *would appear that the DPO does not exercise a form of power independently from the organization in which the DPO is embedded but rather a form of expert-based autonomy, adequately supported by relevant norms of professional conduct*"[75].

---

[70] Em sentido contrário, MIRANDA BARBOSA, Mafalda, "Data Controllers e Data Processors", *cit*., pp. 469-470.

[71] TITO, Karenina Carvalho, "A Figura do Encarregado de Proteção de Dados no Regulamento Geral sobre a Proteção de Dados da União Europeia", *cit*., pág. 1007.

[72] VOIGT, Paul, e VON DEM BUSSCHE, Axel, *The EU General Data Protection Regulation*, *cit*., pág. 59. Ainda acerca da independência do EPD, NISSIM, Jenai, "Accountability and the Role of the Data Protection Officer", *cit*., pág. 236.

[73] ALVAREZ RIGAUDIAS, Cecilia, e SPINA, Alessandro, Anotação ao Art. 38.º, *cit*., pág. 703.

[74] ROCHA ANDRADE, Rodrigo, "Da Responsabilidade do Encarregado de Proteção de Dados", *cit*., pág. 27, e PEREIRA DUARTE, Diogo, Anotação ao Art. 37.º, *cit*., pág. 297.

[75] ALVAREZ RIGAUDIAS, Cecilia, e SPINA, Alessandro, Anotação ao Art. 38.º, *cit*., pág. 703.

5.3. Em torno da responsabilidade autónoma do EPD

Um perscrutar pela literatura repetidamente encontra a afirmação de que o EPD não é pessoalmente responsável em caso de incumprimento das regras de proteção de dados[76], porquanto o sujeito obrigado à sua observância é o responsável pelo tratamento de dados (art. 24.º, n.º 1)[77]. Tal afirmação não só é consentânea com o entendimento pugnado pelo Grupo de Trabalho[78] como parece impor-se mercê do art. 38.º, n.º 3. Sucede que, para além de o Grupo de Trabalho não emitir interpretações vinculativas, a referida norma não pode ser interpretada no sentido de conferir uma espécie de imunidade ao EPD; e pelas seguintes razões: "*Firstly, the limitation to the possibility of dismissing or penalising is to be applicable only to the performance of his tasks. Thus, penalisation or dismissal is possible if the DPO does not fulfil the tasks. Secondly, the issue of limitation concerns the controller or the processor and does not cover potential rights of an entity that the EU legislator refers to as the highest management level. If the head of a unit is also the controller, they may undertake steps against the DPO within the performance of a managerial function. Thirdly, the provision cannot be treated as a mechanism ensuring a lack of criminal, disciplinary or civil liability*"[79].

---

[76] *Vide*, por exemplo, TITO, Karenina Carvalho, "A Figura do Encarregado de Proteção de Dados no Regulamento Geral sobre a Proteção de Dados da União Europeia", *cit*., pág. 1003, PIMENTA COELHO, Cristina, Anotação ao Art. 82.º, *cit*., pág. 634, PEREIRA DUARTE, Diogo, Anotação ao Art. 38.º, *cit*., pág. 298, e RÜCKER, Daniel, e KUGLER, Tobias, *New European General Data Protection Regulation*, *cit*., pág. 182.

[77] No sentido de que é o responsável pelo tratamento de dados que tem a "*main responsibility and liability for data protection complicance*", *idem*, pág. 24. Referindo-se ao responsável como o "principal centro de imputação", RODRIGUES ROCHA, Francisco, Anotação ao Art. 24.º, *in* MENEZES CORDEIRO, António Barreto (coord.), *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, *cit*., pág. 234.

[78] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Orientações sobre os Encarregados de Proteção de Dados (EPD)*, 2016 (última redação revista e adotado a 05 de abril de 2017), pág. 28.

[79] SZAŁOWSKI, Ryszard, "Data Protection Officer in the Light on the Provisions of the General Data Protection Regulation", *cit*., pág. 124.

Não se coloca em causa que o RGPD é completamente omisso quanto à responsabilidade pessoal do EPD[80]; mas esta mera omissão (que nada obsta à aplicação dos princípios gerais) não permite concluir pelo que seja[81]. Se não se pode aceder à responsabilidade do EPD *ex vi* art. 82.º, norma que se dirige apenas ao responsável pelo tratamento de dados e ao subcontratante, nada nos impede de chamarmos à colação as normas internas de responsabilidade civil, cuja aplicabilidade já verificamos não ser arredada.

A responsabilidade do EPD será apenas a outra parcela do binómio da importância e relevância das funções que desempenha, sem a qual o ligame com um princípio de liberdade eticamente conformada romper-se-ia. O estatuto do EPD é balizado por um padrão de diligência acrescida, devendo este conduzir a sua função de *compliance*[82] e de *awareness-raising*[83] de forma particularmente zelosa e diligente. Ora, no encalço de MIRANDA BARBOSA, "ao assumir as suas funções, [o EPD] assume concomitantemente uma esfera de risco"[84]. Seria francamente um convite à incúria fornecer ao EPD uma égide contra quaisquer ações de responsabilidade civil a pretexto da salvaguarda da sua independência e autonomia. Com efeito, "o papel do EPD só faz sentido se for, pelo menos em alguma medida, responsabilizador do próprio e responsabilizador do próprio perante todos os que devem beneficiar da sua diligente atuação"[85]. A circunstância de o EPD desempenhar um papel de

---

[80] ALVAREZ RIGAUDIAS, Cecilia, e SPINA, Alessandro, Anotação ao Art. 38.º, *cit*., pág. 707.

[81] Conforme a observação de ROCHA ANDRADE, Rodrigo, "Da Responsabilidade do Encarregado de Proteção de Dados", *cit*., pág. 34, o legislador cuidou apenas da responsabilidade civil do responsável e do subcontratante, "não prevendo nem a responsabilidade nem a irresponsabilidade de terceiros, como o EPD".

[82] No sentido de que o RGPD considera o EPD como um "*cornerstone of the accountability principle*", ALVAREZ RIGAUDIAS, Cecilia, e SPINA, Alessandro, Anotação ao Art. 38.º, *cit*., pág. 701.

[83] RÜCKER, Daniel, e KUGLER, Tobias, *New European General Data Protection Regulation*, *cit*., pág. 185.

[84] MIRANDA BARBOSA, Mafalda, "Data Controllers e Data Processors", *cit*., pág. 470.

[85] ROCHA ANDRADE, Rodrigo, "Da Responsabilidade do Encarregado de Proteção de Dados", *cit*., pág. 32.

conselheiro (*role as an advisor*)[86] e uma "função consultiva e de monitorização"[87] não o deverá exonerar de qualquer responsabilidade (a tal não obsta, como veremos, o art. 485.º do Código Civil), a qual deverá ser aquilatada – na ausência de uma norma específica no RGPD – por referência às estruturas de imputação presentes nas legislações internas[88].

5.4. A responsabilidade contratual e extracontratual do EPD

A responsabilidade civil do EPD deve ser analisada em dois planos: perante a entidade que o designou e perante terceiros. A primeira – é óbvio – assumirá a fisionomia de uma responsabilidade obrigacional (art. 798.º do Código Civil), com determinadas particularidades caso o EPD for um trabalhador subordinado (art. 323.º do Código do Trabalho). A esta responsabilidade não obsta a norma do art. 38.º, n.º 3, que apenas fornece uma imunidade ao EPD pela correta ou cabal prossecução das suas funções ("*protection against unfair dismissal*"[89]). O EPD pode ser responsabilizado ou destituído caso não desempenhar cabalmente as suas funções, ou seja, caso incumprir ou cumprir defeituosamente as suas obrigações[90]. São concebíveis várias situações de responsabilidade *ex contractu* do EPD, como a recusa em dar pareceres ou em providenciar por ações de formação e sensibilização[91].

---

[86] VOIGT, Paul, e VON DEM BUSSCHE, Axel, *The EU General Data Protection Regulation*, *cit*., pág. 62.

[87] ROCHA ANDRADE, Rodrigo, "Da Responsabilidade do Encarregado de Proteção de Dados", *cit*., pág. 27.

[88] Como referem VOIGT, Paul, e VON DEM BUSSCHE, Axel, *The EU General Data Protection Regulation*, *cit*., pág. 62, "*the DPO is generally responsible for fulfilling its tasks properly. Therefore, based on EU Member State legislation, data subjects or the controller/processor might be able to claim compensation for damages resulting from a breach of the DPO's obligations. Inter alia, national legislation might enable entities to claim compensation based on their employment relationship with the DPO*". No sentido da aplicação ao EPD do regime geral de responsabilidade civil, ROCHA ANDRADE, Rodrigo, "Da Responsabilidade do Encarregado de Proteção de Dados", *cit*., pág. 35.

[89] RÜCKER, Daniel, e KUGLER, Tobias, *New European General Data Protection Regulation*, *cit*., pág. 182.

[90] PIMENTA COELHO, Cristina, Anotação ao Art. 38.º, *cit*., pp. 475-476.

[91] ROCHA ANDRADE, Rodrigo, "Da Responsabilidade do Encarregado de Proteção de Dados", *cit*., pág. 33.

Deve-se, contudo, assinalar que, na medida em que o EPD não dispõe de poderes decisórios, não lhe pode ser exigido que assuma o encargo de garantir a conformidade com a legislação de proteção de dados. As suas obrigações esgotam-se apenas no adequado aconselhamento, recaindo sobre o responsável pelo tratamento de dados ou o subcontratante a escolha de se guiarem ou não pelas advertências feitas pelo EPD[92]. Verificando-se um ilícito contratual, o EPD será chamado a responder pelos danos causados à entidade que o designou (e consequente credora contratual), abarcando a dupla fenomenologia de lucros cessantes e danos emergentes.

Diante terceiros, a responsabilidade do EPD encontrar-se-á, *prima facie*, nos mastros comuns dos arts. 483.º e ss., do Código Civil. A ilicitude da sua conduta decorrerá primariamente da preterição das obrigações que o RGPD lhe impõe[93], as quais podem ser perfiladas, para efeitos do art. 483.º, n.º 1, 2.ª parte, do Código Civil, como disposições legais de proteção. Em todo o caso, os interesses por si ofendidos regra geral consistirão em vantagens atribuídas através de um direito subjetivo absoluto.

Porquanto a atividade do EPD consiste sobretudo na emissão de conselhos e recomendações, importa superar o obstáculo edificado pelo art. 485.º do Código Civil. Tal disposição, como a homóloga alemã, apenas tem em vista clarificar que a mera solicitação e prestação de informações não encerra nenhum contrato tácito nem responsabiliza

[92] Embora tal dicotomia seja atualmente objeto de crítica pela doutrina, pode-se ainda assim afirmar *grosso modo* que o EPD assume uma obrigação de meios e não de resultados (ROCHA ANDRADE, Rodrigo, "Da Responsabilidade do Encarregado de Proteção de Dados", *cit*., pág. 33). Consequentemente, não se pode aplicar, sem mais, a presunção de culpa prevista no art. 799.º, n.º 1, do Código Civil, a qual se encontra apenas gizada para os casos em que o devedor assegurou a verificação de um determinado resultado (cfr. CARNEIRO DA FRADA, Manuel A., *Direito Civil – Responsabilidade Civil*, reimp., Almedina, Coimbra, 2010, pág. 81).

[93] Assim sucederá, partindo dos exemplos de ROCHA ANDRADE, Rodrigo, "Da Responsabilidade do Encarregado de Proteção de Dados", *cit*., pág. 37, caso o EPD não informe ou aconselhe mal o responsável, o subcontratante e seus colaboradores, não monitorize devidamente a conformidade da atividade da entidade nomeadora com a legislação de proteção de dados ou não cumpra a sua obrigação de cooperação com a autoridade de controlo.

sem mais o emitente pela inexatidão da informação por si prestada[94]. O seu conteúdo normativo é, na realidade, bastante exíguo, ao consistir essencialmente numa remissão para outras normas. Importa então questionar: assistia ao EPD o "dever jurídico de dar o conselho, recomendação ou informação"? Tal dever existe perante a entidade que o designa, mercê da relação contratual que com ela entreteceu; mas, por força do princípio da relatividade (art. 406.º, n.º 2, do Código Civil), o titular dos dados pessoais, terceiro perante tal relação, não pode exigir do EPD o cumprimento desse dever ou reclamar uma indemnização pelo seu inadimplemento. Isto não obvia a que possamos considerar que o contrato entre o EPD e a entidade que o designa tem uma eficácia protetora do titular dos dados pessoais, já que a sua execução se dirige, essencialmente, à proteção dos interesses materiais e imateriais deste. A eficácia protetora desse contrato estende-se reflexamente ao titular de dados pessoais, que poderá assim reclamar do EPD uma indemnização pela prestação de conselhos ou recomendações faltosos que originaram um tratamento desconforme e danoso de dados pessoais.

Por outro lado, como se sabe, o art. 485.º do Código Civil não esgota a possibilidade de intervenção das regras gerais de Direito, como a proibição do abuso do direito[95], pelo que sempre será possível aceder à responsabilidade delitual do EPD se o seu comportamento representar uma ofensa clamorosa do mínimo ético-jurídico (art. 334.º do Código Civil): assim sucederá, apoditicamente, quando agir com dolo (caso em que a sua responsabilidade se impõe por respeito ao *neminem laedere*) ou, quando muito, houver negligenciado gravemente as suas obrigações legais e estatutárias[96].

---

[94] SINDE MONTEIRO, Jorge, *Responsabilidade por Conselhos, Informações e Recomendações*, Almedina, Coimbra, 1989, pp. 449 e ss..

[95] CARNEIRO DA FRADA, Manuel A., *Uma «Terceira Via» no Direito da Responsabilidade Civil?*, Almedina, Coimbra, 1997, pág. 72.

[96] Cfr. SINDE MONTEIRO, Jorge, "Responsabilidade Delitual. Da Ilicitude", *in* AA.VV., *Comemorações dos 35 Anos do Código Civil e dos 25 Anos da Reforma de 1977*, Vol. III, Coimbra Editora, Coimbra, 2007, pág. 463.

5.5. Aspetos avulsos da responsabilidade civil do EPD. A *culpa in elegindo* da entidade que o designa

Em nota de encerramento, deve-se referir que raramente o EPD será chamado a responder isoladamente pelos danos causados pelo tratamento desconforme de dados pessoais. Um desempenho deficitário do EPD das suas funções em princípio resultará numa atuação do responsável pelo tratamento de dados ou do subcontratante desconforme com o RGPD, donde decorrerá a responsabilidade destes por via do art. 82.º. Por conseguinte, em conformidade com a regra do art. 497.º, do Código Civil, os sujeitos envolvidos na lesão responderão solidariamente[97]. Tal asserção leva-nos, no entanto, como *prius* lógico, a justificar a responsabilidade da entidade designadora pelos atos praticados pelo EPD.

Tratando-se de um EPD interno, em relação de trabalho subordinado, essa responsabilidade já vimos decorrer do art. 500.º do Código Civil. Mas, mesmo quando o EPD for um órgão externo à entidade que o designa, assentando o seu ligame contratual numa prestação de serviços que, por sua natureza, inviabiliza uma relação de comissão, não se pode olvidar a *culpa in elegindo* da entidade que o nomeou. Raros serão os casos em que, por hipótese, o responsável pelo tratamento de dados ou o subcontratante poderão eximir-se da sua responsabilidade invocando, ao abrigo do art. 82.º, n.º 3, que "o facto que causou o dano não lhe é imputável". Na realidade, a entidade em causa, quer se encontre legalmente vinculada à nomeação de um EPD ou o faça voluntariamente, assume o risco inerente à designação, ainda que por via de um contrato de prestação de serviços, de um EPD inábil ou negligente[98].

Sucede ainda que, podendo a *causa petendi* da ação indemnizatória sustentar-se não no ilícito aquiliano previsto no art. 82.º, mas no

---

[97] *Vide* ROCHA ANDRADE, Rodrigo, "Da Responsabilidade do Encarregado de Proteção de Dados", *cit*., pág. 37.

[98] Em sentido não inteiramente coincidente, excluindo a responsabilidade do responsável pelo tratamento de dados sempre que este "teve cuidado em escolher um EPD que prestava garantias de competência", *idem*, pág. 36.

incumprimento do programa contratual acordado entre o responsável pelo tratamento de dados e o titular de dados pessoais ou na inobservância dos deveres laterais que a relação obrigacional congrega (art. 762.º, n.º 2, do Código Civil), o art. 800.º do Código Civil – que prescinde tanto da relação de comissão[99] como de uma dupla imputação – projetará diretamente sobre a esfera do responsável pelo tratamento de dados os atos praticados pelo EPD, como se tivesse sido aquela entidade a os praticar[100].

[99] Exige-se apenas uma "*relação específica entre o devedor e o terceiro utilizado no cumprimento*" (GRAÇA TRIGO, Maria, *Responsabilidade Civil Delitual por Facto de Terceiro*, Coimbra Editora, Coimbra, 2009, pp. 242 e ss.), mesmo na ausência de qualquer subordinação, através da qual esse terceiro amplie o raio de atividade do devedor, auxiliando-o ou coadjuvando-o no cumprimento das suas obrigações contratuais.

[100] Sobre a contraposição entre os arts. 500.º e 800.º do Código Civil, por todos, MIRANDA BARBOSA, Mafalda, *Lições de Responsabilidade Civil*, *cit*., pp. 429 e ss..

O teste de ponderação 4.0 da lei geral de proteção de dados no brasil: análise do LIA (*legitimate interests assessment*) como uma inovação na eficácia horizontal dos direitos fundamentais

Francisco Soares Reis Júnior[1]

Resumo: A Lei Geral de Proteção de Dados representa um marco jurídico de equalização entre os direitos da privacidade dos titulares de dados e da liberdade econômica do mercado. Como tal, revela-se como uma norma que regula a eficácia dos direitos fundamentais entre particulares. Para a base legal do Legítimo Interesse, instituiu-se um regime de controle de validade através de um teste de ponderação, com mais requisitos do que o método criado por Robert Alexy. Este artigo sustenta a hipótese de que esse instituto representa uma inovação na proteção de direitos fundamentais e aprofunda o ônus argumentativo ao poder judiciário quando acionado.

Palavras-chave: *Eficácia horizontal de direitos fundamentais. Lei Geral de Proteção de Dados. Legítimo Interesse. Teste de Ponderação.*

Abstract: The General Data Protection Law represents a legal framework for equalizing the privacy rights of data subjects and the economic freedom of the market. As such, it appears as a norm that regulates the effectiveness of fundamental rights between individuals. For the legal

[1] Mestre em Ciência Política pela UFPI e Doutorando no Programa de Pós-Graduação em Direito da Universidade do Oeste de Santa Catarina/Brasil, e-mail: franciscotjma@gmail.com. Este paper foi originalmente concebido como trabalho para avaliação final no âmbito da disciplina de Direitos Fundamentais e Direito Privado no Doutorado.

basis of Legitimate Interest, a validity control regime was instituted through a weighting test, with more requirements than the method created by Robert Alexy. This article supports the hypothesis that this institute represents an innovation in the protection of fundamental rights and deepens the argumentative burden on the judiciary when triggered.

Keywords: *Horizontal effectiveness of fundamental rights. General Data Protection Act. Legitimate Interest. Balancing Test.*

1. Introdução

A Lei Geral de Proteção de Dados Pessoais (LGPD) representa o marco legal brasileiro para tratar, de modo transversal, sobre a principal característica do capitalismo contemporâneo: a existência de uma economia movida a dados (*data-driven economy*)[2].

Numa elaborada formulação, a professora da Universidade de Brasília (UnB) Ana FRAZÃO, em seu artigo "Fundamentos da proteção dos dados pessoais" (2020), compreende essa proteção em seus aspectos essenciais: 1) como forma de endereçar os efeitos nefastos do capitalismo de vigilância (privacidade como um negócio); 2) como forma de endereçar os riscos que os algoritmos representam às liberdades individuais e à própria democracia; e 3) como forma de endereçar o problema da opacidade e da ausência de *accountability* da economia movida a dados[3].

No Brasil, a LGPD inovou no sistema legal de proteção de dados ao visar, para além dos direitos fundamentais de liberdade e de

[2] O capitalismo no século XXI passou a centrar-se na extração e no uso de dados pessoais (SRNICEK, Nick. *Platform Capitalism.* Cambridge: Polity Press, 2018)

[3] FRAZÃO, Ana. *Fundamentos da proteção dos dados pessoais* – Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados, in Lei Geral de Proteção de Dados e suas repercussões no Direito Brasileiro. 2ª Ed. São Paulo: Thomson Reuters Brasil, 2020.

privacidade, a proteção do livre desenvolvimento da personalidade da pessoa natural (art. 1.º), cuja disciplina tem, entre seus fundamentos, o desenvolvimento econômico/tecnológico e a inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor (art. 2.º, incisos V e VI).

Desde já se pode apontar que o âmbito de incidência da LGPD gira em torno de uma atividade: o tratamento de dados, cujo conceito adotado foi o expansionista[4].

Nesse sentido, o tratamento de dados pessoais, para que respeite direitos individuais dos titulares e para que não seja utilizada para embaraçar o empreendedorismo no país, deve obedecer a princípios estabelecidos (art. 6.º) e somente ser realizado quando atender a requisitos legais bem delimitados (denominadas de bases legais e jurídicas de tratamento de dados pessoais – art. 7.º e 11).

Uma dessas bases legais é o Legítimo Interesse, através do qual as empresas, como controladoras dos dados pessoais dos titulares, podem realizar operações de tratamento independentemente do encaixe em qualquer outra base legal e mesmo sem consentimento da pessoa titular dos dados.

Em verdade, a previsão do legítimo interesse se ajusta à contemporaneidade das trocas maciças de dados pessoais, de forma que a exigência do consentimento expresso dos titulares colocaria em risco a viabilidade econômica e operacional de vários modelos negociais das empresas. Dessa forma, garantiu-se uma solução legal, em atenção ao livre mercado e à livre iniciativa, desde que sejam operações de tratamento que visem (a lei, de modo lacônico, inclui a expressão "mão não se limitam") ao apoio e à promoção de atividade do controlador e à proteção, em relação ao titular, do exercício regular de seus direitos ou

[4] Para fins da LGPD, tratamento de dados corresponde a "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (art. 5.º, X).

prestação de serviços que o beneficiem (art. 10, incisos I e II).

Como instrumento de equilíbrio dessa operação em relação aos direitos de privacidade e de personalidade dos titulares de dados pessoais, a lei previu que somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados, cabendo ao controlador garantir a transparência do tratamento de dados baseado em seu legítimo interesse (art. 10, §2.º).

Na prática, vários conflitos podem surgir, razão pela qual, na União Europeia, o *General Data Protection Regulation* (GDPR) esclareceu que[5]:

> De qualquer modo, a existência de um interesse legítimo requer uma avaliação cuidada, nomeadamente da questão de saber se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são recolhidos, que esses poderão vir a ser tratados com essa finalidade. Os interesses e os direitos fundamentais do titular dos dados podem, em particular, sobrepor-se aos interesses do responsável pelo tratamento, quando que os dados pessoais sejam tratados em circunstâncias em que os seus titulares já não esperam um tratamento adicional.

Nesse cenário, a solução europeia foi instituir um teste de ponderação (*balancing test*), o qual representa uma metodologia que serve para se determinar qual dos interesses em jogo deve prevalecer ao se utilizar o legítimo interesse como base legal de tratamento (Oliveira e Cots, 2021, p. 100).

No Brasil, Bruno BIONI[6] explica que houve uma a escolha do legislador em não fazer um transplante legal daquilo que vinha sendo desenvolvido no contexto europeu, mas desenvolver um modelo de teste de legítimo interesse em quatro fases, dispostas no art. 10 da LGPD.

---

[5] CONSIDERANDO 47 da GDPR. Disponível em: https://gdpr-text.com/pt/read/recital-47/. Acesso em 03.10.2022.

[6] BIONI, Bruno. *Proteção de Dados Pessoais.* A função e os limites do consentimento. 3ª Edição. São Paulo: Editora Forense, 2021, p. 244.

Essa estratégia normativa corresponde a uma corporificação textual de uma solução possível para as hipóteses de conflitos de direitos fundamentais entre particulares.

Com isso, mobiliza-se a discussão sobre a eficácia horizontal dos direitos fundamentais para a temática da proteção de dados pessoais.

Nesse momento, molda-se o caminho para o problema de pesquisa a que este artigo procura responder: *O teste de ponderação, utilizado para o tratamento de dados pessoais baseados no legítimo interesse, inova na temática da vinculação dos particulares a direitos fundamentais em relação à metodologia desenvolvida por Robert Alexy?*

Esse problema possibilita uma discussão fértil, no campo da teoria da eficácia horizontal dos direitos fundamentais, sobre as metodologias empregadas por Robert Alexy e pela Lei Geral de Proteção de Dados no Brasil.

Neste artigo, pretende-se, inicialmente, apresentar a proteção de dados pessoais como um direito fundamental autônomo.

Em seguida, demonstrar-se-á qual a justificativa da inclusão do legítimo interesse como uma base legal para tratamento de dados pessoais na LGPD.

Do mesmo modo, serão apresentados alguns elementos da teoria de Robert Alexy sobre a eficácia horizontal dos direitos fundamentais, para que seja viabilizada uma comparação panorâmica dos seus argumentos em relação ao teste de ponderação (*Legitimate Interests Assessment – LIA*) disposto na LGPD, para responder o problema central desse artigo.

O método lógico-argumentativo utilizado foi o indutivo. Assim, parte-se de constatações mais particulares de fenômenos até a aproximação a planos mais abrangentes de leis e de teorias (conexão ascendente), através das técnicas de pesquisa documental dos textos normativos e de pesquisa bibliográfica.

Em jeito de conclusão, será apresentada a tese de que o teste de ponderação como requisito prévio para o tratamento de dados pessoais, baseado no legítimo interesse do controlador, representa uma inovação

na temática da proteção de direitos fundamentais, por instituir novos requisitos autorizadores e por internalizar uma metodologia constitucionalizante na análise funcional desse marco civilista previsto na Lei Geral de Proteção de Dados Pessoais no Brasil.

2. A proteção de dados pessoais como um direito fundamental autônomo

A recente alteração da Constituição Federal brasileira promovida pela Emenda Constitucional n. 115/2022[7], a qual incluiu a proteção de dados pessoais entre os direitos e garantias fundamentais, delimitou a autonomia desse direito em relação ao direito de privacidade. Esse desfecho momentâneo encerra um ciclo e inicia uma nova era sobre o tratamento e a proteção dos dados pessoais.

Por certo que a coleta de dados pessoais, para fins econômicos, não é uma atividade nova. Como esclarece DONEDA, Danilo (2021), a matéria da proteção de dados foi impulsionada *"a partir da aplicação de determinadas concepções do direito à privacidade e da proteção da pessoa em face do desenvolvimento tecnológico"*. Ocorre que *"a própria expressão ´proteção de dados´ não reflete fielmente o seu âmago, pois é resultado de um processo de desenvolvimento do qual participaram diversos interesses em jogo"*.

Com efeito, a proteção efetiva é do direito da personalidade, entre cujos bens[8] tutelados, encontram-se os dados pessoais dos titulares. Nesse sentido, BIONI, Bruno (2021, p. 55) demonstra a projeção da personalidade por meio dos dados, apontando, como condição essencial para tanto, que o dado assuma o adjetivo de "pessoal", para que se

[7] CONSTITUIÇÃO FEDERAL DO BRASIL, Art. 5.º, LXXIX – é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

[8] BIONI, Bruno (2021, p. 54) pontua que o conceito de bens da personalidade é dirigido para a satisfação do livre desenvolvimento da personalidade. Segundo António Menezes CORDEIRO, o progressivo domínio dogmático da ´periferia´ da personalidade permitiu o esforço de abstração necessária para se alcançar a ideia de ´bem de personalidade´.

caracterize como uma projeção, extensão ou dimensão do seu titular.

De maneira lapidar, Stefano RODATÀ[9] reflete que:

> Estamos diante da verdadeira reinvenção da proteção de dados – não somente porque ela é expressamente considerada como um direito fundamental autônomo, mas também porque se tornou uma ferramenta essencial para o livre desenvolvimento da personalidade. A proteção de dados pode ser vista como a soma de um conjunto de direitos que configuram a cidadania do novo milênio.

A abrangência da proteção, portanto, não leva em questão simplesmente o eixo da privacidade, haja vista que os dados pessoais públicos, que circulam e estão à disposição de todos por força legal (v.g. as leis de acesso à informação e do processo eletrônico), também se qualificam como passíveis de proteção. Assim, como adverte Bruno BIONI, "a esfera do que é público ou privado revela-se incompleta para dar vazão a esse tipo de dinâmica normativa"[10].

Contudo, a Constituição Federal brasileira de 1988, em seu texto original, deixou de tratar especificamente acerca do direito à proteção de dados como distinto do direito à privacidade. Isso não impediu que se desenvolvessem fundamentos jurídicos, atrelados ao direito à privacidade como um direito humano fundamental, os quais refletiram a preocupação do constituinte com o tratamento e com proteção de dados, como decorrência de uma série de garantias fundamentais, como o direito à autodeterminação de dados e de informações[11].

Na realidade, os dois direitos estão ligados, conforme explica

---

[9] RODATÀ, Stefano. *A vida na sociedade da vigilância*. A privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 17.

[10] BIONI, Bruno. *Proteção de Dados Pessoais.* A função e os limites do consentimento. 3ª Edição. São Paulo: Editora Forense, 2021, p. 58.

[11] GARCEL, Adriane; MORO, Sergio Fernando; SOUZA NETTO, José Laurindo de; HIPPERTT, Karen Paiva. "Lei geral de proteção de dados: diretrizes e implicações para uma sociedade pandêmica" *in Coletâneas de artigos jurídicos: em homenagem ao Professor José Laurindo de Souza Netto*. 1.ª Edição, Curitiba: Clássica Editora, 2020, pp. 319-344.

Danilo DONEDA[12], (2021, p. 94):

> a informação pessoal está, quase como ato reflexo, ligada à privacidade por uma equação simples e básica que associa um maior grau de privacidade a menor difusão de informações pessoais e vice-versa. Esta equação nem de longe encera toda a complexa problemática em torno dessa relação, porém pode servir como ponto de partida para ilustrar como a proteção das informações pessoais passou a encontrar guarida em nosso ordenamento jurídico: como um desdobramento da tutela do direito à privacidade.

Numa sinalização de que compreendeu a dimensão e o impacto dos novos tempos, o Supremo Tribunal Federal, no julgamento de cinco Ações Diretas de Inconstitucionalidade (ADI´s 6387, 6388, 6389 e 6390/DF[13]), reconhecera a fundamentalidade do direito à proteção de dados, através, especialmente, de uma justificativa fático-pragmática e outra jurídico-constitucional.

Quanto à primeira, o STF afirmou que não há dados irrelevantes, de forma que a CF/88 não protege apenas os dados sigilosos (como decorrência do art. 5.º, inciso XII), mas todo dado que tenha por característica ser um atributo da personalidade humana (BIONI, 2021, p. 104). Segundo registrado pela Min. Cármen Lúcia[14], *"é crucial ter presente que o que podia ser feito a partir da publicização de tais dados pessoais não se compara ao que pode ser feito no patamar tecnológico*

---

[12] DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais.* 3ª ed. São Paulo: Thomson Reuters, 2021.

[13] Para a Corte brasileira, a Constituição Federal expressamente assegura o direito à autodeterminação informativa, por isso o uso de dados e informações pessoais deve ser controlado pelo próprio indivíduo, conforme expressamente positivado na LGPD (Lei n.º 13.709/2018) em seu art. 2.º, I e II. Não obstante, o direito à autodeterminação informativa e à privacidade são desmembramentos dos direitos da personalidade e subsidiam a proteção não só da democracia, mas também de uma série de direitos fundamentais previstos no art. 3.º, I e II; art. 4.º, II; art. 5.º, X e XII; art. 7.º, XXVII; e art. 219 da CF.

[14] SUPREMO TRIBUNAL FEDERAL. MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE N. 6.387, Relatora Ministra Rosa Weber. Disponível em https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Acesso em 04.08.2022.

atual, em que poderosas tecnologias de processamento, cruzamento e filtragem de dados permitem a formação de perfis individuais extremamente detalhados".

Com isso, utilizou-se, como *ratio decidendi*, um argumento que chamou a atenção de pensadores como Nick SRNICEK, para quem os dados pessoais são o novo petróleo nessa *data-driven economy*[15], e Yuval HARARI, para quem a regulação da propriedade de dados talvez seja a questão política mais importante da nossa era[16].

Em verdade, Ana FRAZÃO[17] explica que as atividades de obtenção, de coleta, de registro e de acesso a dados pessoais, após o *Big Data* e o *Big Analytics*, ocorrem de maneira muito mais eficiente, com mais veracidade, velocidade, variedade e volume (4V), possibilitando utilizações que não seriam sequer imagináveis há pouco tempo.

Ademais, o STF instituiu uma virada histórica de sua jurisprudência, apontando, como menciona Bruno BIONI, para uma *"evolução, a partir da construção do conceito de autodeterminação informativa, do direito à privacidade, liberdade negativa, para um direito à proteção de dados, liberdade positiva e projeção da personalidade, a ser protegida e promovida pelo Estado[18]"*. Em passagem lapidar, o voto do Min. Gilmar Mendes afirma que, *"para além desses desenvolvimentos normativos, a abertura do texto constitucional ao reconhecimento da autonomia do direito fundamental à proteção de dados pode ser identificada na própria jurisprudência desta Corte[19]"*.

---

[15] SRNICEK, Nick. *Platform Capitalism.* Cambridge: Polity Press, 2018.

[16] HARARI, Yuval Noah. *21 Lições para o Século 21*. São Paulo: Companhia das Letras, 2018.

[17] FRAZÃO, Ana. "Fundamentos da proteção dos dados pessoais – Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados"*, in Lei Geral de Proteção de Dados e suas repercussões no Direito Brasileiro.* 2ª Ed. São Paulo: Thomson Reuters Brasil, 2020, pp. 23/52.

[18] BIONI, Bruno. *Proteção de Dados Pessoais.* A função e os limites do consentimento. 3ª Edição. São Paulo: Editora Forense, 2021, p. 105.

[19] SUPREMO TRIBUNAL FEDERAL. MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE N. 6.387, Relatora Ministra Rosa Weber. Disponível em https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Acesso em 04.08.2022.

Em resumo, Bruno BIONI[20] demonstra que, desse diálogo entre o direito à privacidade (liberdade negativa) e à proteção de dados pessoais (liberdade positiva), o saldo foi o reconhecimento de uma série de liberdades individuais, atreladas à proteção de dados, que não são abraçadas pelo direito à privacidade, modificando o centro gravitacional da discussão da tradicional dicotomia privado/público para um novo rol aberto dos direitos da personalidade.

Acolhendo essa perspectiva, a Lei Geral de Proteção de Dados, mesmo antes da promulgação da Emenda Constitucional n. 115/2022, já internalizara a disciplina da proteção de dados pessoais como condição para a proteção dos direitos fundamentais e do livre desenvolvimento da personalidade (art. 1.º), bem como garantia de um ambiente de segurança jurídica para o desenvolvimento econômico-tecnológico e da inovação (art. 2.º). Bruno BIONI aponta que o produto dessa dialética normativa de conciliação de interesses corporifica-se no que se entende por autodeterminação informacional. Segundo esse autor:

> O principal vetor para alcançar tal objetivo é franquear ao cidadão controle sobre seus dados pessoais. Essa estratégia vai além do consentimento do titular dos dados, pelo qual ele autoriza o seu uso. Tão importante quanto esse elemento volitivo é assegurar que o fluxo informacional atenda às suas legítimas expectativas e, sobretudo, não seja corrosivo ao livre desenvolvimento da sua personalidade[21].

Com uma posição diferenciada, Ingo Wolfgang SARLET apresenta argumentos para justificar que a proteção de dados pessoais vai além da privacidade e da autodeterminação. Segundo o professor:

---

[20] BIONI, Bruno. *Proteção de Dados Pessoais.* A função e os limites do consentimento. 3ª Edição. São Paulo: Editora Forense, 2021, pp. 91/96.

[21] BIONI, Bruno. *Proteção de Dados Pessoais.* A função e os limites do consentimento. 3ª Edição. São Paulo: Editora Forense, 2021, p. 99

> No que diz respeito ao seu conteúdo (âmbito de proteção), embora sua articulação com o princípio da dignidade da pessoa humana e de outros direitos fundamentais, em especial o direito ao livre desenvolvimento da personalidade e alguns direitos especiais de personalidade, como é o caso, entre outros, do direito à privacidade e do assim chamado direito à autodeterminação informativa, o direito fundamental à proteção de dados, na condição de direito autônomo (o que não quer dizer sem pontos de contato relevantes) não se confunde com o do objeto da proteção de tais direitos[22].

É dizer, não há sobreposição entre autodeterminação informativa e proteção de dados, nem privacidade e outros direitos de personalidade. Em síntese, o direito à autodeterminação tem uma dimensão individual, como a possibilidade de cada um decidir sobre o acesso, uso e difusão dos seus dados pessoais, e outra coletiva (metaindividual), por se constituir como precondição para uma ordem comunicacional livre e democrática. Já o objeto (âmbito de proteção) do direito à proteção de dados pessoais é mais amplo, porquanto, com base num conceito ampliado de informação, abarca todos os dados que dizem respeito a uma determinada pessoa natural, sendo irrelevante a qual esfera da vida pessoal se referem (íntima, privada, familiar, social), descabida qualquer tentativa de delimitação temática (Sarlet, 2021).

Por tais peculiaridades, conclui Ingo Wolfgang SARLET:

> o direito à proteção de dados vai além da tutela da privacidade e da autodeterminação informativa, cuidando-se, de tal sorte, de um direito fundamental autônomo, diretamente vinculado à proteção da personalidade[23].

---

[22] SARLET, Ingo Wolfgang. *Proteção de dados pessoais: para além da privacidade e autodeterminação informacional*. Conjur, publicado em 16.07.2021. Disponível em: https://www.conjur.com.br/2021-ago-15/direitos-fundamentais-direito-protecao-dados-pessoais-direito-subjetivo. Acesso em 02.10.2022.

[23] SARLET, Ingo Wolfgang. *O direito fundamental à proteção de dados pessoais como direito subjetivo.* Conjur, publicado em 15.08.2021. Disponível em: https://www.conjur.com.br/2021-ago-15/direitos-fundamentais-direito-protecao-dados-pessoais-direito-subjetivo. Acesso em 03.10.2022.

Na prática, Adriane GARCEL[24] et al. esclarece que *"o âmago do direito à proteção de dados reside na vedação à coleta, processamento e circulação de dados irrestrita sem o consentimento do usuário, que impõe a estruturação de um sistema de segurança para proteção, garantindo a autonomia, autocontrole e autodeterminação do titular[25]"*.

Conquanto haja espaço para divergências quanto à sua exatidão conceitual, o direito à proteção de dados pessoais, enquanto direito fundamental autônomo, possui dupla dimensão: uma subjetiva, ligada à defesa do indivíduo; e outra objetiva, relacionada ao dever de proteção Estatal.

Numa série de artigos ao sítio eletrônico brasileiro Conjur, Ingo Wolfgang SARLET resume que, em relação à proteção de dados, o Estado terá dever negativo de deixar de interferir no direito e o dever positivo de agir criando medidas para sua proteção. E *"essa eficácia irradiante ou horizontal, também chamada de Drittwirkung, ainda, estende tais deveres ao setor privado[26]"*.

Como direito subjetivo, o direito fundamental à proteção de dados pessoais cumpre uma multiplicidade de funções na ordem jurídico-constitucional. Segundo Ingo SARLET:

> Na sua condição de direito subjetivo, e considerado como um direito em sentido amplo, o direito à proteção de dados pessoais se decodifica em um conjunto heterogêneo de posições subjetivas de natureza defensiva (negativa), mas também assume a condição de direito a prestações,

---

[24] GARCEL, Adriane; MORO, Sergio Fernando; SOUZA NETTO, José Laurindo de; HIPPERTT, Karen Paiva. "Lei geral de proteção de dados: diretrizes e implicações para uma sociedade pandêmica" *in Coletâneas de artigos jurídicos: em homenagem ao Professor José Laurindo de Souza Netto*. 1.ª Edição, Curitiba: Clássica Editora, 2020, pp. 319-344.

[25] O maior objetivo encontra-se na garantia de que a pessoa se cientifique acerca de quais dados estão sendo acessados, coletados e armazenados, para qual fim e por quem (Garcel et al., 2021).

[26] SARLET, Ingo Wolfgang. *O direito fundamental à proteção de dados pessoais como direito subjetivo.* Conjur, publicado em 15.08.2021. Disponível em: https://www.conjur.com.br/2021-ago-15/direitos-fundamentais-direito-protecao-dados-pessoais-direito-subjetivo. Acesso em 03.10.2022.

cujo objeto consiste em uma atuação do estado mediante a disponibilização de prestações de natureza fática ou normativa.

No tocante à sua eficácia objetiva[27], Ingo SARLET explica que *"a perspectiva objetiva dos direitos fundamentais não representa um mero 'reverso da medalha' da perspectiva subjetiva"*, para *"desembocar no reconhecimento de conteúdos normativos e, portanto, de funções distintas aos direitos fundamentais[28]"*.

Destacam-se as funções de (1) efeito irradiante (*Ausstrahlungswirkung*) dos direitos fundamentais, por meio do qual se *"fornecem impulsos e diretrizes para a aplicação e interpretação do Direito infraconstitucional, o que, além disso, apontaria para a necessidade de uma interpretação conforme aos direitos fundamentais"*. Como efeito decorrente, tem-se o (2) *"fenômeno da constitucionalização do Direito, incluindo o Direito Privado, o que também remete à eficácia dos direitos fundamentais nas relações privadas[29]"*, o qual guarda estreita relação com os deveres de proteção estatais (S*chutzpflichten*), caracterizada como função *"desenvolvida com base na existência de um dever geral de efetivação atribuído ao Estado [...], no sentido de que a este incumbe zelar, inclusive preventivamente, pela proteção dos direitos fundamentais dos indivíduos não somente contra*

---

[27] Na lição de SARLET (2021), "o descobrimento e o desenvolvimento da assim chamada dimensão objetiva dos direitos fundamentais – como já é de amplo conhecimento – pode ser reconduzido ao labor da doutrina e da jurisprudência constitucional alemã, notadamente a partir da década de 1950. Nesse contexto, sempre é recordada a paradigmática afirmação do Tribunal Constitucional Federal, no sentido de que os direitos fundamentais não se limitam à função precípua de serem direitos subjetivos de defesa do indivíduo contra atos do poder público, mas que, além disso, constituem decisões valorativas de natureza jurídico-objetiva da Constituição, com eficácia em todo o ordenamento jurídico e que fornecem diretrizes para os órgãos legislativos, judiciários e executivos".

[28] SARLET, Ingo Wolfgang. *Proteção de dados pessoais e deveres de proteção estatais.* Conjur, publicado em 27.08.2021. Disponível em: https://www.conjur.com.br/2021-ago-27/direitos-fundamentais-protecao-dados-pessoais-deveres-protecao-estatais. Acesso em 03.10.2022.

[29] Também abordada sob a denominação de eficácia horizontal (*Drittwirkung*) ou eficácia em relação a terceiros.

os poderes públicos, mas também contra agressões provindas de particulares[30]*".*

Desse modo, configurado o direito à proteção de dados pessoais como direito fundamental autônomo, sobressaem suas dimensões subjetiva e objetiva, destacando-se o desdobramento da perspectiva objetiva, a qual se expressa, segundo Ingo SARLET, *"sob o aspecto de parâmetros para a criação e constituição de organizações (ou instituições) estatais e para o procedimento. Nesse contexto, há de considerar a íntima vinculação entre direitos fundamentais, organização e procedimento".*

A seguir, será apresentada a teoria geral da eficácia dos direitos fundamentais na esfera das relações privadas para viabilizar a análise do arranjo normativo instituído pela lei geral de proteção de dados quanto aos requisitos jurídicos necessários para o tratamento legítimo de dados pessoais com base no legítimo interesse.

3. A eficácia horizontal dos direitos fundamentais na teoria de Robert Alexy

Ingo SARLET destaca a ideia de os direitos fundamentais irradiarem efeitos também nas relações privadas como um dos mais relevantes desdobramentos da perspectiva objetiva[31] dos direitos fundamentais. Já Wilson STEINMETZ e Cristhian Magnus DE MARCO esclarecem que, necessariamente, "analisar a eficácia horizontal é analisar o significado

[30] SARLET, Ingo Wolfgang. *Proteção de dados pessoais e deveres de proteção estatais.* Conjur, publicado em 27.08.2021. Disponível em: https://www.conjur.com.br/2021-ago-27/direitos-fundamentais-protecao-dados-pessoais-deveres-protecao-estatais. Acesso em 03.10.2022.

[31] SARLET, Ingo Wolfgang. *Proteção de dados pessoais e deveres de proteção estatais.* Conjur, publicado em 27.08.2021. Disponível em: https://www.conjur.com.br/2021-ago-27/direitos-fundamentais-protecao-dados-pessoais-deveres-protecao-estatais. Acesso em 03.10.2022.

que as normas de direitos fundamentais têm para todo o sistema jurídico[32]".

A controvérsia, que orienta toda a discussão jusconstitucionalista, relaciona-se ao modo (*como*) e à amplitude (*extensão*) desses efeitos. Na lapidar lição de STEINMETZ e DE MARCO (2014), "a questão do *como* é um problema de construção; a da *extensão* é um problema de colisão".

Com o propósito de sintetizar o estado da arte sobre o assunto, pode-se lançar mão de três construções teóricas.

Há a Teoria da Eficácia Mediata[33] (ou Teoria dos Efeitos Indiretos perante terceiros), segundo a qual os direitos fundamentais, enquanto "decisões axiológicas", "normas objetivas" ou "valores constitucionais", influenciam a interpretação e aplicação das disposições de direito privado, em especial no "preenchimento" das cláusulas gerais e dos conceitos jurídicos indeterminados[34].

Para essa teoria, os efeitos não se operam *ex constitucione*. Mas pelos parâmetros dogmático-hermenêuticos do direito privado, cabendo ao legislador o "desenvolvimento concretizante dos direitos fundamentais por meio da criação de normas. Ao juiz compete dar eficácia por meio da interpretação de normas imperativas de direito privado, sobretudo das cláusulas gerais (ordem pública, boa-fé, abuso de direito, etc), as quais serviriam como cláusulas de abertura[35] para a influência ou a irradiação dos direitos fundamentais no direito privado" (Steinmetz, 2004).

---

[32] Segundo esses autores, "esse significado depende da fundamentalidade formal e da fundamentalidade material dos direitos fundamentais. Da fundamentalidade formal e da fundamentalidade material dos direitos fundamentais, assim entendidas, resulta que as normas de direitos fundamentais projetam efeitos não só sobre as relações entre o Estado e os cidadãos (relações de direito público), mas também sobre as relações entre os cidadãos (relações de direito privado)". STEINMETZ, Wilson e DE MARCO, Cristhian Magnus. *A eficácia horizontal dos direitos fundamentais na teoria de Robert Alexy.* Porto Alegre, Revista da AJURIS, v. 41, n. 134, 2014.

[33] Formulada por Günter DÜRIG em 1953 e adotada pelo Tribunal Constitucional Federal alemão a partir do caso Lüth (1958).

[34] STEINMETZ, Wilson e DE MARCO, Cristhian Magnus. *A eficácia horizontal dos direitos fundamentais na teoria de Robert Alexy.* Porto Alegre, Revista da AJURIS, v. 41, n. 134, 2014.

[35] Como pontos de irrupção (*einbrchstellen*), conforme expressão de Günter DÜRIG.

Sobre o tema, lapidar a reflexão de Wilson STEINMETZ[36]:

> As normas não incidem como direitos subjetivos constitucionais, mas como normas objetivas de princípio (como sistema de valores, cujo centro é o livre desenvolvimento da personalidade humana). A correção dessa teoria repousa em que: a) considera e preserva a autonomia privada como princípio fundamental do direito privado, de modo que assegura a identidade, autonomia e função desse ramo do direito como um todo; b) evita a "panconstitucionalização" do ordenamento jurídico, sobrecarregando a jurisdição constitucional. Assim, quanto à teoria da eficácia mediata, que em sua matização mais dura nega a vinculação imediata dos particulares a direitos fundamentais e que em sua matização mais fraca a admite como exceção, a Constituição (tanto a brasileira como a alemã, local onde se desenvolveu essa teoria) se apresenta como uma "ordem fundamental liberal democrática", ou seja, um constitucionalismo liberal mitigado democrática e socialmente.

Como contraponto, a Teoria da Eficácia Imediata[37] (ou Teoria dos Efeitos Diretos perante terceiros) justifica que, dos direitos fundamentais previstos na Constituição, "fluem também diretamente direitos subjetivos privados para os indivíduos" (NIPPERDEY[38]).

Essa teoria postula uma eficácia não condicionada à mediação concretizadora dos poderes públicos. Em sua versão "intermediária", Wilson STEINMETZ explica que o problema da eficácia das normas de direitos fundamentais entre particulares é um problema de colisão de direitos fundamentais, haja vista que, "em razão de a autonomia privada (princípio fundamental de direito privado) ser um bem constitucionalmente protegido, o alcance da eficácia imediata em cada

---

[36] STEINMETZ, Wilson. *A vinculação dos particulares a direitos fundamentais.* São Paulo: Malheiros Editores, 2004.

[37] Formulada por Hans C. NIPPERDEY.

[38] *Apud* ALEXY, Robert**.** ***Teoria dos direitos fundamentais.*** São Paulo: Malheiros Editores, 2008.

caso concreto deve resultar de uma justificada ponderação dos direitos, interesses ou bens em jogo[39]".

Como fundamento para orientar o Estado-juiz, "se há um desenvolvimento legislativo de direitos fundamentais e se este desenvolvimento é compatível com a Constituição, então o juiz não poderá se sobrepor a ele sob pena de violar os princípios democrático e da separação dos poderes[40]".

Já há uma terceira teoria, denominada Teoria da Imputação e desenvolvida por Jürgen SCHWABE, a qual sustenta que o Estado se vincula aos direitos fundamentais nas relações entre particulares por decorrerem de direitos de defesa, de maneira que "as violações de direitos fundamentais entre particulares devem ser imputadas ao Estado [...], à medida que ao Estado cabe criar e impor as normas de direito privado. Portanto, os efeitos dos direitos fundamentais entre cidadãos se justificam e se processam pela dimensão defensiva dos direitos fundamentais do cidadão contra o Estado[41]".

Segundo SCHWABE, toda lesão de direito fundamental entre particulares deve ser imputada ao Estado, porque a lesão, em última análise, resulta de uma permissão estatal ou de uma não-proibição estatal. Por esse rigor, para Wilhelm Franz CANARIS[42], é um equívoco aplicar essa teoria às relações negociais privadas.

Coube a Robert ALEXY[43] identificar que tais teorias não se encontram em condição de aporia. Bem o contrário: há algo em comum nessas teorias. Todas têm como destinatário o Poder Judiciário, de modo que, no plano da decisão judicial, elas produzem resultados equivalentes.

---

[39] STEINMETZ, Wilson. *A vinculação dos particulares a direitos fundamentais.* São Paulo: Malheiros Editores, 2004.

[40] STEINMETZ, Wilson. *A vinculação dos particulares a direitos fundamentais.* São Paulo: Malheiros Editores, 2004.

[41] STEINMETZ, Wilson e DE MARCO, Cristhian Magnus. *A eficácia horizontal dos direitos fundamentais na teoria de Robert Alexy.* Porto Alegre, Revista da AJURIS, v. 41, n. 134, 2014.

[42] CANARIS, Claus Wilhelm. "Considerações a respeito da posição de proibições de discriminação no sistema do direito privado". *Revista Direitos Fundamentais & Justiça.* Ano 7, n.º 22, Porto alegre, 2013, pp. 15-20

[43] Conhecida como Teoria Integradora de Alexy.

Com efeito, essas teorias não ignoram que a relação cidadão--cidadão é diferente da relação entre cidadão-Estado, porque naquela ambos os lados são titulares de direitos fundamentais. A consequência intuitiva e mais relevante é que os efeitos dos direitos fundamentais nas relações entre cidadãos devem ser modulados. Em última análise, Robert ALEXY[44] ensina que "a medida do efeito dos direitos fundamentais na relação cidadão/cidadão é, no final das contas, uma questão de sopesamento", o que significa que, "em determinados âmbitos do direito privado, determinados direitos fundamentais podem ceder totalmente ou em grande medida".

Em resumo, tem-se como aspectos em que há consenso nas três teorias: *a)* na relação entre particulares, ambas as partes são titulares de direitos fundamentais; *b)* por essa razão, a eficácia deve ser matizada; e *c)* a medida da eficácia deve ser definida, em última instância, pela ponderação (sopesamento). Em relação à ponderação, a diferença é que, para a teoria da eficácia mediata, ela deve ser realizada no marco do direito civil válido.

Wilson STEINMETZ e Cristhian Magnus DE MARCO destacam a relevância da contribuição de Robert ALEXY para o debate sobre a eficácia horizontal dos direitos fundamentais:

> Não existindo uma construção dogmática unitária para a eficácia dos direitos fundamentais nas relações jurídicas entre particulares, Alexy propõe um modelo de três níveis, integrando as três teorias básicas: teoria da eficácia mediata, teoria da eficácia imediata e teoria da imputação de Schwabe (direitos de defesa contra o Estado)[45].

Sendo assim, ALEXY propôs um modelo de níveis com os deveres do Estado, com os direitos ante o Estado e com o direito nas relações

[44] ALEXY, Robert. *Teoría de los derechos fundamentales*. Tradução Ernesto Garzón Valdés. Madrid: Centro de Estudios Constitucionales, 1997, p. 521.

[45] STEINMETZ, Wilson e DE MARCO, Cristhian Magnus. *A eficácia horizontal dos direitos fundamentais na teoria de Robert Alexy.* Porto Alegre, Revista da AJURIS, v. 41, n. 134, 2014.

entre particulares. A Teoria da Eficácia Mediata (ou indireta) situa-se no nível dos deveres do Estado, cujos princípios objetivos dos direitos fundamentais se projetam sobre todos os âmbitos do direito e obrigam o Estado a tomá-los em conta na legislação e na jurisdição. A Teoria da Imputação (a Teoria de SCHWABE) situa-se no nível dos direitos ante o Estado. Aqui, o particular, em conflito com outro particular, tem o direito fundamental a que o Estado-juiz, em suas decisões, considere os princípios objetivos *jusfundamentais* que apoiam a posição do particular[46]. Por último, no terceiro nível, situa-se a Teoria da Eficácia Imediata (ou indireta), cuja definição de Robert ALEXY[47], "consiste em que, por razões *jusfundamentais*, na relação cidadão/cidadão existem determinados direitos e não-direitos, liberdades e não-liberdades, competências e não-competências que, sem essas razões, não existiriam".

Através dessa formulação, ALEXY conclui que a eficácia imediata resulta também da teoria da eficácia mediata e da teoria da eficácia por meio da mediação estatal (teoria de SCHWABE). Essa reconciliação semântica na gramática da eficácia horizontal dos direitos fundamentais fortalece a noção de uma Constituição mista material procedimental[48], por meio da qual o texto constitucional não determina todo o conteúdo do direito ordinário (incluído aí o direito privado), mas reconhece que "os direitos fundamentais excluem alguns conteúdos como

[46] "Esse direito fundamental é um direito fundamental ante (contra) a jurisdição. Se o juiz ou o Tribunal, na decisão proferida, não tomar em consideração esse direito fundamental, estará lesando esse direito fundamental como direito de defesa" (STEINMETZ, Wilson e DE MARCO, Cristhian Magnus. *A eficácia horizontal dos direitos fundamentais na teoria de Robert Alexy.* Porto Alegre, Revista da AJURIS, v. 41, n. 134, 2014).

[47] ALEXY, Robert. *Teoría de los derechos fundamentales*. Tradução Ernesto Garzón Valdés. Madrid: Centro de Estudios Constitucionales, 1997, p. 524.

[48] Para Alexy (2008, p. 522), "o fato de uma constituição ter elementos procedimentais e materiais combinados entre si tem importantes consequências para todo o sistema jurídico. Isso significa que, ao lado dos conteúdos que, no sistema jurídico, são simplesmente *possíveis* em relação à constituição, há também conteúdos que são, também em relação à constituição, *necessários* ou *impossíveis*. O fato de as normas de direitos fundamentais estabelecerem os conteúdos constitucionalmente necessários e impossíveis para o sistema jurídico constitui o núcleo da fundamentalidade formal desses direitos".

constitucionalmente impossíveis e exigem alguns conteúdos como constitucionalmente necessários[49]".

Identificado o espectro de convivência dos direitos fundamentais entre os particulares, um novo âmbito de incidência se descortina ao princípio da proporcionalidade, o qual é compreendido, segundo Wilson STEINMETZ, como norma (dimensão jurídico-constitucional) e como método (dimensão hermenêutico-aplicativa).

De fato, como norma, a proporcionalidade garante a convivência da autonomia privada, um bem constitucionalmente protegido, dentro do campo de discussão dos conflitos entre direitos fundamentais. A consequência, ressalta Wilson STEINMETZ, é que "a possibilidade de restrição a direitos fundamentais é condição para a própria efetividade e concordância prática desses direitos (Princípio da Restringibilidade dos Direitos Fundamentais)". Mas adverte[50]:

> As restrições podem ser inadequadas, desnecessárias e desproporcionais. Daí porque à restringibilidade se põe como contraponto a proporcionalidade. Restringibilidade e proporcionalidade são pratos de uma mesma balança. Se há restrição a direito fundamental, então está ordenado o exame de proporcionalidade.

Aqui se abre espaço para se discorrer sobre a importância da proporcionalidade como metodologia racional-discursiva para a solução de conflitos entre princípios[51].

Especialmente no que toca à eficácia horizontal dos direitos fundamentais, o bem jurídico da autonomia da vontade das partes envolvidas deve ser empregado no momento da determinação das relações de

---

[49] ALEXY, Robert. *Teoría de los derechos fundamentales*. Tradução Ernesto Garzón Valdés. Madrid: Centro de Estudios Constitucionales, 1997, p. 543.

[50] STEINMETZ, Wilson. *A vinculação dos particulares a direitos fundamentais.* São Paulo: Malheiros Editores, 2004, p. 30.

[51] Teoria dos princípios (ALEXY) tem os seguintes elementos básicos: diferença entre regras e princípios; tese da relação de precedência condicionada (lei de colizão); estruturas de ponderação procedimentalizadas no princípio da proporcionalidade e a tese das prioridades *prima facie*.

precedência condicionada. Ou seja, a autonomia da vontade deve orientar quando e em que condições, no caso concreto, um princípio deve preceder o outro. Segundo o Tribunal Constitucional Alemão, o qual utiliza a "metáfora do peso", este equivale a "razões suficientes[52]".

E, através da formulação da lei de colizão de ALEXY, indica-se o que precisa ser fundamentado: o resultado que se alcança com a ponderação. Assim, o resultado da ponderação pode ser formulado como uma regra – uma regra de preferência que expressa uma relação de precedência condicionada.

Wilson STEINMETZ esclarece que "a ponderação é o método: primeiro, a mensuração do grau de não-satisfação de um princípio (o princípio restringido). Segundo, avaliação da importância (peso) da realização do outro princípio (o princípio oposto). Terceiro, demonstração da importância da realização do princípio oposto[53]". Por fim, reconhece-se a precedência *prima facie*. Para ser superada, exige-se o cumprimento de um ônus argumentativo em favor da preferência do princípio oposto.

E acrescenta que[54]:

> Quanto maior é o grau de não-satisfação ou de afetação de um princípio, tanto maior tem que ser a importância da satisfação do outro. As precedências prima facie podem ser argumentativamente usadas como contra-objeção à objeção segundo a qual a eficácia imediata de direitos fundamentais entre particulares medida e modulada pela aplicação do princípio da proporcionalidade poderia instaurar a incerteza jurídica e provocar a erosão normativa do princípio da autonomia privada.

---

[52] STEINMETZ, Wilson. *A vinculação dos particulares a direitos fundamentais.* São Paulo: Malheiros Editores, 2004, p. 36.

[53] STEINMETZ, Wilson. *A vinculação dos particulares a direitos fundamentais.* São Paulo: Malheiros Editores, 2004, p. 42.

[54] STEINMETZ, Wilson. *A vinculação dos particulares a direitos fundamentais.* São Paulo: Malheiros Editores, 2004, p. 48.

Aprofundando a metodologia de ALEXY, o professor Wilson STEINMETZ propôs uma ordem de precedências *prima facie*[55], em relação à eficácia horizontal dos direitos fundamentais, elegendo, como fator legítimo de *discrímen*, a igualdade fática dos particulares na relação contratual, como circunstância ou condição relevante de ponderação. O resultado de sua formulação apresenta os seguintes *standards* hermenêuticos[56]: 1) *Particulares em situação de igualdade*, há uma precedência do direito fundamental individual de conteúdo pessoal ante o princípio da autonomia privada; 2) *Particulares em desigualdade*, precedência do direito fundamental individual de conteúdo pessoal ante o princípio da autonomia privada; 3) *Particulares em situação de igualdade*, há uma precedência do princípio da autonomia da vontade ante o direito fundamental individual de conteúdo patrimonial; 4) *Particulares em desigualdade*, precedência do direito fundamental individual de conteúdo patrimonial ante o princípio da autonomia privada. Em última análise, trata-se de formar um juízo sobre a qualidade do consentimento do particular cujo direito fundamental foi ou é afetado.

No que diz respeito à eficácia horizontal dos direitos na temática de proteção dos dados pessoais, pode-se ajustar, via de regra, as situações práticas de tratamento de dados à segunda previsão de STEINMETZ,

---

[55] STEINMETZ, Wilson. *A vinculação dos particulares a direitos fundamentais.* São Paulo: Malheiros Editores, 2004, p. 51.

[56] O professor Virgílio Afonso DA SILVA, não obstante reconhecer a qualidade e inovação do pensamento de STEINMETZ, apresentou as seguintes críticas: "A mim me parece, contudo, que esse raciocínio não pode ser transportado para as relações entre particulares e a razão é trivial: exigir que os particulares adotem, nos casos de restrição a direitos fundamentais, apenas as medidas estritamente necessárias – ou seja, as menos gravosas – para o atingimento dos fins perseguidos nada mais é do que retirar-lhes a autonomia de livremente dispor sobre os termos de seus contratos. Em outras palavras: exigir a obediência à regra da necessidade não é uma forma de solução da colisão entre direito fundamental e autonomia privada, já que essa autonomia estará necessariamente comprometida pelas próprias exigências dessa regra. Se aos particulares não resta outra solução que não a adoção das medidas estritamente necessárias, não se pode mais falar em autonomia. E, diante disso, as precedências *prima facie* estabelecidas pelo próprio Steinmetz perdem um pouco de seu sentido, já que mesmo que a relação contratual tenha sido estabelecida sob condições de igualdade fática (ou de sinceridade) e o direito fundamental envolvido tenha conteúdo patrimonial, se os termos do contrato não forem os menos gravosos a esse direito, o contrato será sempre nulo". DA SILVA, Virgílio Afonso. "Direitos Fundamentais e relações entre particulares". *Revista FGV.* Vol. 01, n.º 01, São Paulo, 2005, pp. 173-180.

uma vez que as relações negociais ocorrem entre particulares em desigualdade fática, bem como por se configurar o direito fundamental à proteção de dados pessoais como uma decorrência da proteção ao livre desenvolvimento da personalidade (direito fundamental de conteúdo pessoal).

Ocorre que a Lei Geral de Proteção de Dados, como marco civil vigente brasileiro, estabeleceu um regime jurídico diferenciado, entre cujas inovações, há um teste de ponderação a ser realizado pelas próprias empresas, antes de iniciarem suas atividades de tratamento de dados pessoais dos titulares com base no legítimo interesse.

As características desse arranjo jurídico e suas repercussões na temática da eficácia horizontal dos direitos fundamentais serão tratadas a seguir.

4. Análise do teste de ponderação do legítimo interesse (*lia*) sob a ótica da eficácia horizontal dos direitos fundamentais

Uma das principais novidades da Lei Geral de Proteção de Dados (Lei n. 13.709/2018) refere-se à exigência de tratamento de dados pessoais com embasamento em uma das hipóteses previstas nos artigos 7.º e 11 (denominadas de bases legais).

Segundo a natureza dos dados tratados, há dez bases legais para os dados pessoais comuns e oito para os dados pessoais sensíveis. E, como adverte Ricardo OLIVEIRA, e Márcio COTS[57], *"se o tratamento de dados de determinado Controlador não estiver enquadrado em uma base legal, ele é irregular e o Controlador poderá ser punido administrativamente ou processado judicialmente"*[58].

[57] OLIVEIRA, Ricardo e COTS, Márcio. *O Legítimo Interesse e a LGPD.* 2ª Ed. São Paulo: Thomson Reuters, 2021.

[58] Para ambas espécies de dados pessoais, há que se observar os princípios que regulamentam a proteção de dados no país dispostos no art. 6.º da Lei – boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

Dentre os propósitos legais, os quais versam desde a execução de políticas públicas até a proteção de bens jurídicos determinados (vida, incolumidade física e crédito), o *legítimo interesse* é a base legal que mais gera discussão, por seu grau de subjetividade.

O fundamento dessa hipótese legal gira em torno da necessidade de se criar uma medida essencial para o empreendedorismo e para a inovação das empresas, de forma a autorizá-las a realizar atividades de tratamento de dados pessoais, mesmo sem o consentimento dos titulares.

A versão brasileira do legítimo interesse recebeu forte influência do direito europeu, reconhecendo Ana Lúcia de Lyra TAVARES que houve uma "apreensão integradora[59]" do instituto ao direito pátrio. E, segundo Bruno BIONI, *"o legítimo interesse tem sido encarado como a mais flexível das bases legais de tratamento de dados no regime do direito europeu[60]"*.

Prossegue o autor explicando que o legítimo interesse serve como "válvula de escape para que as demais bases legais não fossem sobrecarregadas". Isso porque as quatro bases legais típicas (execução de contrato, obrigação legal, interesse público e proteção de interesses vitais do titular) são aplicáveis em situações específicas. Já em outros casos, seria desnecessário coletar novo consentimento ou por estar dentro de uma relação preestabelecida, ou quando terceiros não tivessem meios para obter tal tipo de autorização, ou por essa autorização inviabilizar o próprio tratamento de dados.

Sendo assim, com a emergência das tecnologias, o legítimo interesse teria alcançado *status* de uma nova "carta coringa regulatória". Daí porque, na Europa, critérios foram estabelecidos para trazer previsibilidade e segurança jurídica, além de evitar que o legítimo interesse

[59] TAVARES, Ana Lúcia de Lyra. *A crescente importância do direito comparado*. Disponível em: www.idclb.com.br/revistas/19/revista19%20(15).pdf. Acesso em 02.10.2022.

[60] BIONI, Bruno. *Proteção de Dados Pessoais.* A função e os limites do consentimento. 3ª Edição. São Paulo: Editora Forense, 2021, p. 238.

fosse uma "porta aberta" para contornar a obrigação de tratamento para outras bases legais[61].

Conquanto o debate sobre legítimo interesse na Europa aconteça há décadas, tem-se que, em sua primeira fase, não havia detalhes quanto aos critérios para sua aplicação. Em verdade, legítimo interesse se enquadrava como um conceito jurídico indeterminado. O que provocou aplicação divergente entre os países integrantes da União europeia.

Diante dessa situação, explica OLIVEIRA, Ricardo e COTS, Márcio (2021, p. 100) que:

> o Grupo de Trabalho do Artigo 29[62] para Proteção de Dados Pessoais, órgão da União Europeia dedicado ao estudo e à análise de temas ligados ao tratamento de dados pessoais na vigência da Diretiva 95/46/CE, norma anterior à GDPR, propôs o chamado Teste de Ponderação (balancing test), metodologia que serviria para se determinar qual dos interesses em jogo deve prevalecer ao se utilizar o Legítimo Interesse como base legal de tratamento.
>
> Ou seja,
>
> a propositura do Teste de Ponderação surgiu em 2014 e sugere a "necessidade de adotar uma abordagem pragmática que permita utilizar presunções práticas baseadas no que qualquer pessoa razoável consideraria aceitável nas mesmas circunstâncias (expectativas razoáveis) e baseadas nas consequências da atividade de tratamento de dados para as pessoas em causa ("impacto"). (Oliveira e Cots, 2021, p. 101).

---

[61] BIONI, Bruno. *Proteção de Dados Pessoais.* A função e os limites do consentimento. 3ª Edição. São Paulo: Editora Forense, 2021, p. 239.

[62] Nessa opinião do Grupo de Trabalho do Artigo 29, havia a previsão de um teste multifatorial com os seguintes passos: 1) Avaliação do interesse legítimo do controlador; 2) Impacto nas pessoas em causa; 3) Equilíbrio provisório; e 4) Garantias complementares para evitar qualquer impacto indevido na vida das pessoas em causa (ARTICLE 29, Data Protection Working Party, p. 33).

Como bem pondera BIONI, Bruno (2021, p. 240), o teste de ponderação *"trata-se de um denominador comum entre os titulares dos dados e os agentes reguladores e da cadeia de tratamento de dados diante da necessidade em assegurar previsibilidade à aplicação da base legal do legítimo interesse"*.

Com os devidos ajustes, esse debate se sucedeu também no Brasil. Bruno BIONI esclarece que, ainda que a base legal do legítimo interesse sequer constasse da primeira versão do anteprojeto da LGPD, já havia um debate frutífero entre, de um lado, parte do setor empresarial (com a defesa de que seria necessário transpor o modelo europeu, diante de um cenário de uso intensivo de dados e de ser contraproducente recorrer a todo momento ao consentimento) e, de outro, parte da academia e da sociedade civil (com o argumento de que a lei brasileira dispusesse do conceito de legítimo interesse acompanhado de requisitos para sua aplicação)[63].

Como forma de balancear os direitos em jogo, focou-se na modulação da discricionariedade dos agentes de tratamento de dados, através de previsão de parâmetros de aplicação no próprio texto da LGPD, de modo que se dedicou o Art. 10, exclusivamente, para a base legal do legítimo interesse. Eis a transcrição das previsões normativas para melhor compreensão[64]:

> Art. 7.º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: X – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.
>
> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas

[63] BIONI, Bruno. *Proteção de Dados Pessoais.* A função e os limites do consentimento. 3ª Edição. São Paulo: Editora Forense, 2021, p. 240.

[64] BRASIL. LEI FEDERAL N. 13.709, de 14/08/2018. Lei Geral de Proteção de Dados. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

> a partir de situações concretas […] § 1.º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados. § 2.º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse. § 3.º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

A estrutura normativa brasileira se deu nos moldes do *legitimate interests assessment* (*LIA*), aplicada no contexto europeu da GDPR, o qual segmenta o teste de ponderação em quatro fases.

Com efeito, no *LIA*, há a **Fase 1** – Legitimidade (cabe ao próprio controlador exercer esse juízo de valor da legitimidade do interesse), com seu correspondente, no Brasil, no Art. 10, *caput*, da LGPD, onde se prevê o fundamento a partir de situação concreta e para finalidade lícita. A **Fase 2** – Necessidade (requisitos constitutivos do legítimo interesse como adequação e minimização), com previsão equivalente no Art. 10, §1.º, da LGPD. A **Fase 3** – Balanceamento (legítima expectativa, direitos e liberdades fundamentais), também com previsões equivalentes na lei brasileira nos arts. 6.º, I, 7.º, IX e 10, II. Por fim, a **Fase 4** – Salvaguardas (garantias necessárias quando aplicado o legítimo interesse), com medidas de transparência, segurança, direito de oposição e pseudoanonimização (Art. 10, §§2.º e 3.º, da LGPD).

Para Bruno BIONI, a escolha do legislador brasileiro não foi um "transplante legal" daquilo que vinha sendo desenvolvido na Europa, embora concorde que a LGPD manteve uma divisão que *"arquiteta um circuito decisório que considera não apenas o juízo de valor a ser realizado pelo agente de tratamento de dados, mas, também, pelo próprio titular ou representantes de seu direito*[65]*"*.

---

[65] BIONI, Bruno. *Proteção de Dados Pessoais.* A função e os limites do consentimento. 3ª Edição. São Paulo: Editora Forense, 2021, p. 244.

A técnica brasileira do Teste de Ponderação, em síntese, verifica a legitimidade do interesse do controlador, através da enunciação de uma finalidade legítima dentro da articulação de uma situação concreta. Em seguida, deve demonstrar que vai tratar somente os dados necessários para essa finalidade e se não existe outra base legal mais adequada que o legítimo interesse. A essa finalidade, dois fatores foram acoplados pela lei: o respeito às legítimas expectativas do titular e aos seus direitos e liberdades fundamentais.

Vê-se que, a partir dessa fase, entra em cena o momento de efetivo sopesamento dos interesses dos controladores e dos titulares ou terceiros, através da ponderação entre legítimo interesse e legítimas expectativas (outro conceito jurídico indeterminado) ou entre legítimo interesse e direitos e liberdades fundamentais (Art. 10, II, da LGPD).

Para a primeira condicionante legal, Bruno BIONI entende que *"o legislador brasileiro amarrou duplamente os conceitos jurídico-indeterminados da legítima expectativa e do 'legítimo interesse' a um elemento bastante tradicional da cultura jurídica brasileira*[66]*"*. O autor se refere ao princípio geral da boa-fé, presente no Art. 6.º, *caput*, da LGPD, a qual cumpriria a função de modulação em torno da introjeção de um conceito jurídico indeterminado até então estranho no Brasil.

Tal solução prestigia o paradigma funcionalista do direito civil-constitucional, ao proporcionar um aparato jurídico orientado pelo marco civil vigente, cuja cláusula geral da boa-fé exerce a função de princípio dos princípios.

Contudo, as dificuldades para se garantir um nível adequado de proteção aos titulares são consideráveis, pois, conforme explicam Ricardo OLIVEIRA e Márcio COTS[67]:

---

[66] BIONI, Bruno. *Proteção de Dados Pessoais.* A função e os limites do consentimento. 3ª Edição. São Paulo: Editora Forense, 2021, p. 245-246.

[67] OLIVEIRA, Ricardo e COTS, Márcio. *O Legítimo Interesse e a LGPD.* 2ª Ed. São Paulo: Thomson Reuters, 2021, p. 114.

> No Brasil, inexiste uma teoria robusta sobre expectativas legítimas aplicada ao campo da privacidade. O conceito corrente considera que os sujeitos aderem a relações jurídicas específicas em virtude de representações manifestadas por terceiros, exclusivamente pela confiança depositada na própria relação jurídica, independentemente de uma maior ponderação sobre todas as consequências causais dessa adesão.

Como solução, esses autores defendem que a legítima expectativa do titular dos dados deve corresponder aos fins que lhe foram informados e para os quais consentiu com o tratamento de seus dados pessoais. Desse modo, há uma substituição de um conceito subjetivo para uma análise objetiva de correspondência entre a finalidade informada ao titular e aquela efetivamente dada às informações[68].

Daniel BUCAR e Mario VIOLA[69] acrescentam que se pode utilizar, ao mesmo tempo, a ferramenta gradativa do abuso de direito para filtrar casos de contrariedade a valores e princípios, delimitando qual interesse do controlador poderá ser legítimo.

Do mesmo modo, Bruno BIONI reflete sobre possibilidades e limites a partir das lentes do abuso de direito, a partir do direito de oposição previsto na LGPD: não se trata de um direito como exercício potestativo, mas decorrente de uma violação a uma de suas normas[70]. Nas palavras do autor:

> Em razão da autodeterminação informacional, a oposição justificada pela não identificação subjetiva da legítima expectativa ao titular dos dados, faz com que o exercício dessa oposição vincule o agente de

---

[68] OLIVEIRA, Ricardo e COTS, Márcio. *O Legítimo Interesse e a LGPD.* 2ª Ed. São Paulo: Thomson Reuters, 2021, p. 119.

[69] BUCAR, Daniel e VIOLA, Mario. "Tratamento de dados pessoais por "legítimo interesse do controlador": primeiras questões e apontamentos", *in Lei Geral de Proteção de Dados e suas repercussões no Direito Brasileiro*. 2ª Ed. São Paulo: Thomson Reuters Brasil, 2020, pp. 459/478.

[70] Art. 18, §2.º – O titular pode opor-se a tratamento realizado com fundamento em uma das bases legais de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei. BRASIL. LEI FEDERAL N. 13.709, de 14/08/2018. Lei Geral de Proteção de Dados. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

> tratamento a cessar, sob pena de estar violando umas das normas da LGPD. Contudo, esse direito do titular não é absoluto, devendo ser controlado pela cláusula geral do abuso de direito. O direito de oposição tende a ser relativizado frente a um interesse coletivo. É uma dialética normativa que coteja a autodeterminação informacional frente aos demais fundamentos da LGPD (art. 2.º)[71].

Portanto, através do crivo da legítima expectativa expressa pelo próprio titular dos dados pessoais, como decorrência de sua autodeterminação informacional, estabelece-se uma espécie de contraditório e ampla defesa, de modo a cumprir uma função de extrema importância para a qualidade desse teste de ponderação[72].

Adiante, no que diz respeito à segunda condicionante, a LGPD determina que o tratamento de dados pessoais somente pode ocorrer *"quando necessário para atender aos interesses legítimos do controlador ou de terceiro,* ***exceto*** *no caso de prevalecerem* ***direitos e liberdades fundamentais*** *do titular que exijam a proteção dos dados pessoais"* (Art. 7.º, IX) e *"o legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas […] respeitados* [adaptado] *os* ***direitos e liberdades fundamentais****, nos termos desta Lei"* (Art. 10, II).

Aqui, o texto pretendeu o implausível: alcançar um equilíbrio abrangente entre possíveis (até inevitáveis) colisões entre direitos fundamentais. Numa primeira leitura, tende-se a formular uma interpretação dessa condição excepcional como uma restrição ao tratamento de dados

---

[71] BIONI, Bruno. *Proteção de Dados Pessoais.* A função e os limites do consentimento. 3ª Edição. São Paulo: Editora Forense, 2021, p. 249.

[72] Segundo Sérgio Miguel José CORREIA, o direito de oposição do titular de dados pessoais apresenta uma conformação específica quando se refere à definição de perfis (*profiling*), de modo que "o teste de ponderação imposto pelo n.º 1 do art. 21.º do RGPD é diferente daquele que resulta da alínea f*)* do n.º 1 do art. 6.º do RGPD: não basta que o responsável demonstre que os interesses, direitos ou liberdades fundamentais do titular não prevaleceram sobre os seus interesses legítimos, mas que estes são, também, imperiosos". CORREIA, Sérgio Miguel José, "Direito de Oposição à Definição de Perfis", *in*: *Anuário da Proteção de Dados*, (coord. Francisco Pereira Coutinho e Graça Canto Moniz), CEDIS, 2022, p. 209.

pessoais com base no legítimo interesse do controlador nos casos em que prevaleçam direitos e liberdades fundamentais.

Ocorre que, mais adiante, o texto delimita tais direitos e liberdades aos que exigirem proteção dos dados pessoais.

Surge, então, um caso de aporia: há direitos e liberdades que não exijam proteção de dados pessoais? Ora, com o exercício desses direitos e/ou liberdades fundamentais, cada pessoa deixa rastros e registros de suas ações. Então, com base em qual critério se diferenciam situações que justifiquem ou não a proteção dos dados pessoais?

O que a previsão normativa pretendeu diferenciar foi o direito fundamental à proteção de dados pessoais dos demais direitos e liberdades fundamentais que podem ser afetados pelo tratamento de dados pelo controlador com base no legítimo interesse (como o direito à vida, à saúde, à segurança, etc).

Contudo, essa exceção legal não exclui a necessidade de sopesamento (de matização) entre o direito do controlador e dos titulares, para se reconhecer a legitimidade ou não do tratamento de dados a partir dessa base legal.

Nesse sentido, a pretensão do legislador de instituir um regime jurídico dentro de um marco civilista segmentado em fases não tem o condão de afastar ou contornar eventuais controvérsias quanto ao choque de direitos fundamentais em rota de colisão.

Apresentadas as características centrais para tratamento de dados pessoais com base no legítimo interesse do controlador, o problema de pesquisa deste artigo deve ser enfrentado: *O teste de ponderação, utilizado para o tratamento de dados pessoais baseados no legítimo interesse, inova na temática da vinculação dos particulares a direitos fundamentais em relação à metodologia desenvolvida por Robert Alexy?*

A resposta afirmativa justifica-se por três ordens de argumentos.

Primeiro, porque se refere a um sopesamento obrigatório entre direitos fundamentais, realizado por uma das partes envolvidas (o controlador), como condição prévia para o exercício de sua atividade

de tratamento de dados pessoais. É dizer, o marco civil vigente, tido como expressão imediata da proteção de direitos fundamentais, passou a se utilizar de uma técnica típica da hermenêutica constitucional.

Segundo, o teste de ponderação da LGPD ultrapassa a noção de ALEXY no que tange à ponderação como método hermenêutico, em razão de instituir um rito (procedimento) para o reconhecimento de qualquer tratamento válido com base no legítimo interesse. Com efeito, há necessidade, além do efetivo sopesamento dos direitos nas situações concretas, de documentação (para o registro das atividades de tratamento e dos possíveis impactos à proteção de dados pessoais) e de salvaguardas[73] (medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais). Desse modo, o teste de ponderação da LGPD fortalece a eficácia horizontal na perspectiva objetiva, pois se criou um rito auto-executável como *conditio sine qua non* para a validade da operação (procedimento) e se outorgou à ANPD (Autoridade Nacional de Proteção de Dados) poderes de fiscalização. Nesse contexto, portanto, há de considerar a íntima vinculação entre direitos fundamentais, organização e procedimento[74].

Por fim, mas não menos importante, esse teste de ponderação para aferição do legítimo interesse se direciona, primordialmente, às partes

[73] Art. 46, da LGPD: Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. BRASIL. LEI FEDERAL N. 13.709, de 14/08/2018. Lei Geral de Proteção de Dados. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

[74] SARLET, Ingo Wolfgang. *Proteção de dados pessoais e deveres de proteção estatais.* Conjur, publicado em 27.08.2021. Disponível em: https://www.conjur.com.br/2021-ago-27/direitos-fundamentais-protecao-dados-pessoais-deveres-protecao-estatais. Acesso em 03.10.2022.

envolvidas na relação civil[75] e não ao judiciário. De fato, cabe ao controlador realizar, de forma documentada, as fases da aferição da legitimidade, da necessidade, do balanceamento e das salvaguardas, após o que se garante o direito de oposição aos titulares como garantia de contraditório.

Atento a essa condição sensível, Daniel BUCAR e Mario VIOLA[76] ponderam: "*Quem controla o controlador: ANPD ou Judiciário?*".

Essa preocupação está de acordo com a velocidade das atividades de tratamento de dados pessoais numa economia de larga escala de fluxos informacionais. Assim, qual o modelo mais efetivo: A expertise da ANPD ou a cognição ampla, democrática e morosa da Justiça?

Danilo DONEDA e Mario VIOLA (no prelo) defendem que o judiciário estabeleça *"canais de cooperação com o órgão técnico responsável (ANPD), inclusive para fins de solicitação de parecer técnico sobre o tema ou a modalidade de tratamento de dados"*[77].

Portanto, o teste de ponderação (*LIA*) para fundamentar o tratamento de dados pessoais com base no legítimo interesse apresenta regime jurídico inovador. Ele incorporou, para o direito civilista, uma

---

[75] Nas relações laborais, a necessidade do tratamento de dados para a execução do contrato de trabalho não será o único fundamento de legitimidade, cabendo, segundo Sergio Coimbra HENRIQUES e João Vares LUÍS, a consideração de que "a invocação de um interesse legitimo para o tratamento pela entidade empregadora, nos termos da alínea f) do número 1 do art. 6.o do RGPD, implica que a própria finalidade do tratamento de dados pessoais deve ser tambem legitima, o tratamento deve ser realizado mediante métodos ou tecnologias especificas que, por referência a finalidade de tratamento, sejam de considerar estritamente necessários, adequados, proporcionais e aplicados da forma menos intrusiva possível para a privacidade e respeito de outros direitos fundamentais da pessoa singular. Este crivo, demarcadamente apertado, coloca sobre as entidades empregadoras o ônus de assegurar que se encontram aptas a demonstrar que tomaram as medidas adequadas a garantir o necessário equilíbrio entre a prossecução de uma finalidade (legitima) de tratamento de dados e o respeito pelas liberdades e direitos fundamentais dos trabalhadores e as expectativas razoáveis destes na relação com as suas entidades empregadoras". HENRIQUES, Sergio Coimbra e LUÍS, João Vares, "Consentimento e outros fundamentos de licitude para o tratamento de dados pessoais em contexto laboral", *in*: *Anuário da Proteção de Dados*, (coord. Francisco Pereira Coutinho e Graça Canto Moniz), CEDIS, 2019, p. 31.

[76] BUCAR, Daniel e VIOLA, Mario. "Tratamento de dados pessoais por "legítimo interesse do controlador": primeiras questões e apontamentos", *in Lei Geral de Proteção de Dados e suas repercussões no Direito Brasileiro*. 2ª Ed. São Paulo: Thomson Reuters Brasil, 2020, pp. 459/478.

[77] DONEDA, Danilo; VIOLA, Mario. *Relatório sobre a proteção de dados no Brasil*. *Policy Paper* (no prelo).

técnica própria da hermenêutica constitucional, para dar mais transparência, segurança e controle (*accountability* legal) nas cada vez mais frequentes atividades de tratamento dos dados pessoais por empresas, mesmo sem consentimento de seus titulares. Para além desse escopo, o *LIA* acoplou aos controladores obrigações de índole administrativa (expedição e disponibilização de relatórios), de segurança da informação (medidas de salvaguardas técnicas e operacionais) e de gestão de risco (plano para incidentes de vazamento, por exemplo), tudo sob a fiscalização da ANPD. O que demonstra que o *LIA* está inserido num sistema de proteção de dados a encargo das empresas.

E, nesse contexto, o papel do Poder Judiciário deve se alinhar aos novos tempos, na medida em que, no exercício de suas funções judicantes, o Estado-juiz deve considerar o auto-teste de ponderação pelos controladores e a atuação normativa e fiscalizatória da ANPD, de forma que se aprofundará seu ônus argumentativo quando for acionado em nome de último guardião dos direitos fundamentais.

5. Conclusão

No Brasil, a Lei Geral de Proteção de Dados inovou no sistema legal de proteção de dados ao visar a proteção dos direitos fundamentais de liberdade, da privacidade e do livre desenvolvimento da personalidade da pessoa natural, em pretensa harmonia com o desenvolvimento econômico tecnológico e a inovação, a livre iniciativa e concorrência e a defesa do consumidor.

Por outro lado, considerando que os dados se tornaram um dos bens mais preciosos na atualidade (chegam a ser equiparados ao petróleo) e sua relevância para todas as esferas da vida social, econômica, política, cultural, ambiental e jurídica, há a necessidade de se assegurar a eficácia do direito fundamental à proteção de dados pessoais também na esfera das relações entre particulares, em especial por se tratarem de atores privados dotados de elevado poder econômico e social.

Nesse sentido, o tratamento de dados pessoais, para que respeite os direitos individuais dos titulares e para que não seja utilizada para embaraçar o empreendedorismo no país, deve obedecer princípios estabelecidos e somente ser realizado quando atender a requisitos legais bem delimitados.

Uma dessas bases legais é o Legítimo Interesse, através do qual as empresas, como controladoras dos dados pessoais dos titulares, podem realizar operações de tratamento independentemente do encaixe em qualquer outra base legal e mesmo sem consentimento da pessoa titular dos dados.

Como instrumento de equilíbrio dessa operação em relação aos direitos de privacidade e de personalidade dos titulares de dados pessoais, a lei previu que somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados, cabendo ao controlador garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

No Brasil, houve uma a escolha do legislador em não fazer um transplante legal daquilo que vinha sendo desenvolvido no contexto europeu, mas sim, em desenvolver um modelo de teste de legítimo interesse em fases dispostas no art. 10 da LGPD. Essa estratégia normativa corresponde a uma corporificação textual de uma solução possível para as hipóteses de conflitos de direitos fundamentais entre particulares.

Com isso, pode-se mobilizar esse teste de ponderação previsto na LGPD para uma discussão sobre a eficácia horizontal dos direitos fundamentais.

Nesse contexto, este artigo pretendeu responder ao seguinte problema: *O teste de ponderação, utilizado para o tratamento de dados pessoais baseados no legítimo interesse, inova na temática da vinculação dos particulares a direitos fundamentais em relação à metodologia desenvolvida por Robert Alexy?*

A resposta afirmativa justificou-se, em síntese, pelos argumentos adiante: primeiro, porque se refere a um sopesamento obrigatório entre direitos fundamentais, realizado pelo controlador, como condição

prévia para o exercício de sua atividade de tratamento de dados pessoais. É dizer, o marco civil vigente, tido como expressão imediata da proteção de direitos fundamentais, passou a se utilizar de uma técnica típica da hermenêutica constitucional. Segundo, esse teste de ponderação ultrapassa a noção de Alexy no que tange à ponderação como método hermenêutico, em razão de instituir um rito (procedimento) para o reconhecimento de qualquer tratamento válido com base no legítimo interesse. Com efeito, há necessidade, além do efetivo sopesamento dos direitos nas situações concretas, de documentação (para o registro das atividades de tratamento e dos possíveis impactos à proteção de dados pessoais) e de salvaguardas (medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais). Desse modo, o teste de ponderação da LGPD fortalece a eficácia horizontal na perspectiva objetiva, pois se criou um rito auto-executável como *conditio sine qua non* para a validade da operação (procedimento) e se outorgou à ANPD (Autoridade Nacional de Proteção de Dados) poderes de fiscalização. Nesse contexto, portanto, há de considerar a íntima vinculação entre direitos fundamentais, organização e procedimento. Por último, esse teste de ponderação se direciona, primordialmente, às partes envolvidas na relação civil e não ao judiciário. De fato, cabe ao controlador realizar, de forma documentada, as fases da aferição da legitimidade, da necessidade, do balanceamento e das salvaguardas, após o que se garante o direito de oposição aos titulares como garantia de contraditório.

Portanto, nesse contexto, o papel do Poder Judiciário deve se alinhar aos novos tempos, na medida em que, no exercício de suas funções judicantes, o Estado-juiz deve considerar o auto-teste de ponderação pelos controladores e a atuação normativa e fiscalizatória da ANPD, de forma que se aprofundará seu ônus argumentativo quando for acionado em nome de último guardião dos direitos fundamentais.

Regulamento Geral sobre a Proteção de Dados e o mercado de dados – Mercado de dados 1.0 e a licitude da partilha de dados (pessoais) através de serviços de intermediação de dados no âmbito do Regulamento de Governação de Dados, por via do consentimento do titular dos dados – uma imposição de base legal?

Patrícia Carneiro[1]

Resumo: Partindo do pressuposto que é transversalmente assumida a existência de um mercado de dados pessoais *de facto*, propomo-nos a analisar os desenvolvimentos legislativos que surgem no sentido de regular essa realidade, em especial, o Regulamento de Governação de Dados, que introduz o serviço de intermediação de dados, concretamente, através da partilha de dados. Neste trabalho, limitamos a nossa análise à identificação de uma estrutura, legalmente assumida, de mercado de dados, e, então, ponderamos se o legislador europeu, no Regulamento de Governação de dados, procurou impor o consentimento do titular enquanto fundamento jurídico para partilha dos seus dados pessoais.

Palavras-chave: *Proteção de dados pessoais; mercado de dados; base de licitude; RGPD.*

[1] Pós-Graduação em Direito e Tecnologia da Faculdade de Direito da Universidade Católica – Escola do Porto.

Abstract: Assuming that a data market is a well-established *de facto* reality, our aim is to analyse the legal developments emerged to regulate said market. Specifically, our focus is the Data Governance Act, which introduces, among others, the figure of data intermediation service providers, namely, via a data sharing concept. For purposes of this article, we have limited our analysis to the identification of a legally assumed data market structure, whilst wondering if the european legislator have had the intention of imposing data subjects' consent as a legal basis for sharing their personal data.

Key words: *Data protection; data market; legal basis; GDPR.*

1. Introdução

O tema escolhido parte de um trabalho prévio de investigação por parte da autora, através do qual se pretendeu sobressair a existência de um mercado de dados pessoais não regulado e demonstrar que a sua regulação é uma pretensão assumida do legislador europeu no Regulamento de Governação de Dados[2], entretanto aprovado.

Nos dias que correm, é patente o cenário em que os grandes operadores de mercado aproveitam a sua posição para obter, valorizar e monetizar dados pessoais, ainda que tal seja feito em prejuízo do direito à proteção de dados do respetivo titular, ou dos seus interesses. Desde logo, é-nos possível observar e registar que o titular de dados pessoais poucas ou nenhumas vantagens económicas retira de um mercado obscuro de dados pessoais. Um mercado não regulado e, consequentemente, não monitorizado, camuflado por floreados legais de difícil compreensão, explorado por aqueles grandes operadores através da obtenção e

[2] Regulamento (UE) 2022/868 do Parlamento Europeu e do Conselho de 30 de maio de 2022 relativo à governação europeia de dados e que altera o Regulamento (UE) 2018/1724 (Regulamento Governação de Dados). OJ L 152, 3.6.2022. Doravante, apenas "Regulamento Governação de Dados".

monetização em massa de dados pessoais. Por outro lado, aqueles modelos de negócio, não sendo uma novidade, mas, ao invés, uma preocupação crescente[3], são conhecidos por potenciar a perda de controlo sobre os dados pessoais, pelo seu titular, e, bem assim, minar a confiança do titular na partilha da sua informação. Esta é, no mais, um problema reconhecido da Comissão Europeia no quadro da estratégia europeia para os dados[4] e, que, como tal, procurou colmatar com o Regulamento de Governação de Dados.

Neste artigo, procuramos esquematizar o raciocínio por trás das afirmações mencionadas supra, somando-se-lhe o nosso foco na relação entre o Regulamento de Governação de Dados e o Regulamento Geral sobre a Proteção de Dados[5]. O Regulamento de Governação de Dados, por ser um pilar daquela estratégia europeia de dados, que, cremos, nos permite falar de um mercado 1.0 de dados pessoais, consequência da regulação do mercado instituído de *facto*. A este respeito, procuraremos explorar o conceito de "Personal Data Store" e a sua importância na emergência daquele mercado regulado – chamamos-lhe, "mercado regulado 1.0" –, partindo de uma análise teórica sobre o quadro técnico-jurídico aplicável, até ao desenho e análise de um caso de estudo. Com este caso de estudo, pretendemos não só demonstrar a

[3] Veja-se a opinião 9/2016 da Autoridade Europeia para a Proteção de Dados (doravante, "EDPS"): "EDPS Opinion on Personal Information Management Systems Towards more user empowerment in managing and processing personal data" [Em linha]. (20-10-2016) [Consult. 11-03- 2023]. Disponível em WWW: <https://edps.europa.eu/sites/edp/files/publication/16--10-20_pims_opinion_en.pdf>. Neste documento, a EDPS, reconhecendo o quadro que descrevemos, em que o titular de dados pessoais tem cada vez menos controlo sobre a sua pegada digital, preconiza a adoção e implementação de um Sistema de Gestão de Informação Pessoal que tem como objetivo primeiro empoderar o titular dotando-o de ferramentas que lhe permitem não só maior controlo sobre os seus dados pessoais, mas, consequentemente, participar ativamente e beneficiar – social e economicamente – da monetização dos seus dados, aumentando o seu grau de confiança na partilha da sua informação com terceiros, e, assim, permitir a concretização dos objetivos europeus direcionados à livre e ágil circulação de dados.

[4] Com(2020) 66 final.

[5] Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. OJ L 119, 4.5.2016, pp. 1-88. Doravante, apenas "Regulamento Geral sobre a Proteção de Dados" ou "RGPD".

estrutura de mercado regulado existente, reflexo dos recentes avanços legislativos, mas, também, que existem aspetos pouco explorados da formulação legal atual que têm como consequência a criação de uma margem para dúvidas de interpretação capazes de impactar o comércio jurídico e, consequentemente, económico.

Neste sentido, entendemos por pertinente atentar na articulação entre aquele Regulamento e o RGPD, por o texto do Regulamento de Governação de Dados, também instituído para aumentar o nível de confiança na partilha de dados pessoais pelo respetivo titular, expor inconsistências com a tutela do direito à proteção de dados pessoais. Como têm vindo a salientar as autoridades de controlo e de supervisão[6], a necessidade de aumentar os níveis de disponibilização de dados pessoais pelos titulares em prol do Mercado Único Digital[7], não pode traduzir-se na subversão da tutela de um direito de personalidade universalmente reconhecido – o direito à proteção de dados pessoais[8]. Em particular, sobressaímos as dificuldades de interpretação relacionadas com a garantia do princípio da licitude prevista na alínea a) do n.º 1 do art. 5.º do RGPD, entendendo que o Regulamento de Governação de Dados poderá ter procurado impor o consentimento como fundamento legal[9] para a partilha de dados pessoais pelo titular ou quem, de uma forma geral, os detém.

---

[6] Ainda a respeito da Proposta de Regulamento de Governação de Dados, veja-se, por exemplo, o ponto 19 a p. 8 do documento "EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act)" [Em Linha]. Disponível em WWW: <https://edpb.europa.eu/system/files/2021-03/edpb-edps_joint_opinion_dga_en.pdf>.

Com(2020) 66 final, p. 8.

[7] COM(2020) 767 final – SEC(2020) 405 final – SWD(2020) 296 final, p.e., p. 1, pp. 8*ss* e p. 17.

[8] Veja-se, ainda, o comentário da Commission Nationale de l'Informatique et des Libertés – "CNIL" ao Regulamento de Governação de Dados, na sua página na Internet: < https://www.cnil.fr/en/european-strategy-data-cnil-and-its-counterparts-comment-data-governance-act-and--data-act> [Consult. 11-03-2023]. Dali, resulta a óbvia a preocupação direcionada à supervisão da articulação entre aquele Regulamento e o Regulamento Geral sobre a Proteção de Dados, de forma a assegurar que este último não é comprometido quanto ao nível de proteção que confere aos titulares de dados pessoais.

[9] Al. a) do n.º 1 do art. 6.º do RGPD.

2. Um mercado europeu de dados – uma abordagem subtil?

2.1. Enquadramento da emergência de um mercado de dados

A aposta da União Europeia (U.E.) num Mercado Único Digital movido por dados, veio novamente destacada na comunicação da Comissão Europeia sobre a respetiva estratégia europeia que servirá os próximos cinco anos. Daquela comunicação, foi-nos possível depreender a vontade de a U.E. se tornar um "modelo líder" para a sociedade na economia de dados, através da valorização destes bens[10], incluindo, dados pessoais – "Data is the lifeblood of economic development", é uma das expressões que podemos encontrar naquela Comunicação. A este respeito, para agilizar o enquadramento sobre o Mercado Único Digital, remetemos o leitor para o que havíamos escrito a este respeito:

«Em 2013, a Comissão Europeia estudava já como fazer com que os dados pessoais "funcionassem da melhor forma para a economia digital europeia". Em maio de 2015, nasce o Mercado Único Digital – ou "Digital Single Market" ("DSM") –, marcado pela consciência de que "a internet e as tecnologias digitais estão a transformar a nossa vida (…) à medida que se integram mais profundamente em todos os setores da nossa economia e da nossa sociedade"[11], a par de renovadas preocupações relacionadas com a proteção de dados pessoais que o legislador sabe não poder descurar e, concretamente, o RGPD.»[12]

Portanto, o propósito de a U.E. se tornar um "modelo líder" não surpreende quando não é novidade que existe, num primeiro momento, um mercado sedimentado e não regulado de dados pessoais, como já tivemos, igualmente, oportunidade de abordar[13]. Nesta senda, apelamos

[10] Com(2020) 66 final, p. 1.

[11] COM(2015) 192 final, pp. 420 e 423– onde também se reconhece que "daqui a menos de uma década, a maior parte da atividade económica dependerá de ecossistemas digitais que integrem infraestruturas digitais, hardware e software, aplicações e dados.".

[12] P. CARNEIRO, Patrícia – «"Coisificação" dos Dados Pessoais no Âmbito das Relações Contratuais» [Em linha]. In: *Privacy and Data Protection Magazine*, 02 (2021), p. 111. Disponível em WWW: <Revista_Privacy_and_Data_Protection_Magazine_N2.pdf (europeia.pt)>.

[13] P. CARNEIRO, Patrícia – cit., pp. 102ss.

à atenção do leitor para uma análise realizada e que continua a ser atual e ilustrativa de tal mercado de dados pessoais sedimentado, pautado por modelos de negócio assentes na partilha de dados em troca de um preço. Em 2019, vimos o relatório anual de contas da Facebook, Inc. (agora, Meta), relativo ao ano fiscal de 2017, e percebemos que a sua principal fonte de receita foi gerada pela publicidade direcionada aos seus utilizadores por terceiros à sua plataforma[14]. Note-se[15]:

"(…) entre os anos de 2013-2017 associado a um aumento médio anual de receitas de 47%: de 7,87 para 40,65 mil milhões de dólares americanos, (…) 39,94 mil milhões dessas receitas advêm da publicidade direcionada contratada por terceiros (…)".

Esta realidade, continua visivelmente inalterável – veja-se o "[i] ncome [s]tatement" da Meta, partilhado no último trimestre de 2022[16].

Tal como a outrora Facebook, agora Meta, este mercado, digital por natureza, subjaz aos prestadores de serviços e fornecimento de conteúdos digitais em geral, e esteve essencialmente relacionado com os modelos de negócio considerados gratuitos, mas que consistiam no fornecimento ativo de dados por parte dos consumidores finais. Este mercado, emergiu a par da chamada revolução 4.0, caracterizada pelo impacto do progresso tecnológico na economia e sociedade em geral, e, em particular, pela facilidade da criação de monopólios de dados motivada pela falta de resposta legal adequada em matéria de proteção de dados pessoais. A Comissão Europeia também o admite quando se refere aos monopólios de informação e à distribuição do poder de

[14] Substantially all of our revenue is currently generated from third parties advertising on Facebook (…) For 2017, 2016, and 2015, advertising accounted for 98%, 97% and 95%, respectively, for our revenue. O relatório anual de contas encontra-se diretamente na página na Internet: < https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/FB_AR_2017_FINAL.pdf>. [Consult. 28- 01-2019]; e, juntamente com os relatórios de contas relativos a anos fiscais precedentes, na página na Meta Investor Relations:. [Consult. 28-01-2019]. 14 Idem, Parte II, item 6 – "Selected Financial Data" e item 7 – "Management's Discussion and Analysis of Financial Condition and Results of Operations".

[15] P. CARNEIRO, Patrícia – cit., p. 107.

[16] Na página na Internet: < https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/FB_AR_2017_FINAL.pdf>. [Consult. 11-03-2022].

mercado, no sentido de que são os grandes operadores nesse mercado que, unilateralmente, estipulam as regras e as condições de acesso e uso da informação[17]. Pois, que, não obstante a pertinência do Regulamento Geral sobre a Proteção de Dados no sentido de munir os titulares de dados pessoais de ferramentas que lhe permitem maior controlo sobre os seus dados pessoais, não devemos desconsiderar que o direito à proteção de dados pessoais, no contexto do mercado de dados não regulado, não teve impacto imediato. Pelo contrário, observamos outros ramos do Direito serem chamados à colação para dar resposta à necessidade de tutelar o titular de dados pessoais, como o Direito da Concorrência[18] e o Direito do Consumo[19]. Neste seguimento, parece-nos pertinente que, naquela mesma comunicação, a Comissão Europeia tenha manifestando o objetivo de criação de um mercado único de dados e o respetivo modelo de governação[20], ciente da necessidade de assumir as rédeas deste novo mercado económico em expansão.

2.2. Sobre o impacto da estratégia europeia de governação nas garantias dos titulares dos dados pessoais

De facto, e como temos vindo a defender, a definição de um modelo de governação de dados que tem em conta o cerne do direito à proteção de dados pessoais, é essencial. Basta refletirmos sobre a origem histórica do direito à proteção de dados pessoais no contexto europeu e o núcleo de posições jurídicas que visa tutelar:

---

[17] Com(2020) 66 final, p. 8.

[18] Exemplo flagrante é a decisão (Ref.ª B6-22/16) da Autoridade Alemã da Concorrência (Bundeskartellamt), que inicia, oficialmente, a discussão sobre a gratuitidade dos serviços prestados pela então Facebook, Inc. e a necessidade de o titular dos dados pessoais fornecer o seu consentimento informado no contexto em apreço.

[19] Sendo referência fulcral a Diretiva (EU) 2019/770 do Parlamento Europeu e do Conselho de 20 de maio de 2019 sobre certos aspetos relativos aos contratos de fornecimento de conteúdos e serviços digitais OJ L 136, 22.5.2019, pp. 1-27, que veio reconhecer, explicitamente, no quadro normativo europeu, a atribuição de valor económico aos dados pessoais partilhados pelos consumidores de conteúdos e serviços digitais.

[20] Com(2020) 66 final, pp. 4-5.

"Na sua essência repousa um conjunto de posições ativas do titular dos dados, como o direito a conservar informação pessoal longe da invasão de terceiros não autorizados, o direito a definir o âmbito do acesso a essa informação pessoal por terceiros (sejam estes entidades públicas ou privados), o direito a definir e a balizar as condições de tratamento dos seus dados, o direito a conhecer quem tem acesso e em que termos aos seus dados; e, ainda, o direito a manter-se desconhecido pela comunidade. (…) todos os direitos que cabem aos "cidadãos" sobre os seus dados pessoais estão associados a um agregado de princípios que vêm sendo igualmente considerados a respeito do tratamento desses mesmos dados. Estes princípios funcionam como meios e ferramentas legais que visam atribuir o controlo dos dados ao respetivo titular contra, não só o acesso e divulgação indevidos por terceiros, mas, igualmente, a sua centralização, fragmentação ou dissipação de informação."[21]

É neste sentido também, que a Comissão Europeia, na apresentação da estratégia europeia para os dados suprarreferida, identifica a "governação de dados"[22] como sendo um dos problemas que estão a constranger a U.E. de atingir o seu potencial máximo no que diz respeito à economia de dados. Particularizando a necessidade de adoção de estruturas e modelos organizativos que permitam a operacionalização daquilo a que chama de "espaços de dados"[23] [24] em conformidade

[21] PEREIRA CARNEIRO, Patrícia Filipa (2019) – «"Coisificação" dos Dados Pessoais no Âmbito das Relações Contratuais», Tese de mestrado em Direito. Porto, Faculdade de Direito da Universidade do Porto, pp. 27*ss*.

[22] Com(2020) 66 final, p. 8.

[23] "The spaces will include: (i) the deployment of data-sharing tools and platforms; (ii) the creation of data governance frameworks; (iii) improving the availability, quality and interoperability of data – both in domain-specific settings and across sectors. Funding will also support authorities in the Member States in making high value data sets available for reuse in the different common data spaces" – Com(2020) 66 final, p. 17.

[24] Que, na sua globalidade, consistirão no Mercado Único Digital. Cfr. Com(2020) 66 final, pp. 4*ss*: "(…) where personal as well as non-personal data, including sensitive business data, are secure and businesses also have easy access to an almost infinite amount of high-quality industrial data, boosting growth and creating value, while minimising the human carbon and environmental footprint. It should be a space where EU law can be enforced effectively, and where all data-driven products and services comply with the relevant norms of the EU's single market."

com a legislação europeia já em vigor, como o Regulamento Geral sobre a Proteção de Dados. O Regulamento de Governação de Dados surge nesta sequência, como um pilar daquela estratégia europeia, com o objetivo de criar as condições necessárias ao desenvolvimento de um sistema confiável de partilha de dados[25].

Aqui chegados, cumpre-nos assinalar as incongruências que sentimos nas preocupações que a Comissão Europeia tem vindo a partilhar neste contexto e que conduzem as suas ações, entre as quais, o Regulamento de Governação de Dados.

Se é indiscutível que, num primeiro momento, aquelas ações não desfocaram da necessidade de atribuir aos titulares maior controlo sobre os seus dados pessoais[26], na sua comunicação sobre a estratégia europeia para os dados, a Comissão Europeia demonstra preocupar-se em atribuir aos negócios maior controlo sobre os "seus dados"[27]. O que tem como potencial o descurar da necessidade de garantir que um titular de dados pessoais não tem ao seu alcance as ferramentas que lhe permitam o controlo efetivo sobre esses mesmos dados. Este risco torna-se ainda mais prevalente quando se parte de uma ideia utópica de que as organizações irão usar os dados pessoais sob a sua responsabilidade apenas para "fazer o bem", em prol da economia e da sociedade em geral, enquanto desconsideram interesses próprios. O mesmo vale para as entidades de natureza pública, visto que, ainda que se tenha em boa conta a ideia de um mercado aberto relativamente aos dados criados "com o dinheiro público e em prol do benefício público"[28], é perigosa a conceção da "supremacia

[25] V. a Página da Comissão Europeia na Internet relativa ao "Data Governance Act": [Em linha]. 13-07-2022. [Consult. 24-04.2023]. Disponível em WWW: <https://digital-strategy.ec.europa.eu/en/policies/data-governance-act>.

[26] Não obstante, como vimos, o Regulamento Geral sobre a Proteção de Dados ser um elemento-chave nesta afirmação, até enquanto peça integrante de um dos três pilares do Mercado Único Digital – cfr. COM(2015) 192 final; em 2011, Purtova defendia que a Diretiva de Proteção de Dados Pessoais teve como grande objetivo atribuir ao indivíduo (titular de dados pessoais) o controlo sobre os mesmos. Cf. PURTOVA, N. N. – Property rights in personal data: A European perspective. [Em linha]. Oisterwijk: BOXPress BV, 2011, p. 197. [Consult. 04-08-2019].

[27] Com(2020) 66 final, p. 2.

[28] Com(2020) 66 final, p. 7.

moral do Estado e organizações"[29]. Especialmente, quando consideramos que os ideais de privacidade começaram a delinear-se face ao impacto do desenvolvimento tecnológico sobre os direitos e liberdades fundamentais do homem, associada à ideia de vigilância da pessoa[30]. Estas, são apenas algumas das considerações que deverão, em nosso entender, pautar a análise dos vários riscos e desafios associados ao desenvolvimento e implementação de um modelo de mercado de dados pessoais nos diferentes planos do governo de uma sociedade[31]. Também

[29] Ainda que o termo tenha sido usado para retratar o cenário em que as organizações privadas e estatais se consideram titulares de um direito a obter a informação relativa a um individuo que seja necessária da perspetiva dos interesses públicos prosseguidos, a ideia é a de que a privacidade do individuo sempre cederá perante um interesse público superior. V. C. LAUDON, Keneth – Markets and Privacy. NYU: IOMS: Information Systems Working Papers (Topic) (1996), pp. 3ss. Disponível em WWW: <https://www.semanticscholar.org/paper/Markets-and-privacy--Laudon/b8f5938bb25ac559ac2854c50cf8cf365b09ba04>.

[30] V. p.e.: Ponto 180 da página 41 e no ponto 184 da página 42 do Relatório sobre a 26.ª Comissão sobre os Direitos do Homem conduzida nas Nações Unidas – Commission on Human Rights Report on the twenty-seventh session [Em linha]. Doc. E/4949 E/CN.4/1068 (22-02/26--03-1971) [Consult. 23-07-2021]; CONSELHO EUROPEU – Explanatory Report to the Convention for the protection of individuals with regard to automatic processing of personal data [Em linha]. European Treaty Series. 108, (28-01-1981); e, ASSEMBLEIA PARLAMENTAR – Recommendation 509 (1968): Human Rights and modern scientific and technological developments [Em linha]. Documentos que apoiam a contextualização do Tratado n.º 108 (ou Convenção 108), em vigor desde o ano de 1985, mas, também, iniciativas legislativas prévias, de base em matéria de Direitos Fundamentais, como o direito à proteção da vida privada das pessoas a Declaração Universal dos Direitos do Homem, proclamada pela Assembleia Geral das Nações Unidas em 1948, e a Convenção Europeia dos Direitos do Homem, que entrou em vigor em 1953.

[31] Económico, social, político, legal, ético e moral. Planos que acabam, até, reconhecidos, pelo menos em parte e ainda que indiretamente, pela Comissão Europeia, na estratégia comunicada – Com(2020) 66 final, pp. 6ss. Por exemplo, a respeito dos deságios tecnológicos e, concretamente, da interoperabilidade e qualidade dos dados. Para garantir a valorização dos dados pessoais e a sua comunicação/transferência ágil, é preciso que estejam acessíveis as ferramentas que possibilitem que os "pacotes de informação" circulem dentro do percurso acautelado, nomeadamente, através de um formato estruturado que permita a sua interoperabilidade.

estas são as considerações[32] que nos levam a procurar compreender o impacto do modelo de governação preconizado no respetivo Regulamento de Governação de Dados na licitude do tratamento de dados pessoais nos chamados "espaços de dados", e, assim, nas garantias dos titulares dos dados pessoais, tal como introduzidos no Regulamento Geral sobre a Proteção de Dados. Porquanto, como veremos, cremos que o Regulamento de Governação de Dados acaba por impor o consentimento enquanto fundamento legal para o tratamento de dados pessoais[33], recordando que o elenco do art. 6.º do Regulamento Geral sobre a Proteção de Dados não atribuiu prioridade normativa ao consentimento.

---

[32] Juntamente com a análise do procedimento legislativo de base à aprovação do Regulamento Governação de Dados, que evidencia a pobre articulação inicial, do texto da Proposta da Comissão Europeia, com o regime da licitude no tratamento de dados pessoais previsto no Regulamento Geral sobre a Proteção de Dados, em particular, o consentimento enquanto fundamento de licitude para o tratamento de dados pessoais. Veja-se, o Relatório do Parlamento Europeu sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo à governação de dados (Regulamento Governação de Dados) (COM(2020)0767 – C9-0377/2020 – 2020/0340(COD)). Atente-se, por exemplo, nas alterações sugeridas ao considerando (21), a respeito da noção de detentores de dados *versus* titulares de dados, e da consequente necessidade de trabalhar o consentimento enquanto base de licitude – por exemplo, alterações sugeridas ao considerando (38) ou ao art. 2.º, com a introdução do conceito de consentimento. Por outro lado, não obstante a versão em vigor do Regulamento Governação de Dados ser mais madura quanto a esta articulação de regimes, como vimos, a necessidade de garantir a consistência com o Regulamento sobre a Proteção de Dados continua a ser uma preocupação – remetemos novamente o leitor para o comentário da CNIL – cit.

[33] "A presente iniciativa abrange diferentes tipos de intermediários de dados, que tratam de dados tanto pessoais como não pessoais. Por conseguinte, a interação com a legislação em matéria de dados pessoais reveste-se de especial importância. Com o Regulamento Geral sobre a Proteção de Dados (RGPD) e (…) a UE criou um quadro jurídico sólido e fiável de proteção de dados pessoais que é um modelo para o mundo. (…) A presente proposta (…) [v]isa facilitar a partilha de dados, nomeadamente reforçando a confiança nos intermediários de partilha de dados que se espera venham a ser utilizados nos diferentes espaços de dados. Não tem por objetivo conceder, alterar ou suprimir direitos substanciais de acesso e utilização de dados;(…)" – é o que resulta da p. 1 da exposição de motivos da Proposta de Regulamento de Governação de Dados, COM(2020) 767 final. Ao mesmo tempo, a então proposta e agora Regulamento de Governação de Dados, como vamos ver adiante neste artigo, refere que a categoria de intermediários que foca o seu serviço nos dados pessoais, "(…) prestam assistência às pessoas no exercício dos seus direitos ao abrigo do Regulamento (UE) 2016/679, nomeadamente ajudando-as a gerir o seu consentimento (…)." – sublinhado nosso; bem com, aconselham as "(…) pessoas sobre o consentimento relativo a diferentes utilizações dos seus dados e a realização de verificações do dever de diligência junto dos utilizadores dos dados antes de lhes permitir contactar os respetivos titulares, a fim de evitar práticas fraudulentas." – considerando (23) daquela Proposta e respetivo Regulamento aprovado, novamente, com sublinhado nosso.

3. A relação entre o Regulamento de Governação de Dados e as "Personal Data Stores" – mercado regulado 1.0

3.1. Introdução ao modelo de governação implementado: as "personal data stores"

Como vimos, bem cedo na conceptualização e desenvolvimento de um Mercado Único Digital, a Comissão Europeia compreendeu a necessidade de salvaguardar que o titular deve estar dotado dos mecanismos adequados a controlar os seus dados pessoais, de forma a aumentar a sua confiança no comércio jurídico, e, assim, contribuir com a partilha dos seus dados pessoais. Ou seja, não são novos os resultados apresentados em 2020 no relatório da avaliação de impacto da Proposta de Regulamento de Governação de Dados, que apontam para o "problema" de o titular não confiar na partilha dos seus dados pessoais[34].

Por outro lado, é claro que a pretensão do legislador europeu não é regular massiva e detalhadamente o quadro dentro do qual os grandes operadores no mercado de dados podem atuar[35], mas, ao invés, permitir um contexto de "experimentação" ao nível dos quadros regulatórios aplicáveis. Os recentes avanços legislativos que consideramos pertinentes a este respeito, em particular, o Regulamento de Governação de Dados, evidenciam a adoção de um modelo de mercado minimamente estruturado – aquele a que chamamos mercado 1.0.

Em agosto de 2015, foi divulgado um relatório[36] sobre "personal data stores" que a Comissão Europeia encomendou à Cambridge Judge Business School. De forma similar aos "PIMS" – "Personal Information

[34] COM(2020) 767 final – SEC(2020) 405 final – SWD(2020) 296 final, – cit., pp. 11*ss*.

[35] Com(2020) 66 final, p. 12.

[36] Disponível na Página da Internet da Comissão Europeia. Study on Personal Data Stores conducted at the Cambridge University Judge Business School – In Página da Internet da Comissão Europeia [Em linha]. 7-08-2015. [Consult. 27-11-2022]. Disponível em WWW: <https://digital-strategy.ec.europa.eu/en/library/study-personal-data-stores-conducted-cambridge-university-judge-business-school>.

Management Systems"[37], as "personal data stores" surgem enquanto mecanismo viável para aumentar a confiança do consumidor e, consequentemente, o seu envolvimento, no Mercado Único Digital, com o intuito de limitar os constrangimentos à livre circulação de dados entre os Estados-Membros e, nos termos ali vertidos, facilitar uma economia baseada no conhecimento transversal de informação.

O conceito de "personal data stores" diz respeito a uma tecnologia, potencialmente associada a um serviço de computação em nuvem (ou *cloud*), capaz de oferecer aos indivíduos (titulares de dados pessoais), a possibilidade de recolher, armazenar, atualizar, analisar, corrigir e/ou partilhar dados pessoais com as características técnicas necessárias a garantir tanto a gestão como a licitude da informação[38], atribuindo aos respetivos titulares maior controlo sobre os seus dados pessoais.

Esta solução[39], seria capaz de alterar o paradigma de como os dados das pessoas circulam de forma descontrolada no comércio jurídico, distribuídos em função das forças do mercado, transportando-os dos "silos" de informação sobre a alçada de uma diversidade de entidades[40], desde os grandes operadores comerciais privados ao setor público, para um modelo em que o titular passaria a ser o centro de toda a gestão da sua informação e respetivo ecossistema. Paralelamente, também as empresas e demais utilizadores da informação do titular dos dados gozariam de um sistema mais transparente, com mais estabilidade do ponto de

---

[37] Em português, Sistemas de Gestão de Informação Pessoal. EDPS Opinion on Personal Information Management Systems Towards more user empowerment in managing and processing personal data – cit.

[38] Veja-se no relatório da Cambridge University Judge Business School cit., p. 12.

[39] Segundo o referido relatório da Cambridge Judge Business School.

[40] *Idem*, pp., 4, 11*ss*. Tem que ver com a monopolização da informação e a descentralização do modelo de governação de dados que se pretendem combater. A ideia máxima, tanto das "personal data stores", como das PIMS, é a de maximizar a cooperação entre os próprios detentores de dados no sentido de serem transparentes quando à informação de detêm para aumentarem a criação de valor a mesma, passando de um modelo de negócio que tem os detentores de dados como figura central, para um modelo focado no controlo dos dados pessoais pelos seus titulares, que passariam a participar no mercado de monetização dos seus dados pessoais, gerindo e acompanhando os fluxos da sua informação pessoal. Cfr. ainda com os considerandos 27 e 28 do Regulamento de Governação de Dados.

vista do cumprimento das condições de licitude do tratamento, e, até, com maior segurança quanto à qualidade e precisão dos dados usados, que os beneficiaria.

A adoção de um modelo centralizado no titular dos dados pessoais possibilitaria, aos seus titulares, não só o tratamento dos seus dados nos seus termos e nas suas condições, como assim também o fariam no que diz respeito a uma participação ativa no mercado jurídico, atribuindo, diretamente e em função das suas preferências, direitos de utilização sobre os seus dados pessoais. Dando enfoque à perspetiva do interesse público, este modelo poderia, nos termos daquele relatório, ser complementado com um movimento *open data* (de dados abertos) capaz de potenciar as necessidades de desenvolvimento da sociedade e em prol do bem comum – revogando a Diretiva 2003/98/CE, a Diretiva relativa aos dados abertos[41] integrou a estratégia europeia de dados[42], sem prejuízo dos eventuais riscos acima abordados e que ora não ocupam maiores desenvolvimentos.

Como veremos, foi este o modelo largamente adotado pelo legislador europeu no Regulamento de Governação de Dados proposto em 2020.

3.2. Evidenciação do modelo de governação adotado

Neste Regulamento Governação de Dados, o legislador não deixou de considerar a proposta, da Comissão Europeia, de criação de "espaços comuns europeus de dados específicos (…), que constituirão o quadro concreto de partilha e mutualização de dados (…)"[43]. Precisamente, por

[41] Diretiva (UE) 2019/1024 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativa aos dados abertos e à reutilização de informações do setor público. OJ L 172, 26.6.2019, p. 56–83.

[42] "Dados abertos", nos termos descritos do considerando (16) desta Diretiva, são os "(…) dados em formato aberto que idealmente podem ser utilizados, reutilizados e partilhados de forma livre por qualquer pessoa e para qualquer finalidade (…)", não obstando a mesma à reutilização de dados pessoais, sem prejuízo da proteção conferida aos titulares dos dados nos termos do RGPD, e em conformidade com o princípio "tão aberto quanto possível, tão fechado quanto necessário" (v. o Considerando (28) da Diretiva relativa aos dados abertos).

[43] Cfr. Considerando (2) do Regulamento Governação de Dados.

oposição aos silos que caracterizam o ecossistema de dados atual e que mencionamos na subsecção anterior. E é assim que introduzimos alguns dos aspetos integrados no Regulamento de Governação de Dados que nos levam a crer que, neste normativo europeu, existe uma aproximação à ideia de experimentação suprarreferida, de um modelo de mercado de dados a que intitulamos "versão 1.0". Já que, de facto, este será o primeiro modelo de governação que visa regulamentar o mercado de dados *de facto* que conhecemos. Onde os grandes tecnológicos vingam através do aproveitamento das suas capacidades de criar valor através da informação a que têm acesso. Especialmente, nesta era de *Big Data*[44], em que a disponibilidade para a Comparem-se as seguintes figuras:

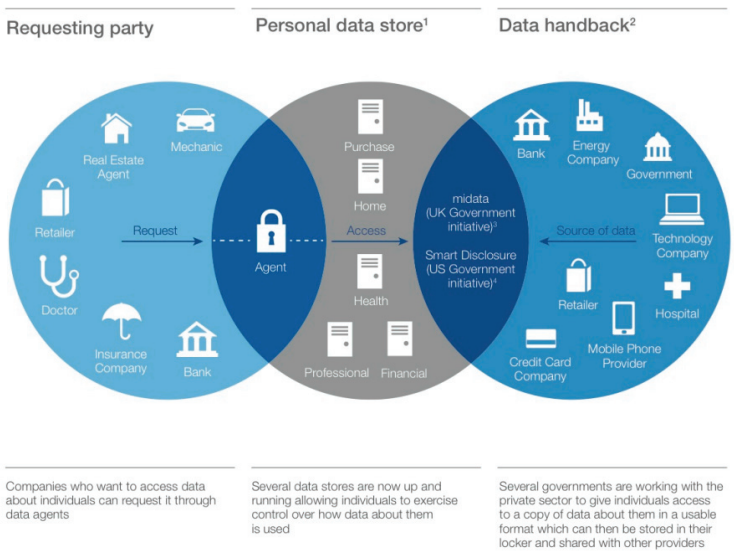

Figura 1 Retirada do relatório da Cambridge Judge Business School "Personal Data Stores", p. 3

[44] Sobre o conceito Big Data & Analytics v. CAVANILLAS, José María; CURRY, Edward; WAHLSTER, Wolfgang – New horizons for a data-driven economy: a roadmap for usage and exploitation of Big Data in Europe [Em linha]. Springer Open, 2016. [Consult. 14-01-2019]. p. 31ss.

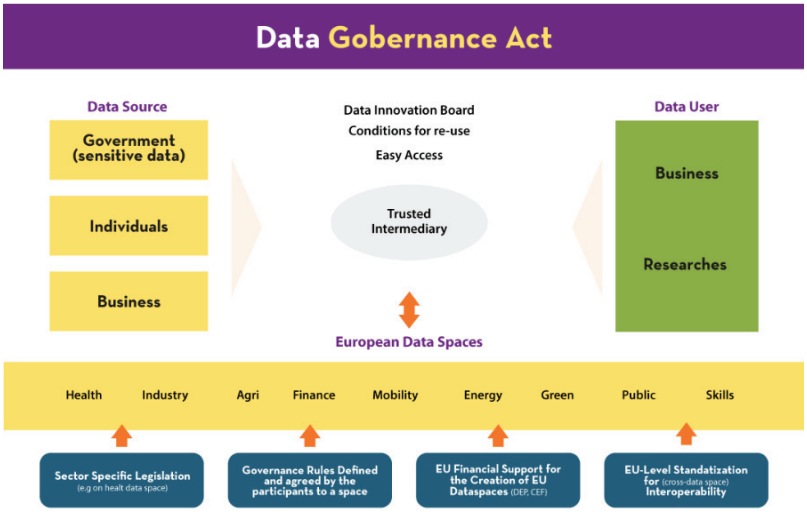

Figura 2 Diagrama criado a partir da Proposta de Regulamento de Governação de Dados, retirada da página na Internet "datos.gob.es" e que se mantém atual no correspondente Regulamento aprovado[45]

Agora, faça-se o exercício de cruzar as figuras de "detentor de dados", "utilizador de dados", "titular de dados" e "serviço de intermediação de dados", introduzidas nas definições do art. 2.º do Regulamento de Governação de Dados. Não é possível desenvolver o desenho e a construção de um tal mercado regulado 1.0? Vejamos:

- Em ambas as figuras temos um elemento central – na Figura 1, este elemento é o "agent"/"data agents"[46], que é quem gere a "personal data store"; e, na Figura 2, o "trusted intermediary"[47].

[45] Disponível na Página da Internet do Secretariado do Estado Espanhol para a Digitalização e Inteligência Artificial do Ministério da Economia e Transformação Digital [Consult. 20-11--2022]. Disponível em WWW: <https://datos.gob.es/en/blog/impact-assessment-proposal-european-data-governance-regulation>.

[46] Na Figura 1 Retirada do relatório da Cambridge Judge Business School "Personal Data Stores", p. 3.

[47] Na Figura 2 Diagrama criado a partir da Proposta de Regulamento de Governação de Dados, retirada da página na Internet "datos.gob.es" e que se mantém atual no correspondente Regulamento aprovado.

No Regulamento de Governação de Dados, surge o prestador de serviços de intermediação de dados, que irá funcionar como uma entidade reconhecida e regulada, servindo de agente de confiança na intermediação de relações comerciais que têm como objeto a partilha de dados que pode ocorrer entre titulares ou detentores de dados, e os utilizadores de dados.

- No contexto do serviço de intermediação de dados nos termos do Regulamento de Governação de Dados, a nova figura do "utilizador de dados" passa a titular um direito de tratar os dados que lhe são disponibilizados pela via da intermediação. "Requesting party" e "data user" na figura 1 e na figura 2 acima – respetivamente.
- Os titulares de dados (acrescente-se, pessoais, na aceção do RGPD), que podem fornecer os dados de que são titulares, no âmbito do serviço de intermediação, a utilizadores de dados.[48]
- Quanto à figura do "detentor de dados", acaba por ser igualmente considerada uma fonte dos dados, que, não sendo titular de dados pessoais, tem um direito de comunicar os mesmos, seja através de concessão de acesso aos mesmos, seja através da sua partilha, a utilizadores de dados.

Assim se introduz a tríade representada nas figuras acima – i.e., "quem disponibiliza os dados", o "utilizador" e a "fonte de dados": a fonte de dados objeto do serviço de intermediação de dados, que se pode traduzir na possibilidade de ser o titular dos dados ou um detentor a disponibilizar os dados pessoais, a um utilizador desses dados.

Nesta senda, continuamos em crer[49] que, a este respeito, Kenneth Laudon, em 1996, mostrou-se visionário, com a sua ideia de criação de

[48] Em ambas as figuras, Figura 1 Retirada do relatório da Cambridge Judge Business School "Personal Data Stores", p. 3 e Figura 2, aparecem assumidamente como a fonte dos dados ("source of data"/"data source – respetivamente, e em tradução livre).

[49] PEREIRA CARNEIRO, Patrícia Filipa (2019) – cit.

um Mercado Nacional de Informação ("*National Information Market*" ou "NIM")[50]. Com a referência ao "NIM", Laudon visionava que um modelo de governação de dados pessoais que, entre outros possíveis agentes, contasse com os elementos daquela tríade-chave que mencionamos, permitiria aos titulares dos dados gerir a sua informação de forma mais eficiente dentro do quadro dos seus direitos, e, consequentemente, permitindo maior tutela da sua privacidade. Isto, partindo ainda da premissa de que a privacidade do indivíduo seria salvaguardada se lhe atribuíssemos direitos de propriedade sobre a sua informação pessoal. Aqui chegados, e em clarificação do n.º 2 do art. 17.º do RGPD[51], somamos-lhe a natureza inesgotável dos dados pessoais preconizada pelo Regulamento de Governação de Dados[52], portanto, passíveis de serem reproduzidos sem afetar o seu caráter de bens jurídicos que derivam da personalidade do indivíduo, ultrapassando, paralelamente, a ideia, de que tais bens estão indisponíveis para circular no comércio[53].

[50] LAUDON, Kenneth C. – cit., pp. 93 e 99ss.

[51] "Quando o responsável pelo tratamento tiver tornado públicos os dados pessoais e for obrigado a apagá-los nos termos do n.º 1, toma as medidas que forem razoáveis, incluindo de caráter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos."

[52] Desde logo, no âmbito da reutilização de dados.

[53] V. p.e., JANEČEK, Václav – Ownership of personal data in the Internet of Things. Computer Law & Security Review [Em linha], pp. 1039-1052, pp. 5ss. Disponível em WWW: <https://ssrn.com/abstract=3111047>. Cfr., p.e., com os considerandos (30) e (31) do Regulamento de Governação de Dados, onde se poderá questionar, inclusive, a existência de um direito à utilização de dados pessoais para fins comerciais não obstante o irrenunciável direito de personalidade à proteção de dados pessoais, a partir da consideração de uma vertente patrimonial daquele direito.

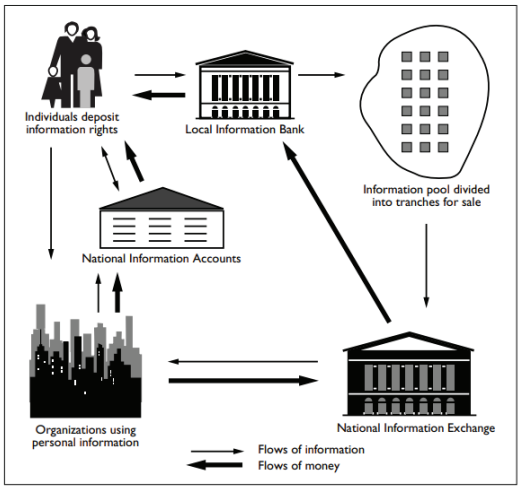

Figura 3 "How a National Information Market Would Work", do artigo ora referenciado "Markets and Privacy"

Para nós, esta é a principal inovação e reinvenção no/do pensamento jurídico, em que o legislador europeu, ainda que, como temos vindo a apontar, com alguns aspetos menos virtuosos para o direito fundamental à proteção de dados, procurou ultrapassar a ideia de que os dados pessoais são considerados meras "mercadorias de troca"[54] no âmbito de um mercado de dados. Diríamos, assim, que o legislador assume que a participação, do titular de dados pessoais, no comércio jurídico, não significa uma transmissão de um direito inalienável[55], pelo contrário, cremos que se trata de maximizar o potencial de um direito

[54] Cfr. com a posição da EDPS em "Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content". [Em linha]. (14-03-2017) [Consult. 13-03-2022]), a posição do reiterada pelo Comité Europeu da Proteção de Dados relativamente ao Regulamento Governação de Dados em "Statement 05/2021 on the Data Governance Act in light of the legislative developments". [Em linha]. (19-05-2021). [Consult. 19-03-2023]; e, mais tarde, em semelhantes moldes, por este Comité e a EDPS na sua opinião conjunta "DPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)" on the Data Act proposal". [Em linha]. (04-05-2022). [Consult. 19-03-2023].

[55] Cfr. Considerando (31): "(…) são direitos pessoais do titular dos dados aos quais este não pode renunciar."

de personalidade. Por exemplo, como acontece com a exploração económica da imagem nos termos do Código Civil[56] [57].

Usamos o exemplo da exploração económica da imagem porque, de uma forma geral, no contexto da compatibilização entre aquele Regulamento de Governação de Dados e o RGPD, está a necessidade de cumprir os requisitos do RGPD[58] – como é o caso da necessidade de assegurar uma base jurídica para a comunicação de dados pessoais[59]. Já de uma forma particular, o Regulamento de Governação de dados[60] tende em assumir que o consentimento é o fundamento de licitude adequado nos termos da al. a) do n.º 1 do art. 6.º do RGPD[61] [62].

Assim[63], recorrendo a um caso de estudo, propomo-nos a averiguar, de entre os vários desafios legais, o subjacente ao fundamento de licitude para a partilha de dados pessoais para efeitos da sua valorização e monetização através de serviços de intermediação de dados pessoais no âmbito do Regulamento de Governação de Dados, em cumprimento do RGPD.

---

[56] P. CARNEIRO, Patrícia – cit., pp. 124*ss*.

[57] Adicionalmente, poderemos considerar que a partilha de dados pessoais no âmbito do Regulamento de Governação de Dados, nem será uma limitação voluntária ao exercício dos seus direitos por via do consentimento, tal como decorre do art.º 81.º do Código Civil e continuando o exemplo da exploração da imagem acima iniciado, quando o próprio legislador admite, como vimos, essa partilha como sendo uma necessidade supra individual – uma necessidade da comunidade europeia.

[58] Vejam-se os considerandos (6) e (35) do Regulamento de Governação de Dados.

[59] V., p.e., o considerando (15) do Regulamento de Governação de Dados.

[60] Na sequência da ideia de "reforçar a capacidade de ação dos titulares, nomeadamente, o controlo que as pessoas exercem sobre os dados que lhe dizem respeito". Cfr. considerando (30) do Regulamento de Governação de Dados.

[61] "O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações: a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas (...)".

[62] Cfr., p.e., 2.º par. do considerando (15) e considerando (5); 2.º par. do considerando (26) e considerando (52) – não obstante o exposto no considerando (7) *in fine*: "[e]m geral, no que diz respeito a dados pessoais, o tratamento deve basear-se num ou mais dos fundamentos jurídicos para o tratamento previstos nos artigos 6.º e 9.º do Regulamento (UE) 2016/679."

[63] E tendo presente que a criação de um modelo de mercado de dados pessoais acarreta vários riscos e desafios em diferentes planos do governo de uma sociedade nos termos suprarreferidos.

4. Licitude da partilha de dados (pessoais) através de serviços de intermediação de dados no âmbito do Regulamento de Governação de Dados – caso de estudo

No seguimento do ponto anterior, é aquela tríade – fonte dos dados, prestador de serviços de intermediação de dados e utilizador de dados –, que será alvo do nosso caso de estudo, o qual assume o modelo de partilha de dados que se passará a representar. Cenário:

- Uma organização (utilizador de dados na aceção do Regulamento de Governação de Dados), pretende adquirir informação pessoal que possibilite a identificação de padrões e tendências comportamentais de determinado público-alvo que o permita caracterizar determinada tipologia de clientes seus, titulares dos dados pessoais.
- Para que esta transferência seja possível, um prestador de serviços de intermediação, disponibiliza as ferramentas necessárias à partilha de dados, nomeadamente uma plataforma em linha com uma base de dados alimentada por detentores e utilizadores de dados, na qual cabe ao utilizador de dados identificar as suas necessidades de utilização de dados.

Introduzimos este cenário, na medida em que representa os interesses comerciais dos grandes operadores do mercado *de facto* tal como temos vindo a descrever e como é exemplo o caso da Meta (outrora Facebook). Como vimos, a sua fonte primordial de rendimento é a venda de espaço publicitário direcionado aos interesses dos seus utilizadores. Por outro lado, este cenário tem como objeto a comunicação de informação num modelo de negócio válido no âmbito do Regulamento de Governação de Dados.

Neste caso de estudo, iremos aprofundar em que termos o consentimento enquanto fundamento legal é válido e/ou é o mais adequado, nos termos do RGPD, para o tratamento de dados pessoais no âmbito

do cenário em apreço, considerando, como vimos, que o Regulamento de Governação de Dados parece indiciar uma discriminação positiva do consentimento em detrimento dos demais fundamento legais previstos nos art. 6.º e 9.º do RGPD. Sendo que, para o efeito, precisaremos analisar a responsabilidade de cada um dos intervenientes na relação de tratamento de dados como a do cenário a utilizar no caso de estudo.

4.1. Pressuposto à verificação das condições de licitude

As condições de licitude deverão ser aferidas em função do respetivo tratamento de dados pessoais, pelo responsável pelo tratamento. Razão pela qual se entende que a identificação do responsável pelo tratamento de dados pessoais no âmbito do Mercado 1.0, deve ser um pressuposto deste caso de estudo.

Para melhor enquadramento, atentemos no art. 6.º do RGPD, que regula a licitude do tratamento e, a título não taxativo, nas seguintes disposições:

- O parágrafo 2, do n.º 3, do art. 6.º do RGPD, relativo à definição de fundamento jurídico específico para os tratamentos do seu n.º 1, alíneas c) e e), integra a seguinte expressão: "(…) ao qual o responsável pelo tratamento está sujeito (…)" – sublinhado nosso. Daqui, decorre que a definição de tal fundamento vincula o responsável pelo tratamento, adiantando o mesmo preceito que o "(…) fundamento jurídico pode prever disposições específicas para adaptar a aplicação das regras do presente regulamento, nomeadamente: as condições gerais de licitude do tratamento pelo responsável pelo seu tratamento (…)" – sublinhado nosso.
- O considerando (50) do RGPD, a respeito das condições de licitude de tratamento de dados posteriores, refere: "para outros fins que não aqueles para os quais os dados pessoais tenham sido inicialmente recolhidos": "(…) o responsável pelo seu tratamento,

> após ter cumprido todos os requisitos para a licitude do tratamento inicial (…)" – sublinhado nosso.

Do exposto, compreendemos que, de entre os vários sujeitos passíveis de serem encontrados no quadro de uma relação de tratamento de dados pessoais, é o poder de determinação das finalidades e dos meios de tratamento de dados pessoais que permite a definição do responsável pelo tratamento de dados pessoais – como se viu, elementos essenciais à identificação do fundamento de licitude que melhor servirá esse mesmo tratamento. Nos termos da alínea 7) do art. 4.º do RGPD, é o responsável pelo tratamento "que, individualmente ou em conjunto com outras [aqui, um responsável conjunto ou corresponsável nos termos do art. 26.º do RGPD], determina as finalidades e os meios de tratamento de dados pessoais" – sublinhado nosso. Pelo que não se poderia dizer, por exemplo, que seria em função do tratamento de dados realizado pelo subcontratante por conta do responsável, na aceção da alínea 8) do art. 4.º do RGPD, que se averiguaria da licitude do tratamento dos dados pessoais[64].

4.2. Responsabilidade no tratamento de dados pessoais

Não resultando do Regulamento de Governação de Dados, cumpre-nos, portanto, identificar a responsabilidade de cada um dos intervenientes no tratamento de dados pessoais no âmbito do cenário que consubstancia o nosso caso de estudo.

Face às orientações do Comité Europeu da Proteção de Dados sobre os conceitos de responsável e subcontratante, parece não se verificar a condição de "indissociabilidade" entendida como necessária para que se considere que, entre o detentor de dados e o utilizador dos dados

[64] Por outro lado, já se poderia considerar que um o "destinatário" de dados pessoais (na aceção da alínea 9) do art. 4.º do RGPD), poderá ser um responsável no tratamento dos dados pessoais que lhe são comunicados no quadro do mercado projetado, cabendo-lhe o cumprimento das respetivas obrigações jurídicas direcionadas às condições de licitude do tratamento de dados.

objeto de intermediação, exista uma relação de corresponsabilidade pelo tratamento de dados pessoais partilhados, desde logo, por tal tratamento não depender da participação nem de um detentor nem de um utilizador de dados específicos:

(i) o detentor de dados é responsável por garantir que os dados disponibilizados não extravasam os direitos de conceder acesso ou de partilhar dados (quanto ao que nos ocupa, pessoais), portanto;
(ii) o detentor de dados é responsável pela informação realmente disponibilizada ao utilizador da plataforma de intermediação que pretenda aceder ao "produto" e;
(iii) o detentor de dados é responsável por criar uma apresentação da informação que tem para comunicar e a ser transmitida através da plataforma do prestador de serviços de intermediação de dados, nomeadamente, se forem registos relativos a um variado número de categorias de titulares de dados pessoais, as respetivas categorias de titulares de dados cuja informação será objeto da comunicação.

Por outro lado, embora o utilizador de dados seja parte na relação estabelecida com o detentor de dados através da plataforma do intermediário de dados, a finalidade subjacente ao tratamento que pretende fazer dos dados pessoais adquiridos será diferente do propósito que levou o detentor a efetuar a comunicação dos dados em questão que, entendemos, ser a de valorização e monetização da informação. A este respeito, a jurisprudência do Tribunal de Justiça da União Europeia[65], adotando uma conceptualização ampla, admite que, ainda que as entidades não partilhem da mesma finalidade do tratamento em todas as fases do tratamento, existirá corresponsabilidade se os propósitos das partes em determinadas operações de tratamento dos dados em questão

[65] Caso C-40/17 do Tribunal de Justiça da União Europeia (Caso "Fashion ID").

se complementarem ou estiverem intrinsecamente ligados. Por exemplo, através da existência de um benefício comum ou de operações de tratamento de dados subsequentes que reflitam, no quadro global da atividade de tratamento de dados, a participação conjunta das partes na definição da finalidade e dos meios.

No caso de estudo sob análise, o detentor de dados pode ser considerado responsável pelo tratamento no início do ciclo da informação comunicada (desde a recolha dos dados pessoais junto dos seus titulares), e até ao momento prévio à comunicação da mesma através de um intermediário de dados. O que implica, desde logo, que o mesmo responde a condições de licitude próprias no tratamento de dados pessoais que realizar nesse contexto. Relativamente à operação de comunicação dos dados para o seu utilizador, poderá ser considerada realizada em conjunto pelo detentor e o intermediário de dados, respondendo o utilizador enquanto responsável apenas pelo tratamento de dados que realizar desde que teve acesso aos mesmos naquele contexto, para fins próprios. Esta solução parece não coadunar, no entanto, com o exemplo da compra de bases de dados apresentado pela Comissão Europeia no seu sítio *web*[66]. Neste caso, a Comissão Europeia aparenta deixar na responsabilidade de quem vende a base de dados a demonstração de que os mesmos foram recolhidos licitamente[67], cenário em que o utilizador de dados seria um verdadeiro terceiro na aceção da alínea 10) do art. 4.º do RGPD, e destinatário de dados. A este respeito, diz-nos ainda o Comité Europeu da Proteção de Dados nos elementos supracitados, que importa salientar que a mera existência de um benefício económico mútuo (p.e., comercial) não basta para que, por si só, reflita um cenário de corresponsabilidade.

---

[66] Disponível na Página da Internet da Comissão Europeia. [Consult. 27-11-2022]. Disponível em WWW: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/can-data-received-third-party-be-used-marketing_pt>.

[67] Onde se lê: "essa outra organização tem de demonstrar que os dados foram obtidos em conformidade com o Regulamento Geral sobre a Proteção de Dados e que a sua organização os pode utilizar para fins publicitários".

Pelo exposto supra, cremos que o facto de o detentor e o utilizador recorrerem a um canal comum de transferência dos dados objeto da relação comercial entre si estabelecida (por exemplo, via de um serviço de intermediação de dados), não justifica que se considere a responsabilidade conjunta das partes, uma vez que a definição da finalidade de valorização e monetização dos dados do detentor de dados pessoais[68] – assim se compreendendo a mesma –, é independente da vontade do utilizador e dela dissociável.

Em suma, no âmbito do presente caso de estudo, entendemos o detentor e o utilizador de dados pessoais responsáveis, de forma independente, pelo tratamento de dados pessoais objeto da intermediação que se venha a concretizar.

Já a relação estabelecida entre o detentor e o utilizador de dados, e o prestador de serviços de intermediação de dados que disponibiliza e gere a plataforma em linha, apresenta contornos diferentes e, para que este prestador de serviços não seja considerado corresponsável pelo tratamento ou destinatário de dados pessoais, deve o mesmo garantir que não contribui para o tratamento de dados pessoais acima descritos, através da definição de meios e finalidades, influenciando o "se" e "como" o tratamento deveria ocorrer:

- Poderá ser enquadrado como subcontratante na aceção do RGPD caso se considere que não prossegue qualquer finalidade própria no tratamento, tratando os dados pessoais em nome daquelas partes, limitando-se ao fornecimento de meios; e,
- Consequentemente, será considerado responsável pelo tratamento na persecução de uma finalidade própria, nomeadamente, de intermediação de dados, com todos as suas minucias, como a

[68] O titular de dados pessoais está naturalmente dotado de poderes de disposição da sua informação pessoal, daí que o "dever fiduciário" do prestador de serviços de intermediação de dados previsto no considerando (33) do Regulamento de Governação de Dados e depois desenvolvido, por exemplo, no art. 12.º, seja de maior pertinência.

segurança da plataforma e da confidencialidade e integridade base de informação sob a sua alçada[69]; ou,

- Poderá ser visto como corresponsável, com cada um dos intervenientes em questão (detentor e utilizador de dados), se apresentar uma vontade convergente com cada um daqueles intervenientes, nomeadamente, com o mesmo propósito do detentor de dados, identificado como "valorização e monetização de dados".

Concluímos, assim, que, para efeitos do presente artigo, o prestador de serviços de intermediação poderá ser considerado responsável pelo tratamento de dados que realiza no contexto de intermediação de dados e, eventualmente, subcontratante do detentor e utilizador de dados, dependendo da sua participação modelo de intermediação, nomeadamente, do ponto de vista das ferramentas acessórias disponibilizadas para o efeito. Sem mais, não será considerado corresponsável pelo tratamento de dados pessoais, surgindo como um mero "facilitador do negócio" através do fornecimento das ferramentas necessárias ao processo. Pelo que o detentor e o utilizador de dados serão os responsáveis por garantir a licitude do tratamento de dados no âmbito do Mercado 1.0.

4.3. Consentimento do titular dos dados – uma imposição de base legal?

Aqui chegados, resta-nos indagar sobre o fundamento jurídico subjacente à partilha de dados no âmbito de um serviço de intermediação de dados. No RGPD, encontramos no art. 6.º e, em particular, no seu n.º 1, os fundamentos de licitude aplicáveis ao tratamento de dados pessoais que não consubstanciem categorias especiais de dados pessoais nos termos e para os efeitos do art. 9.º do mesmo Regulamento, ou seja,

[69] Cfr. PAR/2022/99 da Comissão Nacional de Proteção de Dados.

aqueles dados pessoais que, pela sua natureza, se considerem especialmente sensíveis. Para estas categorias especiais de dados, vale uma proibição genérica de tratamento de dados (cf. n.º 1 do art. 9.º do RGPD), devendo o responsável pelo tratamento procurar autorização para o tratamento de tais categorias especiais de dados pessoais nas derrogações explícitas à proibição geral de tratamento previstas no n.º 2 do art. 9.º do RGPD, ou nos normativos nacionais, que poderão estabelecer disposições de proteção de dados específicas, "para dar cumprimento a uma obrigação legal, para o exercício de funções de interesse público ou para o exercício da autoridade pública de que está investido o responsável pelo tratamento"[70] (veja-se o n.º 3 do art. 9.º do RGPD).

No que a este ensaio diz respeito, focar-nos-emos, como vimos, no consentimento do titular dos dados enquanto base de licitude –alínea a) do n.º 1 do art. 6.º do RGPD)[71]. Perante os vários os momentos em que o Regulamento de Governação de Dados refere o consentimento como base legal para o efeito, questionamo-nos sobre uma eventual imposição legal de obtenção do consentimento do titular para o tratamento dos seus dados naquele contexto e, em particular, no do cenário proposto no ponto 3.1 deste trabalho. Por exemplo, no considerando (50) daquele Regulamento, prevê que "[r]egra geral, o altruísmo de dados deverá basear-se no consentimento dos titulares dos dados (…)" – sublinhado nosso; já no art. 25.º do Regulamento de Governação de Dados, o legislador refere a necessidade de utilização de um formulário de consentimento. Por sua vez, e porque não é do nosso interesse imediato pronunciarmo-nos sobre o regime da reutilização de dados para fins de altruísmo, trazemos à colação a alínea m) do art. 12.º do Regulamento de Governação de Dados, onde o legislador assume a obrigatoriedade de o prestador de serviços de intermediação de dados obter o consentimento do titular para o tratamento de dados

[70] Cfr. com o considerando (51) do RGPD.

[71] "(…) O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações: a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas (…)" – sublinhado nosso.

pelos utilizadores dos dados[72]. Desta forma, não existindo qualquer ordem ou primazia de base jurídica no RGPD, deverá considerar-se que estamos perante um conflito de leis tal como prevenido no considerando (4) do Regulamento de Governação de Dados[73], ou devemos desconsiderar, por completo, qualquer outro fundamento jurídico, assim como a necessidade de ser o utilizador de dados – como vimos, responsável pelo tratamento –, a assegurar as condições de licitude do tratamento?

Nos termos da alínea b) do n.º 1 do art. 6.º do RGPD, o tratamento de dados pessoais será igualmente lícito se *"*(…) for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados". E, aqui, o contrato pode, até, ser tripartido, entre os elementos da tríade (fonte dos dados, prestador de serviços de intermediação de dados e utilizador de dados). Assim, para analisarmos, por exemplo, se cada um dos vendedores nos cenários acima descritos poderão fundamentar o tratamento dos dados pessoais no âmbito do mercado projetado num contrato, dever-se-á aferir se aqueles dados pessoais são necessários para a celebração e execução do mesmo. Quanto a esta necessidade, tem-se entendido que deve ser interpretada restritivamente, no sentido de que se verificará uma necessidade de tratamento de dados pessoais para a execução de um contrato se existir uma relação direta e objetiva entre o tratamento de dados pessoais em questão e o propósito da execução do contrato[74]. Ou seja, na medida em que não seja possível a realização ou o cumprimento do contrato entre as partes sem que os dados pessoais do respetivo titular sejam tratados. Sendo que, *ab initio*,

[72] Curioso é também atentar no relatório da avaliação de impacto ao Regulamento de Governação de Dados – cit. versus uma das principais preocupações do legislador, voltada para a falta de confiança do titular de dados pessoais para a partilha dos seus dados. Naquele relatório, o consentimento é amplamente explorado enquanto meio de obter esta confiança, recorrendo a esquemas estrangeiros, como é o caso japonês plasmado no seu anexo 6, para fundamentar essa crida mais-valia.

[73] Como referimos na secção 3, em caso de conflito, deverá aplicar-se o RGPD.

[74] V. "Guidelines 05/2020 on consent under Regulation 2016/679" emitidas pelo European Data Protection Board, versão 1.1, de 4-05-2020, ponto 30, p. 10.

conseguimos identificar o âmbito de tal contrato: a partilha de dados, "(…) com base em acordos voluntários ou no direito da União ou nacional (…)"[75]; e, não é novidade que, no sistema jurídico português, os bens da personalidade circulem no comércio em benefício do próprio titular ou de terceiros, designadamente, no contexto dos contratos de cedência de exploração de imagem de desportistas[7677].

Isto posto, ressalvamos que do n.º 3 do art. 7.º do RGPD, resulta que "ao avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato". Ou seja, verificando-se o caso, a licitude tratamento de dados pessoais estaria antes sob a alçada da alínea b) do n.º 1 do art. 6.º do RGPD, e não da alínea a) daquele mesmo preceito, que seria considerada desadequada para o efeito. Isto implica que qualquer pressão[78] ou influência exercida pelos demais intervenientes no tratamento, sobre o titular, na escolha pela monetização dos seus dados pessoais[79], não é permitida sob pena de o consentimento obtido do

[75] Art. 2.º, 10) do Regulamento de Governação de Dados.

[76] Assim como não é novidade que, os dados pessoais, são suscetíveis de ser objeto de "troca" enquanto contrapartida de um serviço, no quadro dos contratos de consumo de conteúdos e serviços digitais, sendo discutível se não serão verdadeiras contraprestações, do ponto de vista obrigacional da relação negocial estabelecida.

[77] A este respeito é, no entanto, interessante, lermos a posição da Autoridade de Controlo Irlandesa (Comissão Irlandesa de Proteção de Dados) tal como escortinada pela NOYB a respeito de a Facebook (agora Meta) utilizar o contrato enquanto fundamento de licitude no contexto que nos levou a criar o cenário do caso de estudo, em linha [Consult. 19-03-2023]. Segundo o entendimento daquela Autoridade de Controlo, o serviço de publicidade direcionada em função do comportamento do utilizador não é necessário à abertura da conta na rede social e usufruição da mesma. Disponível em WWW: <https://noyb.eu/en/breaking-meta-prohibited-use-personal-data-advertising>.

[78] Por exemplo, condicionar o fornecimento de um serviço, um serviço de qualidade superior, ou determinada funcionalidade, à autorização do titular direcionada à monetização dos seus dados pessoais, quando o fornecimento dos mesmos é independente do fornecimento do serviço.

[79] Por exemplo, caso em que o prestador de serviços de intermediação de dados atribuísse um benefício ao titular, como um bónus por cada registo de dados pessoais a partilhar, se o mesmo consentisse em tal valorização e monetização.

titular ser considerado inválido[80]. O mesmo se diga, a respeito das "permissões-imposições legais" que aprecem resultar do Regulamento de Governação de Dados, para o tratamento de dados pessoais no contexto da reutilização[81] [82]. Em última linha, a utilização do consentimento por defeito em detrimento de outros fundamentos de licitude pode criar um efeito adverso face ao mercado de dados projetado pela U.E. Pense-se, por exemplo, no impacto financeiro da abordagem do Regulamento de Governação de Dados na atribuição de controlo, ao titular, sobre os seus dados pessoais, em especial, para efeitos da sua participação no mercado de dados e extração de valor dos seus dados pessoais. Considerar-se-á o n.º 4 do art. 6.º do RGPD justificação suficiente para a reutilização dos dados pessoais do seu titular, como opção aparentemente introduzida no considerando (15) do Regulamento de Governação de Dados?

5. Conclusão

Dúvidas não nos restam quanto à paulatina criação estruturada de um mercado interno (europeu) digital que não exclua[83] a "partilha e a mutualização"[84] de dados pessoais, em prol de uma economia digital

[80] Seria curioso também conceber o caso em que o utilizador dos dados fosse uma entidade pública, cenário em que a validade do consentimento seria contestável, pois que uma entidade pública, face ao desequilíbrio de poderes entre as partes, dificilmente poderia contar com o consentimento do titular.

[81] Cfr. como a considerando (15) in fine.

[82] Perguntamo-nos se esta imposição visa o preenchimento dos critérios do n.º 3 do art. 6.º do RGPD.

[83] Cfr. Considerando (6) do Regulamento de Governação de Dados: "(…) No entanto, determinadas categorias de dados, como os dados comerciais confidenciais, os dados que estão sujeitos a confidencialidade estatística e os dados protegidos por direitos de propriedade intelectual de terceiros, incluindo segredos comerciais e dados pessoais, que se encontram em bases de dados públicas, muitas vezes não são disponibilizados, nem sequer para atividades de investigação ou de inovação de interesse público, apesar dessa disponibilidade ser possível nos termos do direito da União aplicável, em particular do Regulamento (UE) 2016/679 e das Diretivas 2002/58/CE e (UE) 2016/680 (…)" – sublinhado nosso.

[84] Considerando (2) do Regulamento de Governação de Dados.

europeia, cuja base é a criação de uma cadeia de valor associada aos dados em geral.

É este o contexto do Regulamento de Governação de Dados, que surge da análise da aplicação de sistemas que visam a adoção de modelo centralizado no titular dos dados pessoais para sua participação ativa no mercado de dados, como é o caso das "Personal Data Stores". Entre os aspetos principais destes modelos, está a alteração de paradigma relativamente ao modo como os dados das pessoas circulam no comércio jurídico, transportando-os dos "silos" de informação que caracterizam os grandes operadores económicos, para um modelo em que o titular passaria a ser o centro de toda a gestão da sua informação e respetivo ecossistema.

Várias questões estão ainda por tratar a este respeito, e a definição das condições de licitude para a intermediação e partilha de dados no âmbito de um Mercado de dados 1.0 é apenas uma delas, e, sempre dependerá, pelo menos, de 2 (dois) pontos: i) da concretização contextual dos cenários de "valorização e monetização de dados pessoais" – finalidade para o tratamento de dados pessoais no caso de estudo em análise e que, é também uma possibilidade de entre várias; ii) da identificação da responsabilidade dos intervenientes no tratamento de dados. Só assim conseguiremos identificar qual dos fundamentos previstos no art. 6.º do RGPD, e das autorizações para o tratamento de categorias especiais de dados listadas no art. 9.º do RGPD, poderia comportar menor risco para os titulares de dados pessoais no mercado de dados projetado[85].

Entendemos a ideia principal do legislador quando, no Regulamento de Governação de Dados, parece impor a utilização do consentimento do titular enquanto fundamento legal, que é a de assegurar que o titular dos dados pessoais tem o controlo efetivo sobre a escolha direcionada ao tratamento dos seus dados pessoais[86].

[85] Riscos legais/sancionatórios, financeiros, e até de imagem/reputação do responsável pelo tratamento de dados tal como descrito mencionados acima.

[86] V. "Guidelines 05/2020 on consent under Regulation 2016/679" – cit., ponto 3, p. 5.

Em todo o caso, este não é o único fundamento jurídico previsto no RGPD e, como tivemos oportunidade de referir, não existe uma ordem para a sua seleção. Ademais, é perigosa a falta de clareza introduzida pelo Regulamento de Governação de Dados, quanto à sua articulação com o RGPD. Embora, ali, o legislador faça essencialmente sobressair a necessidade de recolha do consentimento, estipulando, até, um modelo de formulário de recolha de consentimento[87]; continua a fazer alusão, pontualmente e em paralelo, a outros conceitos que criam alguma margem de dúvida a respeito do fundamento de licitude preconizado. Por exemplo, quando se refere a negociação dos termos e condições do tratamento de dados[88]; ou, à possibilidade de os dados recolhidos serem reutilizados sem tal consentimento[89].

Daí termos introduzido a celebração de um contrato ou a relação pré contratual enquanto fundamento jurídico viável para o tratamento de dados sob análise. Acima de tudo, enquanto fundamento a invocar pelo utilizador de dados, especialmente, se este conseguir demonstrar que: a) o mesmo foi celebrado com o titular dos dados pessoais tratados, embora por via da intermediação; b) o contrato é válido nos termos da legislação aplicável; e, c) os dados pessoais tratados são objetivamente necessários à execução do contrato – portanto, essa necessidade não decorrerá meramente de uma condição contratual aposta no contrato[90].

Concluímos, portanto, que o Regulamento de Governação de Dados cria uma situação de desconforto no que diz respeito à sua

---

[87] Art. 25.º do Regulamento de Governação de Dados.

[88] Al. 15) do art. 2.º do Regulamento de Governação de Dados.

[89] Considerando (15) in fine.

[90] Neste sentido, v. o parecer do "Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do art. 7.º da Diretiva 95/46/CE" adotado pelo Grupo de Trabalho do Artigo 29.º para a proteção de dados em 9 de abril de 2014 (WP217): "A disposição deve ser interpretada de forma estrita e não abrange as situações nas quais o tratamento não seja verdadeiramente necessário para a execução de um contrato, mas sim imposto unilateralmente à pessoa em causa pelo responsável pelo tratamento." Acrescentando: "A disposição deve ser interpretada de forma estrita e não abrange as situações nas quais o tratamento não seja verdadeiramente necessário para a execução de um contrato, mas sim imposto unilateralmente à pessoa em causa pelo responsável pelo tratamento" – cf. p. 26.

articulação com o RGPD, sendo necessária reformulação no seu texto, sob pena de cairmos em interpretações diversas e prejudiciais do ponto de vista da proteção de dados pessoais, nomeadamente, potenciando tratamentos diferenciados dos titulares dos dados pessoais enquanto "fontes de dados" no Mercado de dados 1.0.

Não é claro se o legislador, no Regulamento de Governação de Dados, pretendia estipular o consentimento como fundamento de licitude para o tratamento de dados pessoais no contexto do modelo de governação que institui. E, ainda que tivesse sido, tal sempre teria de ser analisado do ponto de vista do princípio da licitude estipulado na al. a) do n.º 1 do art. 5.º do RGPD. Desde logo, a respeito da compatibilização daquela imposição legal com o preceituado nos n.ºs 3 e 4 do art. 6.º do RGPD.

Como vemos as coisas, o consentimento não é o único fundamento legal, nos termos do RGPD, passível de ser invocado neste contexto.

Por fim, não obstante o esforço de rever o texto do Regulamento de Governação de Dados em função das críticas que lhe foram tecidas no âmbito do seu processo legislativo, criticamos a leviandade com que o legislador desconsiderou o RGPD no Regulamento de Governação de Dados, o que era ainda mais evidente no texto da sua proposta.

Parece-nos, pois, evidente, a necessidade de maior desenvolvimento sobre o tema, começando pela fiscalização das estruturas de mercado entretanto criadas.

Consequences of Schrems II case: could the specific consent of art. 49 (1) of the GDPR be used as a regular legal basis for cross-border data transfers?

Amanda Costa Novaes[1]

Abstract: In this article, it is analyzed to what extent there is, after the Schrems II decision, the possibility of using the consent of art. 49(1) of the General Data Protection Regulation (GDPR) as a regular mechanism for international data transfer. Thus, the current understanding and requirements of the European legal system are examined for such scenario. Also, consent as a tool to limit fundamental rights is considered in order to determine if it should be used for cross-border data transfer. Hence, the assessment methodology will be focused on the European Legislation, selected relevant Court decisions and theoretical literature.

1. Introduction

The transfer of data between countries are a common phenomenon in the business model of an internet-based globalized world. Even though it is widely spread, some data flows are especially important due to the economic and politic forces of its agents, such as the ones between countries of the European Union and the United States of America. In this scenario, tensions arose from the American politics of national

[1] Master's student of Business Law and Technology at NOVA School of law, researcher at Whatnext.law.

security and the European fundamental right of data protection, culminating, on July of 2020, in the preliminary ruling by the Court of Justice of the European Union (CJEU) of a case known as Schrems II.[2]

After putting in check the most common legal basis for data exportation of the General Data Protection Regulation (GDPR) [3] between Europe and United States of America (USA), this decision left business without a secure legal ground to make this international transfer, especially online platforms from the United States, which tend to make this in on a daily basis. Although a new agreement for an adequacy decision between USA and the European Union is being currently developed, known as the new data privacy framework, many fear that the core incompatibilities of both political entities cannot be conciliated.

No wonder, in 2021, in a pool lead by the International Association of Privacy Professionals (IAPP-EY), 59% of privacy professionals said complying with cross-border data flows is their most difficult task.[4] The solution adopted by 25% of them was the use of consent as a data transfer mechanism.[5] However, the use of consent for cross-border data transfer is listed in art. 49 of GDPR as a "derogation for specific situations". Still, could such consent be used as a regular tool for data transfer to third countries, after the Court's Decision on the Schrems II Case?

Hence, the general objective of this paper is to conclude if, after the CJEU decision in the Schrems II case, the consent of art. 49(1)(a) of the GDPR can be used as a regular legal basis for international data transfers. The specific objectives are: (a) exam if the requirements of the law and jurisprudence for this specific consent allow it to be used as a regular mechanism; and (b) analyze the theory of consent as tool

[2] CJEU Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems 16 July 2020 EU:C:2020:559.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016) OJ L119/1.

[4] IAPP-EY, "Annual Privacy Governance Report 2021" (2021) 21 Available at https://iapp.org/resources/article/privacy-governance-report/ accessed 3 February 2023.

[5] Ibid 23.

to limit fundamental rights, in order to assess whether the same understanding should be adopted on the right of data protection in cross-border data flows.

For this, exploratory research was conducted. Moreover, the assessment methodology focused on: (a) the European legislation granting the fundamental right to data protection; (b) selected relevant Court decisions interpreting fundamental rights and its limitations; and (c) theoretical literature in the matter. In Section 2, the Schrems II Decision and its consequences will be briefly analyzed. Afterwards, in Section 3, there will be detailed the requirements of a valid consent in the General Data Protection Regulation, both the general consent for data processing (art.6) and the specific for international data transfer (art.49). Subsequently, in Section 4, a more theoretical approach of consent to limit fundamental rights will be adopted. In the end, it will be concluded to what extent consent could – or should – be used as a data transfer mechanism.

2. Consequences of the Schrems II Case (C-311/18 CJEU)

Until 16 of July 2020, the data transfers between United States of America and Europe mostly relied on art. 45 of the GDPR, specifically on the Privacy Shield agreement, which stated that the United States had the same level of data protection as the European Union. Yet, on the Schrems II decision, the CJEU declared that this agreement was invalid. This was, in summary, due to three main aspects: (a) the possibility of American Security Agencies, with non-judiciable activities, process bulk collections of personal data trough companies like Facebook; (b) the impossibility of EU citizens accessing effective legal remedies to ensure their data protection rights; and (c) the general primacy of national security over data protection that exists in the United States.[6]

[6] Data Protection Commissioner (n 1), paras 192-201.

With this decision, the most used legal basis for data transfer between EU and USA, grounded on art. 45 of the GDPR, was invalidated with *ex-tunc* effects. Consequently, companies were left in high risk of liability for past transfers based on this decision.[7] The risk is even higher, since the negotiations between States demonstrate a core incompatibility between the national security policies of the United States and the fundamental data protection right in Europe, so new adequacy decisions, as the new data privacy framework currently being developed, can also be invalidated in the future. Consequently, at any time huge costs can be created for companies due to unlawful transfers based on such invalid agreements.

Regarding art. 46 of the GDPR, namely the use of Standard Contractual Clauses to export data to the USA, the Court decided that they need complementary measures to guarantee protection.[8] However, two considerations can be made in this regard. First, those are contractual mechanisms that cannot be ensured in face of the government if it demands data for national security reasons. The second is that the decision did not make clear which mechanisms would actually ensure the data security. Hence, companies are – as well – in risk of implementing contractual or even technical measures for transfer data internationally and, in the future, those being considered not enough to compensate for the lack of protection in the third country.[9]

The CJEU concluded that this did not create a legal vacuum, since art. 49 of the GDPR "details the conditions under which transfers of personal data to third countries may take place in the absence of an adequacy decision under art. 45(3) of the GDPR or appropriate safeguards

[7] TRACOL, Xavier, "Schrems II: The return of the Privacy Shield" (2020) 39 Computer law & security review, 8. Available at www.sciencedirect.com/science/article/pii/S0267364920300893 accessed 3 February 2023.

[8] Data Protection Commissioner (n 1), para 133.

[9] MELTZER, Joshua P. "After Schrems II: The Need for a US-EU Agreement Balancing Privacy and National Security Goals" (2021) 2(1) Global Privacy Law Review, 87. Available at https://kluwerlawonline.com/journalarticle/Global+Privacy+Law+Review/2.1/GPLR2021007 accessed 3 February 2023.

under art. 46 of the GDPR".[10] In this scenario, art. 49(1)(a) of the GDPR allows cross-border transfers if the data subject has explicitly consented to it, after having been informed of the possible risks due to the absence of an adequacy decision and appropriate safeguards.

Even though the CJEU decision on the Schrems II case highlighted that art. 49 of the GDPR could still be applied, it also states that this data transfer mechanism is a "derogation for specific situation", which leads to an interpretation of, in essence, it being exceptional. Then, companies were left with no secure legal basis to transfer data to the United States, creating a high risk of responding for material or even non-material damages suffered by the data subject, as stated in art. 82(1) of the GDPR. They were also put in danger of having to pay the fines specified in art. 83(5)(c) of the GDPR, which can go up to 20 million euros or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year.

The tension culminated until the point where the Irish Data Protection Commission, in September 2020, demanded Facebook/Meta to stop exporting data to United States, and, in response, the company affirmed that if that was the case, it would stop its activities in Europe.[11] Now, the EDPB adopted a dispute resolution decision concerning a draft decision of the Irish Data Protection Authority on the matter.[12] In this scenario, since art. 49 of the GDPR was mentioned in the Court's Decision as the basis for inexistence of a legal vacuum to make international transfers, also considering the personal autonomy and freedom to contract of European citizens, should data subjects be able to consent

[10] Data Protection Commissioner (n 1), para 202.

[11] BEESLEY, Arthur, "Facebook's Meta facing order from Irish regulator to suspend data transfers to US" *The Irish Times* (Dublin, 22 February 2022). Available at www.irishtimes.com/business/facebook-s-meta-facing-order-from-irish-regulator-to-suspend-data-transfers-to--us-1.4808534 accessed 3 February 2023.

[12] 'EDPB resolves dispute on transfers by Meta and creates task force on Chat GPT' (13 April 2023) <https://edpb.europa.eu/news/news/2023/edpb-resolves-dispute-transfers-meta-and--creates-task-force-chat-gpt_en?mkt_tok=MTM4LUVaTS0wNDIAAAGLGpYNZFqROYpy4BUfa0wqSL4bSi6aLZ_2QXGb6JnYRcOjc8Cu6TuUKfDuBu0cmXYyqdGoKT2UPKJ5AMS5RXAQYB4lh0RMq54ddmE3l9mQK-wD> accessed 15 April 2023

with this data exportation in order to be able to use, for example, Facebook/Meta online services?

3. Consent in the GDPR and the special requirements of art. 49(1)(a)

Consent is accepted in art. 6(1) of the GDPR as a general legal basis for data processing. Nonetheless, the specific consent to perform cross-border data transfers shall be different from the one for data processing in general, according to the European Data Protection Board (EDPB) Guidelines 2/2018.[13] In this sense, both consents have specific requirements that need to be met. Concerning the consent of art. 49 of the GDPR, for international data transfers, it needs to comply with all the requirements for the two forms of consent, both the general and specific ones.

3.1. Validity of consent for data processing (art. 6(1) of the GDPR)

Consent is accepted as a mechanism to proceed with a lawful data processing, consonant art. 6(1) of the GDPR. In order to be valid, before accepting its terms, the data subject must have informational self-determination, meaning that he or she shall know all the risks and important factors involved with such data processing. This is an effort to prevent abusive privacy policies, as specified in several guidelines of the Data Protection Authorities.[14]

Hence, in order to be valid, in summary, consent shall be: (a) voluntarily given; (b) specific to each processing; and (c) with information about the controller's identity, what kind of data will be processed, how

[13] European Data Protection Board (EDPB), "Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679", 7. Available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en accessed 3 February 2023.

[14] See GDPR consent guidance of the Data protection authority UK and Guidelines on Consent by the Data Protection Working Party.

it will be used, and the purpose of the processing operations. The possibility of withdrawing consent must always be given and informed to the data subject. Lastly, consent must be unambiguous, granted by a clear affirmative act, which, according to the interpretation of the Court of Justice of the European Union, means an opt-in design.[15]

The main idea here is that a consent request actually makes the subject pause and reflect about the consequences of such act. As it is affirmed by Schermer, Custers and Van Der Hof, "In a sense, a consent transaction functions as a warning that a potentially harmful or legally meaningful moral transformation will take place that requires the (undivided) attention of the individual".[16]

In this way, in order to maintain the possibility of refusing or withdrawing consent, there should be an alternative to perform the service without it. This is because, denying or withdrawing consent and, consequently, being prevented from having access to the service, might have such a big negative impact in the life of the data subject that give him no other option other than to consent with it.[17] Consequently, in the case of international data transfers, the necessity of consenting with such transfer in order to be able to use the service would remove the 'freedom to consent' of the subject.

Hence, there should be a second possibility of performance of the service, either without the cross-border data transfer or through other transfer mechanism. This is due to the fact that, to comply with the freedom to consent and possibility of withdrawing, the data subject must have access to the service even if he or she declines to consent. The EDBP Guidelines highlights that the necessity of maintaining the

---

[15] See CJEU Case C-673/17 Bundesverband e.V. v Planet49 GmbH 01 October 2019 EU:C:2019:801.

[16] SCHERMER, Bart W., CUSTERS, Bart and VAN DER HOF, Simone, "The crisis of consent: how stronger legal protection may lead to weaker consent in data protection" (2014) 16 Ethics Inf Technol 171, 172.

[17] VAN CASTEREN, D.C.J., *Consent now and then*, Tilburg University, 2017, 14. Available at chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://arno.uvt.nl/show.cgi?fid=143636 accessed 02 February 2023.

possibility of withdrawing consent at any time might make it not a "feasible long-term solution for transfers to third countries".[18]

Then, although consent, in theory, could be used as an international data transfer mechanism, in order to be valid, it needs to comply with the necessary aspects to ensure a self-determination of the data subject. In this sense, there would be the necessity of creating a process where consent is not the only possible form of providing the service, in order maintain the data subject's freedom, while also being unambiguous. Nonetheless, if done so, all the requirements for a valid consent, as current interpreted, could be met.

3.2. Requirements of art. 49 of the GDPR

In addition to the requirements for the validity of consent in general, there are also the specific requirements of art. 49 of the GDPR, which claims to be a mere "derogation for specific situations". Hence, also in line with the Schrems II decision, this is a subsidiary possibility. To invoke it, first of all, the controller must reasonably explain why it was not possible to rely on the appropriate safeguards of art. 46 and 47 of the GDPR, as outlined by the European Data Protection Board. [19] After that, it shall be proven that the consent was valid, meaning that the data subject have the necessary information to give permission to the limitation of its fundamental right of data protection.

Thus, according to this article, there is also the necessity of informing all categories of data recipients and countries where data will be transferred. In addition, the data subject must be communicated of the possible risks of the exportation, due to the lack of an adequacy

[18] European Data Protection Board (n 13), 8.

[19] European Data Protection board, "Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 – Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems", 4. Available at https://edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union_en accessed in 03 April 2023.

decision and appropriate safeguards.[20] According to the EDPB Guidelines, this notice can be standardized, but it "should include for example information that in the third country there might not be a supervisory authority and/or data processing principles and/or data subject rights might not be provided for in the third country."[21] In this sense, the idea is to comply with the informational self-determination and give the subject all the information concerning that transfer in a clear way.

One issue raised here is that those are, in many times, complex information that simply cannot be passed in a clear and simple way to non-experts in the field. Then, it is considered that both the overload of information and transactions, as well as the absence of meaningful choice, negatively impacts the efficiency of consent in a practical way.[22] According to Schermer, Custers, and Van der Hof: [23]

> "As data processing becomes more and more complex, more factors need to be taken into account. The result is that the reality of data processing will become even further removed from the simplistic mental models employed by data subjects. This undermines the basic notion of consent, as it may be argued that consent is not fully informed and truly transformative, when the person who consents is unable to comprehend the consequences".

However, although difficult, and debatable the attention given to consent forms due to the overload of them, it is not impossible to find a design that put such information in a way that is considered specific enough while being clear to the data subject as well. Also, considering that the subject would have an actual choice on whether to consent or not, with the possibility of refusal and still using the service, as above

[20] European Data Protection Board (n 13), 8.
[21] European Data Protection Board (n 13), 8.
[22] SCHERMER, CUSTERS, and VAN DER HOF (n 16), 10.
[23] SCHERMER, CUSTERS, and VAN DER HOF (n 16), 11.

mentioned, there would not be an absence of choice to negatively impact efficiency of consent in this scenario.

Other requirements present on art. 49 of the GDPR are the non--repetitiveness and limited number of data subjects, which are the ones that translate more with the idea of it being a "derogation for specific situations". However, transfers made on basis of specific consent do not have to comply with those characteristics, as highlighted in the recital 111 of the GDPR and in the EDBP Guidelines. *In verbis*, "Article 49 (1) subpar. 1 (b), (c) and (e)) shall be limited to 'occasional' transfers, while such limitation is absent from the 'explicit consent derogation'".[24] Then, in this point, the regular use of such data transfer mechanism, *per si*, would not be an infringement of the law, since it can be repetitive and without limitation of number of data subjects.

Nonetheless, the premise of art. 49 of the GDPR is only being exceptional, since is supposed to be a "derogation for specific situations", which leads to a restrictive interpretation. In this subject, also according to the EDBP Guidelines, "These terms indicate that such transfers may happen more than once, but not regularly, and would occur outside the regular course of actions".[25] Yet, as above mentioned, in the Schrems II decision, the court asses that exactly this article would mean an absence of legal vacuum if it is not possible to use neither the legal ground of art. 45 and 46 of the GDPR to make international data transfers. [26]

Corroborating with the possibility of further use of this legal basis for cross-border data transfer, Professor Dr. von Danwitz, judge--rapporteur in both Schrems cases, on the German celebration of the 40th Data Protection Day, gave a personal statement about the possibility on expanding reliance on Article 49 GDPR derogations in the absence of an adequacy finding. In his words, "the opportunities granted by Article 49 have not been fully explored yet. I believe they are not so

[24] European Data Protection (n 13), 5.
[25] European Data Protection (n 13), 4.
[26] Data Protection Commissioner (n 1), para 202.

narrow that they restrict any kind of transfer, especially when we're talking about transfers within one corporation or group of companies".[27]

In this sense, given that the provision of art. 49 of the GDPR is brought up almost as a solution to a possible legal vacuum created on the impossibility of using art. 45 and 46 of the GDPR, and considering that the provision of the law does not prohibit the repetitive use and for an unlimited number of data subjects, as a logical consequence, the consent of art. 49(1)(a) can and shall be used in such a case. Also, the situation of having a state with a core incompatibility, inhibiting an adequacy decision or insurance of appropriate safeguards, such as United states' politics of national security, could be interpreted as a specific situation that allows the derogation proposed on art. 49 of the GDPR.

The ponderation commonly made here is that, ultimately, this would be "contrary to the previously-stated policy objective and could even ultimately be less protective for data subjects".[28] Although this is a true statement, given the above mentioned interpretation, the use of consent as a regular mechanism for cross-border transfer is not prohibited by law. Also, considering the necessary characteristics to the consent form, a fine level of protection can be achieved. In that regard, if there is a consent that is freely given, actually giving the data subject a choice in order to decline consent and still so use the service, also with the appropriate information about the risks of the transfer in a clear way, the data subject can be empowered with self-determination to make a clear and valid choice.

On the other hand, if the interpretation of data protection rules is so restrictive that impossibilities the use of consent as a ground for international transfer, it can remove from the data subject the alternative of making such conscient choice. Consequently, the citizen could be left

[27] DANWITZ, von, "Europäischer Datenschutztag 2021" (2 February 2021). Available at https://www.youtube.com/watch?v=2hyETsfhErg&t=4320s Accessed 2 February 2023.

[28] RONCO Emmanuel, GERLACH Natascha and FARMER Natalie, "Recommendations of the EDPB Further to the CJEU's Schrems II Judgment: One Step Forward, Two Steps Back?" 2(1) Global Privacy Law Review, 95. Available at https://kluwerlawonline.com/journalarticle/Global+Privacy+Law+Review/2.1/GPLR2021008 accessed 03 February 2023.

without the possibility of contracting the service at all, as in the Facebook/Meta example, which translate in such an intervention of the state that inhibits the individual's autonomy to contract.

4. Consent as a tool to limit fundamental rights

No fundamental right is absolute, the possibility of limitation is established in art. 52 of the Charter of Fundamental Rights of the European Union (EU Charter). In that light, the personal autonomy can balance the individual's fundamental right, since it is possible to consent to a limitation of it. This is acceptable, for example, when deciding to make a procedure that harms the person's physical integrity, such as body piercing, or even to refuse medical assistance, threatening the subject's right of life, as decided in the case Jehovah's Witnesses of Moscow and Others v. Russia.[29] In this sense, it is a established idea, according to the jurisprudence of the European Court of Human Rights (ECtHR), that the state cannot "protect the individual against himself".[30]

One consequent fundamental right from the personal autonomy is the freedom to contract, which, even though is not explicit in primary Community law, according to the doctrine, "it is nonetheless comprehensively safeguarded through other guarantees found therein"[31] and "enjoys comprehensive recognition in the jurisprudence of the Court of Justice".[32] Therefore, in the analyzed scenario, consent would be used as a tool to consider that the individual freedom to contract can override the subject's right of data protection, if chosen to, even in a case of transfer to a third country without the same level of protection of the European Union.

---

[29] European Court of Human Rights (ECtHR) Jehovah's Witnesses of Moscow and Others v. Russia App no 302/02 (10 June 2010).

[30] VAN DROOGHENBROECK, Sébastien, *When Human Rights Clash at the European Court of Human Rights: Conflict or Harmony?* (OUP 2017), 67.

[31] BASEDOW, Jürgen, "Freedom of Contract in the European Union" (2008)6 European Review of Private Law 901, 909.

[32] Ibid 913.

Along these lines, recital 4 of the GDPR highlights that data protection "is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality", enabling the analysis in face of freedom to contract. After all, the impossibility of such free will would ultimately mean an absolute data protection right and lead to a state that protect the individual against himself, which is unacceptable.[33]

If briefly analyzed this possibility under the guidelines of the EDPS on assessing the proportionality of measures that limit the data protection right, [34] it is possible to conclude that, for instance, the freedom to contract, as an expression of self-determination trough consent to data exportation, can override the fundamental right of data privacy. The assessment must be based on art. 52 of the EU Charter, which defines that any limitation of fundamental rights must be: (a) provided by the law; (b) respect the essence of the right; (c) meet objectives of general interest recognized by the Union; and (d) also be necessary and proportionate.

Regarding the first three elements, the limitation is provided by law, given that consent is established in the EU Charter of fundamental rights and in the General Data Protection Regulation as a tool to limit the subjects right to privacy and data protection. It also respects its essence by giving the subject informational self-determination, thus not emptying the basic content of the right. In this sense, the possibility of consenting with data processing empowers the individual to make an informed decision about one's personal data while using the service provided by the company.

Thirdly, the measure meets an objective of general interest, namely the function of data in society, as declared in the recital 4 of the GDPR,

[33] VAN DROOGHENBROECK (n 30).

[34] European Data Protection Supervisor (EDPS) Assessing the necessity of measures that limit the fundamental right to the protection of personal data, 6-7. Available at https://edps.europa.eu/data-protection/our-work/publications/guidelines/edps-guidelines-assessing-proportionality--measures_en accessed 3 February 2023.

also in relation to what it can make data subjects achieve and their freedom to contract. So, as stated in the law, data can 'serve mankind', not the contrary. In a way, such interpretation is necessary in order to not trying to protect the subject's data up to the point where he/she is not able to enjoin services that are served for his/her self-interest.

In relation to the necessity test, it should be analyzed the effectiveness of the measure for the objective, alongside with whether it is less intrusive compared to other options for achieving the same goal.[35] In this sense, the consent to have data sent to a third country without the same level of data protection – USA in the *Facebook/Meta* case – is effective to guarantee EU Citizens their freedom to contract online platform's services.

Also, it gives the data subject informational self-determination to decide whether to access the online service and have its data shared internationally, or not. Thus, it can be considered less intrusive compared to other options that share it solely relying on measures that don't give proper information and may not ensure the level of protection, since the government can override it. Or even share it laying on adequacy decisions that can, at any time, already be invalid, due to the *ex-tunc* effects of invalidation.

Additionally, the measure is proportionate, since the disadvantages of risking the subject's data protection with the transfer are outweighed by the advantages of respecting the individual's autonomy to contract and ensuring informational self-determination. Highlighting that the measure is the possibility of consent by the data subject, to ensure his/her freedom, not necessarily the transfer itself. Ultimately, the individual should have the power to decide if it wants to protect or limit his/her data protection fundamental right.

To that end, scholars alert to the overload of consent and the impossibility of it being well-informed, leading to the data subject waiving

[35] Ibid 5.

its rights without really comprehending it.[36] Therefore, a case-by-case analysis should focus on the specific consent that was given, making sure it was not abusive, given all the previously mentioned requirements. Also, the controller must have reasons on why it was not possible to ensure one of the appropriate safeguards of article 46 and 47. This residual characteristic of consent to perform cross-border transfers follows both from the rationale of the articles of the GDPR and the CJEU decision in the Schrems II case, as mentioned above. [37]

In that sense, the challenge would be to prove the impossibility of ensuring one of the previous legal grounds and, most of all, have a well--informed and freely given consent. Nonetheless, if it was the case and the consent was, in fact, valid, the person should be able to contract the service accepting the data transfer. After all, if the information is put in a clear way and subjects choose not to give it proper attention, it still falls in their personal autonomy.[38] In addition, there are technical measures that can better inform the subject and facilitate its act of consenting.[39]

Even so, in one hand, the absence of the possibility to consent with the data transfer in order to use the service can be an intervention of the state in the individual's life that is too severe, given that the possibility of consent with a limitation of one's fundamental right apply even for the right of life. However, on the other hand, allowing the data protection of the subject limits itself to a single clause which will probably be ignored by the person in order to use the service, does not balance the power imbalance of huge entrepreneurs that profit billions from the subject's data and the individual himself, as the GDPR aims to do.

Nonetheless, both objectives can be met by a consent that is actually valid, namely given by a person with self-determination to do so, informed and conscient about the risks of the transaction, also with a

[36] SCHERMER, CUSTERS, and VAN DER HOF (n 16), 177-178.

[37] Ibid 24.

[38] BETKIER, Marcin, *Privacy Online, Law and the Effective Regulation of Online Services* (CUP 2019), 30.

[39] Ibid ch 6.

parameter of what will be done with his/her data. In this case, both the empowerment of the individual aimed by the GDPR, and the protection of one's freedom to contract, can be met in order to allow a better data management without such a protection of data that impedes the individual's free will. After all, since consent is a tool to limit fundamental rights stated both in the EU Charter and in the GDPR, it should be ensured to allow cross-border data transfers.

5. Conclusions

In the Schrems II decision, the Court of Justice of European Union invalidated the most common grounds for international data transfer to the United States of America, leaving companies with high risk of being hold liable, due to the difficulty of complying with art. 45 and 46 of the GDPR. In that scenario, art. 49(1)(a) of the GDPR states the possibility of transfers based on specific consent of the data subject. Even though this provision is described as a "derogation for specific situation" and commonly had a strict interpretation, the CJEU Decision on the Schrems II Case highlighted that the absence of possible compliance with art. 45 and 46 of the GDPR would noy create a legal vacuum, due to the provisions of art. 49 of the GDPR.

Therefore, using the specific consent of art. 49(a) of the GDPR as a regular legal basis to transfer data to third countries without the same level of protection of the European Union is compatible with the provisions of the law, as long as fulfilled the requirements for a valid consent. This is mostly because, even though described as a "derogation for specific situation", it does not have to be non-repetitive or to a limited number of data subjects, as have other derogations. Nonetheless, it shall be a different consent than the one given for data processing in general, also informing categories of data recipients and countries where data will be transferred and the possible risks of the exportation, due to the lack of an adequacy decision and appropriate safeguards.

Beyond those specific requirements, in order to be valid the consent shall also respect: (a) the freedom to consent, which would imply in the necessity of an alternative to the consent being withdraw or declined and the service still be provided; and (b) give clear and accurate information, in order to properly give the data subject, the possibility of making a conscience choice about the usage of his or her data. Although it can be tricky to meet all those requirements, there is no factual contradiction that makes it impossible to achieve.

However, despite not being expressively prohibited by any provision of the law, more use of consent forms can generate an overload of consent and be contrary to the policy objective, practically forcing the data subject not to give the proper attention to the information due to its amount. Moreover, the interpretation currently given by the EDBP guidelines to the law do not consider possible to use consent as a regular mechanism for cross-border data transfers, asserting that the consent of art. 49 of the GDPR is an exceptional hypothesis.

Nonetheless, such strict interpretation, inhibiting the use of this mechanism as a regular legal basis for international data transfer, would contradict the Court's decision that point out its usage as an absence of legal vacuum. Moreover, it would not allow the subject to consent with the limitation of his/her fundamental right in order to contract the service, implying in a state that "protect the individual from himself", which is not accepted in the European jurisprudence, not even for the right of life.

Hence, the main point in an assessment of the validity of using consent as a legal basis to make international data transfer should be to verify if the consent in case is not abusive, so it may serve properly as a tool to allow informational self-determination. After all, the GDPR ensures in its recital 4 that "the processing of personal data should be designed to serve mankind", not the contrary. As so, although named as a "derogation for specific situation", given it is not prohibited by law, it should be possible to use the specific consent of art. 49(1)(a) of the GDPR as a regular legal basis to transfer data to third countries

without the same level of protection of the EU, as a consequence of the personal autonomy and freedom to contract.

O Direito da Proteção de Dados nas plataformas digitais: uma relação necessária com o Direito da Concorrência?

Diana Camões[1]

Resumo: O presente artigo visa refletir sobre a possível interligação entre o direito da proteção de dados e o direito da concorrência, analisando os diversos pontos de contacto e os possíveis enquadramentos. Num mundo globalizado e digital, onde as plataformas digitais exercem uma função primordial, vários desafios têm emergido quanto ao cumprimento do regime do direito da proteção de dados, sendo que em determinadas situações o seu incumprimento pode resultar, igualmente, em condutas com efeitos lesivos na concorrência. Neste sentido, procura-se analisar se uma aplicação coerente de ambos os regimes é necessária ou, inversamente, uma possibilidade utópica.

***Palavras-Chave**: RGPD, plataformas digitais, direito da proteção de dados, direito da concorrência*

Abstract: This article aims to reflect on the possibility of the connection between data protection law and competition law, by analyzing the different contact points and the possible framework. In a globalized and digital world, where digital platforms exercise a fundamental function,

[1] Investigadora Júnior no Observatório da Aplicação do Direito da Concorrência. icenciatura em Direito pela Faculdade de Direito da Universidade Católica do Porto, Mestrado em Direito Internacional e Europeu pela Faculdade de Direito da Universidade Católica do Porto (em elaboração da Dissertação) e Pós-Graduação em Direito da Proteção de Dados pelo Centro de Investigação de Direito Privado da Faculdade de Direito da Universidade de Lisboa. ORCID: 0000-0001-8827-007X.

several challenges have arisen regarding the fulfillment of the data protection law's regime and albeit certain situations and their infringement may work, equally, in dealings with harmful effects in competition. That way, we look to analyze if a coherent application towards both regimes is necessary or, inversely, a utopic possibility.

Key words*: GDPR, digital platforms, data protection law, competition law*

1. Introdução

As plataformas digitais revolucionaram o mundo, tendo novas problemáticas emergido. Por um lado, o seu surgimento foi essencial para a revolução tecnológica operada e para "uma democratização do acesso à informação"[2]. Atualmente, estas são o novo fórum público, onde os indivíduos têm a oportunidade de difundir os seus pensamentos, bem como exercer os seus direitos e liberdades. Existiu, por isso, uma verdadeira emancipação face à esfera pública: sendo as plataformas controladas por entidades privadas, são elas que têm o poder, se assim o entenderem, de moldar conteúdos e restringir direitos fundamentais exercidos pelos seus utilizadores nas plataformas.[3]

---

[2] SOUSA, Simão Mendes de – *Constitucionalismo Digital Uma Introdução,* Almedina, 2022, pp. 32-33. O Autor advoga, ainda, que as plataformas se encontram relacionadas com uma sociedade liberal, ao permitir-se que todos os indivíduos, sem exceção, tenham acesso à informação que pretendem.

[3] Como postulam MIR, Joana Barata e BASSINI, Marco "Freedom of Expression in the Internet" *in* Oreste Pollicino and Graziella Romeo (Ed.*) The Internet and Constitutional Law – The protection of fundamental rights and constitutional adjudication in Europe,* Routledge, London*,* pp. 71-93(81), esta nova era de descentralização criou novas oportunidades para os indivíduos receberem conteúdo e comunicar no mundo online. No mesmo sentido, POLLICINO, Oreste, BASSINI, Marco e GREGORIO, Giovanni de – *Internet Law and Protection of Fundamental Rights,* Bocconni University Press, 2022, p. 13, salientam que, ao contrário dos atores públicos, as plataformas digitais não têm de assegurar as mesmas salvaguardas constitucionais quando tomam decisões quanto à organização e remoção dos conteúdos online.

Adicionalmente, assistiu-se a uma massificação do tratamento de dados pessoais, sendo que, num mundo globalizado e digital, estes são "o novo petróleo, sendo um importante bem transacionável."[4] Destarte, e como aponta GIOVANNI DE GREGORIO, há uma diferença primordial: ao contrário do petróleo, na sociedade digital o uso de dados pessoais constitui uma fonte quase inesgotável, podendo ser usada múltiplas vezes[5]. Cada vez mais, as informações armazenadas permitem deter todos os fatores relevantes sobre os indivíduos e, no digital, a informação é poder. Deste modo, pese embora o surgimento do Regulamento Geral de Proteção de Dados (doravante designado por RGPD)[6] tenha permitido "colocar os dados pessoais e o seu tratamento no centro das preocupações jurídicas e empresariais"[7], a realidade demonstra-nos que estas matérias poderão necessitar de uma abordagem holística, mormente quando refletimos sobre o tratamento a dar.

Por conseguinte, o presente artigo visa analisar os principais problemas que se colocam para os utilizadores destas plataformas e, à luz da jurisprudência recente, avaliar se uma articulação com o Direito da Concorrência é possível ou somente uma utopia.

2. Plataformas Digitais e o cumprimento da Proteção de Dados: uma realidade utópica?

As Redes Sociais tiveram um impacto inegável no nosso quotidiano. Parece que foi ontem que o Facebook (atual Grupo Meta) surgiu

---

[4] CARVALHO, Jorge Morais – *Manual de Direito do Consumo,* 7.ª Edição, Almedina, 2021, p. 62.

[5] GREGORIO, Giovanni de – *Digital* Constitutionalism *in Europe – Reframing Rights and Powers in the Algorithmic Society,* Cambridge University Press, 2022, pp. 225-226,

[6] Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados. Substituiu a Diretiva 95/46/EC do Parlamento Europeu e do Conselho de 24 de outubro de 1995 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

[7] CORDEIRO, A. B. M. – *O Direito da Proteção de Dados à luz da Lei n.º 58/2019,* Reimpressão, Almedina, 2020, p. 29.

como novidade, prometendo, sob a aparência de um serviço gratuito[8], conectar-nos com o resto do mundo. Redes sociais como o Hi5 perderiam o seu espaço nesta inegável batalha pela conquista da Internet. Note-se, todavia, que o direito fundamental à privacidade antecede esta revolução no digital[9], pelo que o direito à proteção de dados deve entender-se como o conjunto "sistematizado de princípios, normas e institutos que regula os dados pessoais e o seu tratamento."[10][11] Neste sentido, o surgimento do RGPD foi um dos veículos impulsionadores para a mudança de paradigma: o tratamento de dados pessoais em grande escala dos utilizadores deveria, claro está, seguir os trâmites da legislação europeia, tendo-se atingido um novo nível de proteção, nesta nova era de digitalismo constitucional.[12]

---

[8] "Adira, é gratuito." Este foi o slogan que caracterizou a entrada do Facebook no mercado.

[9] O Direito Fundamental à privacidade antecede a revolução tecnológica, sendo entendido como um mecanismo para proteger os indivíduos contra a ingerência na sua vida privada, conceito este interpretado amplamente. O conceito de vida privada não é passível de definição exaustiva, tal como já afirmado inúmeras vezes pelo TEDH. A título de exemplo, *vide* TEDH, Niemietz c. Alemanha*,* processo n.º 13710/88, 16 de dezembro de 1992, parágrafo 29 e TEDH, Pretty c. Reino Unido, processo n.º 2346/02, 29 de abril de 2002. Ademais, a noção de direito à privacidade foi primeiramente introduzida pela doutrina norte-americana. Assim, na ótica de WARREN, Samuel e BRANDEIS, Louis – "The Right to Privacy", *in Harvard Law Review* Volume 4, N.º 5, 1890, pp. 193-220 (196), o desrespeito por parte da imprensa da privacidade dos indivíduos, a promoção do *gossip,* a intensidade e complexidade da vida demonstraram a importância de respeitar a privacidade dos indivíduos, enquanto valor primordial na sociedade. Este encontra acolhimento em diversos diplomas internacionais, mormente no Art. n.º 12 da DUDH, bem como Art. n.º 8.º da CEDH.

[10] CORDEIRO, A. M. – *O Direito… cit.,* p. 35. O mesmo autor advoga que, atendendo ao conteúdo do RGPD, uma noção restrita se impõe, definindo-o como "o conjunto sistematizado de princípios, normas e institutos que regula os dados pessoais das pessoas singulares e seu tratamento."

[11] PINHEIRO, ALEXANDRE, *Privacy e Proteção de Dados Pessoais: a Construção Dogmática do Direito à Identidade Informacional*, 1.ª edição, AAFDL, 2015, p. 777 defende que este deve ser integrado num direito de maior latitude, o direito à identidade informacional*,* dado estar em causa uma personalidade composta por várias posições jurídicas. Para uma visão crítica, *vide* BARBOSA, Mafalda Miranda, "Proteção de Dados e Direitos de Personalidade: Uma Relação de Interioridade Constitutiva. Os beneficiários da proteção e a Responsabilidade Civil", *in AB Instantia,* Ano V, N.º 7, 2017, pp. 13-47(29).

[12] *Vide* CELESTE, EDOARDO – *Digital Constitutionalism – The Role of the Bill of Rights,* Routledge, 2023, disponível em <https://www.taylorfrancis.com/books/oa-mono/10.4324/9781003256908/digital-constitutionalism-edoardo-celeste> consultado em 21.01.2023.

Destarte, as diversas plataformas não conseguem almejar um pleno cumprimento do RGPD (e de outros diplomas igualmente relevantes). A título de exemplo, em 2022, o Grupo Meta enviou um comunicado à Comissão Europeia, ameaçando deixar a União Europeia, caso não lhe fosse permitido armazenar os dados dos seus utilizadores em servidores fora da União.[13] Recentemente, a Comissão Nacional de Proteção de Dados da Irlanda aplicou uma coima de 390 milhões ao Grupo Meta, por obrigar os seus utilizadores a aceitar novas condições para anúncios.[14] A este propósito, a Comissão Europeia tem, igualmente, deixado vários avisos ao TikTok sobre a necessidade de serem salvaguardados os direitos dos utilizadores em matéria de proteção de dados[15], tendo recentemente proibido os seus funcionários de usar a aplicação.[16] Não obstante todos os mecanismos de proteção reforçados pelo ativismo judicial dos

[13] Não podemos ignorar que o tratamento realizado tem um caráter especial, já que estando em causa a Internet, este é levado a cabo através de uma rede eletrónica de caráter mundial. Ainda assim, podemos falar numa verdadeira extraterritorialidade do RGPD, dado que este se aplica, nos termos do n.º 1 do art. 1.º, ao "tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União." Para mais desenvolvimentos, *vide* GSTREIN, Oskar Josef e ZWITTER, Andrej Janko – "Extraterritorial application of the GDPR: promoting European values or power?" *in Internet Policy Review,* Volume 10, n.º3, 2021, disponível em <https://doi.org/10.14763/2021.3.1576> consultado em 21.01.2023. *Vide* MONIZ, Graça Canto – "Finally: a coherent framework for the extraterritorial scope of EU data protection law – the end of the linguistic conundrum of Article 3(2) of the GDPR" *in EU Law Journal,* Volume 4, n.º 2, 2018, pp. 105-106.

[14] Irish Privacy Regulator Fines Facebook 265 mln euros, Reuters, 28 de novembro 2022, disponível em <https://www.reuters.com/technology/irish-regulator-fines-facebook-265-mln-euros-over-privacy-breach-2022-11-28/> consultado em 22.01.2023.

[15] EU Leaders fire warning shots at tik tok, Politico, 10 de Janeiro de 2023, disponível em <https://www.politico.eu/article/eu-leaders-fire-warning-shots-at-tiktok-over-privacy/> consultado em 22.01.2023.

[16] Comissão Europeia proíbe funcionários de usar aplicação TikTok, Diário de Notícias, 23 de fevereiro de 2023, disponível em <https://www.dn.pt/internacional/comissao-europeia-proibe-funcionarios-de-usar-aplicacao-tiktok-15889194.html> consultado em 24.02.2023.

tribunais[17], e não sendo possível ignorar que a maioria destas plataformas detêm uma posição de primazia nos mercados digitais, aquela que seria uma matéria de direito da proteção de dados passa, igualmente, a poder conflituar com outras áreas do direito, mormente o direito da concorrência – conforme teremos agora a oportunidade de analisar.

3. A Aplicação do Direito da Proteção de Dados pelas Autoridades da Concorrência

Durante muitos anos, existiu uma tendência para dividir clara e evidentemente aquelas que seriam as fronteiras entre estas duas áreas do direito. Recordemos, a título de exemplo, a Decisão da Comissão

[17] Exemplo paradigmático é o Direito ao Esquecimento, sufragado no Caso do Tribunal de Justiça, Google Spain SL e Google inc. contra Agencia Española de Protección de Datos e Costeja González, C-131/12, 13 de maio de 2014. Entre outras questões, estava em causa saber se o Sr. Costeja teria direito a que a Google.es apagasse todas as referências respeitantes às suas dívidas à Segurança Social. Não podemos olvidar que, à data, a Diretiva 95/46/EC era omissa quanto a este ponto, tendo o TJ considerado (contrariamente à posição sufragada pelo Advogado-Geral) que os interesses do Sr. Costeja, atendendo aos arts. 7.º e 8.º da CDFUE, prevaleceriam sobre o interesse económico do operador do motor de busca, bem como o interesse público em aceder a essa informação. A este propósito, POLLICINO, Oreste e ROMEO, Graziella "Concluding Remarks Internet Law, protection of fundamental rights and the role of constitutional adjudication", *in* Oreste Pollicino e Graziella Romeo (Ed) *The Internet and Constitutional Law,* Routledge, 2020, pp. 234-250(248) advogam que uma excessiva proteção do direito ao esquecimento corre o risco de limitar a proteção necessária do direito à liberdade de expressão e o direito a cada utilizador ser devidamente informado, considerando que, *in casu* o TJ simplesmente ignorou o art. 11.º da CDFUE, não avaliando corretamente o conflito de direitos. Pelo contrário, BOTELHO, Catarina – "Novo ou Velho Direito? – O Direito ao Esquecimento e o Princípio da Proporcionalidade no Constitucionalismo Global" *in AB Instantia,* Ano V, n.º 7, 2017, pp. 49-71(66) não concorda com o termo ativista (o qual pode ter uma conotação negativa), considerando que o TJ limitou-se interpretar a Diretiva, o qual implicitamente já consagrava o direito ao esquecimento. Para uma análise da eficácia extraterritorial do direito ao esquecimento *vide* VICENTE, Dário Moura – "Aplicação Extraterritorial do Direito ao Esquecimento na Internet?" *in ROA* Ano 80 Volume III/IV, pp. 475-488. Saliente-se que este acórdão assumiu uma enorme importância, tendo o direito ao apagamento sido transposto para a versão final do Art. 17.º do RGPD. Finalmente, recentemente o TJ deu um novo passo no sentido da densificação deste direito. No Caso do TJ, Tu, Re c. Google LLC*,* C-460/20, 8 de dezembro de 2022, considerou-se que o operador do motor de busca deve remover a informação quando a pessoa que o requer demonstre que essas informações são inexatas. Trata-se, pois, de mais um caso que evidencia a importância da atuação do TJUE.

Europeia relativa à operação de concentração do Facebook/Whatsapp[18] e da Microsoft/Linkedin[19] onde categoricamente se afirmou que qualquer preocupação relacionada com o direito da proteção de dados escaparia ao escopo de aplicação do direito da concorrência. Anteriormente, no caso Asnef-Equifax[20], o Tribunal de Justiça (doravante TJ) adotou a mesma posição. No entanto, temos vindo a assistir a uma progressiva modificação da *praxis* existente, passando a proteção de dados a ser um elemento a ter em consideração.[21]

A mudança de paradigma ocorreu com a Decisão da Autoridade da Concorrência Alemã (*Bundeskartellamt*)[22], na qual se considerou que o Facebook estaria a incorrer num abuso de posição dominante (Art. 102.º do TFUE) por tornar a utilização desta rede social sujeita à condição de se aceitar que os dados recolhidos pelo Facebook fossem misturados com dados provenientes de serviços terceiros, violando-se, assim, o RGPD. Esta foi a primeira vez que uma Autoridade da Concorrência baseou a sua decisão numa violação do RGPD, daí o seu caráter pioneiro.[23] Tal decisão foi objeto de recurso por parte do Grupo Meta para o Tribunal Regional de Düsseldorf, tendo este procedido ao reenvio prejudicial para o TJ.

Estamos, assim, diante aquilo que alguns autores apelidam de "dilema de regulação."[24] A doutrina divide-se nesta questão. Contra esta aplicação, postula-se que outras áreas serão mais adequadas a regular este tipo de situações, mormente o direito da proteção de dados e do

---

[18] Decisão da Comissão Europeia, COMP/M.7217 – Facebook/Whatsapp, 3 de outubro de 2014, parágrafos 164-165

[19] Decisão da Comissão Europeia, COMP/M.814, 6 de dezembro de 2016.

[20] Caso do TJ, Asnef-Equifax c. Ausbanc*,* C-238/05, 23 de novembro de 2006, parágrafos 63-64.

[21] PAIS, Sofia – "Big Data and Big Databases between privacy and competition", *in* Joe Cannataci, Valeria Falce e Oreste Pollicino (Ed) *Legal Challenges of Big Data,* Edward Elgar, 2020, pp, 15-45(29).

[22] Bundeskartellamt, B6-22/16, 6 de fevereiro de 2019.

[23] PAIS, Sofia, "Big Data…" *cit.*, p. 30. *Vide* SCHWEITZER, Heike e GUTMANN, Frederick – "Unilateral Practices in Digital Market", *in* Frédéric Jenny e Nicolas Charbit (Ed) *Competition Law Digest,* 5.ª edição, Concurrences, 2022, pp. 483-532(504).

[24] BOTTA, Marco e WIEDEMANN, Klaus – "The Interection of EU Competition, Consumer and Data Protection in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey", in *The Antitrust Bulletin,* Volume 64, n. .º 3, 2019, pp. 428-446(445).

consumo.[25] Na esteira desta doutrina, para aferir se há ou não uma conduta que produza efeitos anticoncorrenciais, a violação de uma outra área do direito (*in casu*, do RGPD) não permite estabelecer qualquer nexo de causalidade quanto ao incumprimento do direito da concorrência.[26] Adicionalmente, evidencia-se que isto é suscetível de gerar a existência de decisões contraditórias, bem como um enfraquecimento do próprio RGPD.[27] Finalmente, advoga-se que tal não tem em consideração as diferenças entre ambos os regimes de proteção.[28]

Inversamente, os defensores da sua aplicação consideram que deverá ser tido em conta a existência de objetivos comuns entre o direito da concorrência e o direito da proteção de dados.[29]

Por outro lado, tal permitirá incrementar a atuação das autoridades em relação às novas formas de condutas comerciais e vice-versa[30], reforçando-se a complementaridade entre ambas.[31] Não obstante todas

---

[25] BERGH, Roger Van Den e WEBER, Franziska – "The German Facebook Saga: Abuse of Dominance of Abuse of Competition Law?" *in World Competition* 44, n. .º 1, 2021, pp. 29-52(39). KADAR, Massimiliano – "European Union Competition Law in the Digital Era", *in Zeitschrift fur Wettbewesbsrecht,* 4/2015, 1-15(11), disponível em <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2703062> consultado em 26/01/2023.

[26] ROBERTSON, Viktoria – "Excessiva Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data", *Working Paper,* 2019, 1-19, disponível em <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3408971> consultado em 26.01.2023.

[27] WITT, Anne – "Facebook v. Bundeskartellamt – May European Competition Agencies Apply the GDPR?", *Competition Policy International, TechREG CHRONICLE,* 2022, p. 7, disponível em <https://ssrn.com/abstract=4089978>, consultado em 26/01/2023.

[28] DZHULIIA, Lypalo – "Can Competition Protect Privacy? An Analysis Based on the German Facebook Case", in *World Competition* 44, n. .º 2, 2021, pp. 169-198(188-189). Como afirma a autora, não só ambos os ramos têm naturezas sancionatórias distintas, como o RGPD baseia-se numa aplicação *ex ante* o que seria difícil de conciliar com o facto de o direito da concorrência ser aplicado *ex post* em certas práticas anticoncorrenciais.

[29] WIEDEMANN, Klaus – "Data Protection and Competition Law Enforcment in the Digital Economy: Why a Coherent and Consistent Approach is Necessary", in *International Review of Intellectual Property and Competition Law,* 52, 2021, pp. 915-933(924) invoca três objetivos comuns: ambos visam proteger o mercado interno, os consumidores em situações de poder ou transações comerciais injustas e ambos protegeriam a concorrência pelo mérito.

[30] Tal como salienta PAIS, Sofia, "Big Data…" *cit.,* p. 35.

[31] CHIRITA, Anca D. – "The Rise of Big Data and the Loss of Privacy", in Mor Bakhoum *et al* (Ed) *Personal Data in Competition, Consumer Protection and Intellectual Property Law Towards a Holistic Approach,* Springer, Volume XXVIII, 2018, pp. 153-187(168) postula que, caso esta fosse uma situação que apenas afetasse poucos indivíduos, o direito do consumo seria suficiente. No entanto, não o sendo, o direito da concorrência não poderá fechar os olhos a estas situações, devido à sua amplitude.

estas considerações, a verdade é que o Advogado-Geral (doravante AG) abriu porta a esta possibilidade nas suas conclusões.[32] Desde logo, advogou não estarmos diante um caso em que o *Bundeskartellamt* tenha aplicado o RGPD a título principal.[33]

Por conseguinte, considerou nuclear que as autoridades da concorrência respeitem o princípio da cooperação leal[34], conquanto *(i)* não se afastem das posições das autoridades competentes em matéria de proteção de dados[35] tendo em conta as investigações por ela realizadas e, na medida do possível, *(ii)* procedam à sua consulta sempre que tenham dúvidas sobre a sua interpretação.[36] *In casu,* além de ter considerado que o *Bundeskartellamt* cumpriu com estas obrigações, concluiu que não houve violação dos Arts. 55.º a 66.º do RGPD[37], abrindo-se, pois, a possibilidade para uma Autoridade Concorrência aplicar, a título incidental[38], o RGPD sempre que tal seja relevante para o procedimento dentro das suas competências. Resta-nos, pois, aguardar com expectativa a posição do TJ, a qual poderá impactar (e de que maneira) a forma como perspetivamos o direito da concorrência e o direito da proteção de dados.[39]

---

[32] Conclusões do Advogado-Geral Athanasios Rantos, C-252/21, 20 de setembro de 2022.

[33] *Ibid,* parágrafos 17-18.

[34] De acordo com o n.º 3, do art. 4.º do TUE, "a União e os Estados-Membros respeitam-se e assistem-se mutuamente no cumprimento das missões decorrentes dos Tratados."

[35] Conclusões do Advogado-Geral, C-252/21, parágrafo 30.

[36] *ibid,* parágrafos 29-30. Não existindo uma decisão sobre a matéria da autoridade de controlo de proteção de dados, deverá ainda assim encetar contactos, no sentido de promover uma maior cooperação entre ambas.

[37] *Vide* SÍTIMA, Inês – "Artigo 55.º Competência", *in* A. M. Cordeiro (Coord.) *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019,* Almedina, 2021, pp. 381-455.

[38] Terá sempre de ocorrer no âmbito de uma investigação dentro dos seus poderes em matéria de direito de concorrência.

[39] HUNT, Matthew e BARON, Victoria – "Is Competition law taking over data protection claims?", in Britows, 10 outubro 2022, disponível em <https://www.bristows.com/news/is-competition-law-taking-over-data-protection-claims/> consultado em 27.01.2023, advogam que tal levará as autoridades da concorrência, dado terem mais recursos e mecanismos, a tomarem conta de situações que de outro modo caberiam às autoridades de proteção de dados.

4. Problemáticas que emergem

4.1 O Consentimento no contexto das plataformas digitais

Um dos tópicos mais sensíveis invocados pelo *Bundeskartellamt* prende-se com a validade do consentimento fornecido pelos utilizadores, já que estes não terão noção da amplitude dos dados pessoais recolhidos pelo Facebook[40] e, encontrando-se numa posição dominante[41], o consentimento não poderá ser livre e informado.

Nos termos do n.º 11 do art. 4.º do RGPD, o consentimento corresponde à "manifestação de vontade, livre, específica, informada e explícita, através do qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados que lhe digam respeito sejam objeto de tratamento."[42] MAFALDA MIRANDA BARBOSA advoga que este "surge como uma forma de afastar a ilicitude de um atentado não contra a própria autonomia que se exerce, mas contra um outro bem jurídico."[43] No contexto das plataformas digitais, é muito comum que os utilizadores, depois de lerem os termos e condições, deem o seu consentimento para o respetivo tratamento dos dados. Destarte, não deixamos de estar perante um fundamento de licitude

[40] Para uma análise do conceito de dado pessoal *vide* CORDEIRO, A. M. – "Dados Pessoais: conceitos, extensão e limites" *in Revista de Direito Civil,* n.º 2, 2018, pp. 297-321.

[41] O Abuso de posição dominante pressupõe: (*i)* que se trate de uma empresa, *(ii)* a existência de uma posição dominante, *(iii)* um abuso (sendo que, de acordo com a jurisprudência do TJ, Continental Can*,* C-6/72, 21 de fevereiro de 1973, par. 26, o conceito de abuso é amplo, compreendendo os abusos de exclusão e os abusos de exploração) e *(iv)* afetação do comércio entre os Estados-Membros. Sem querer entrar em grandes detalhes, importa somente salientar que o primeiro passo para aferir se há, ou não, uma posição dominante é descobrir o mercado relevante, devendo haver um mercado relevante de produto e geográfico. *Vide* PAIS, Sofia – *Entre Inovação e Concorrência Em Defesa de um Modelo Europeu,* UCP Editora, 2011, pp. 453--456. Ademais, mesmo que seja possível identificar o mercado relevante, e sendo certo que há vários indícios que poderão indicar uma posição dominante (definido no caso do TJ, United Brands, C-27/76, 14 de fevereiro de 1978, par. 65) colocar-se-á uma dificuldade adicional de saber que tipo de abuso está em causa, tal como teremos a oportunidade de a breve trecho analisar.

[42] Como assinala RAMOS, Mariana Pinto – "O Consentimento do titular dos dados no contexto da Internet", *in Revista da Faculdade de Direito da Universidade de Lisboa,* Ano LXIII, n.º 1-2, 2022, pp. 663-727(678), "com o RGPD deixou de se partir do consentimento como principal fundamento de licitude num elenco mais abrangente de fundamentação de licitude."

[43] BARBOSA, Mafalda Miranda – *cit.,* p. 28.

frágil, já que, abstratamente, a qualquer momento ele pode ser revogado.[44]

Em primeiro lugar, tem de haver uma manifestação de vontade. A.M. CORDEIRO postula que com isto o legislador conduziu o conceito "ao universo dos negócios jurídicos"[45], comportando dois elementos distintos: *(i)* vontade humana e *(ii)* exteriorização dessa vontade.[46] Deveremos, por isso, encontrar uma manifestação por parte do titular dos dados no sentido de dar o seu consentimento. Como é salientado pelo Grupo de Trabalho ao Artigo 29 (doravante, GT29), no contexto digital, o facto de se receber vários pedidos pode promover um certo aborrecimento nos utilizadores, daí que esta situação possa "resultar num certo cansaço em relação aos cliques."[47] A manifestação de vontade acabará sempre por existir.

Além disso, o consentimento terá de ser *livre,* o que implica "uma verdadeira escolha e controlo para os titulares dos dados."[48] Neste sentido, há que analisar diferentes elementos. Desde logo, o considerando 43 consagra que este não será dado livremente quando exista um desequilíbrio manifesto entre os titulares dos dados e o responsável pelo tratamento, não sendo isto exclusivo das autoridades públicas ou das relações laborais.[49] Esta circunstância, embora não exclua a liberdade do consentimento, é um fator que poderá indiciar a maior probabilidade da sua ausência.[50]

---

[44] KELLEHER, Denis e MURRAY, Karen – *EU Data Protection Law,* Bloomsburry Professional, 2018, p. 155. Para uma análise detalhada da revogação do consentimento no contexto da internet, *vide* RAMOS, Mariana Pinto, *cit.,* pp. 695-699.

[45] CORDEIRO, A. M. – *O Direito… cit.,* p. 172.

[46] *Ibid,* p. 173. Ainda CORDEIRO, A. M – "Artigo 4.º Definições", *in* A.M. Cordeiro (Coord.) *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019,* Almedina, 2021, pp. 77-100(90-91).

[47] GT'29, Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679, Versão 1.1, 4 de maio de 2020, p. 22, disponível em <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pt.pdf>. consultado em 29.01.2023.

[48] *Ibid,* p. 8.

[49] *Ibid,* p. 11.

[50] POLLICINO, Orest, BASSINI, Marco e GREGORIO, Giovanni de – *Internet Law… cit,* p. 201. Será, por isso, mais difícil de se verificar, mas não impossível. BYGRAVE, Lee e TOSONI, Luca – "Article 4(11). Consent" *in* KUNER, Christopher, BYGRAVE, Lee e DOCKSEY, Christopher (Ed.) *The EU General Data Protection Regulation (GDPR) A commentary,* Oxford, 1.ª Edição, 2020, pp. 175-187(182).

A este propósito, há quem defenda que o poder de mercado deve ser um fator a ter em consideração para determinar este desequilíbrio, sendo que as empresas que detenham um poder dominante no mercado digital terão poucas possibilidades de usar o consentimento como fundamento de licitude para o tratamento dos dados pessoais.[51]

In casu, não deixa de ser interessante que o Advogado-Geral, em resposta às questões prejudiciais no Caso Meta Platforms, tenha considerado que, para tal situação ser relevante do ponto de vista do RPGD, não tem de existir uma equiparação ao limiar de posição dominante. Além disso, considerou que existindo uma posição dominante, embora tal seja um indício a ter em consideração, isso não poderá privar o consentimento dos utilizadores de validade.[52] Procurou-se, assim, criar uma posição de equilíbrio. Resta saber se o TJ partilhará a mesma opinião.

O ponto mais problemático prende-se com o disposto no n.º 4 do art. 7.º do RGPD, o qual visa assegurar que "a finalidade do tratamento dos dados pessoais não está camuflada nem agregada à execução de um contrato ou prestação do serviço para os quais esses dados pessoais não são necessários."[53] A existência desta condicionalidade foi um dos motivos que levou o *Bundeskartellamt* a advogar que não poderia existir um consentimento livre, pois este não só funciona como um pré-requisito para a utilização da rede social[54], como o que os termos e condições pedem vai muito mais além daquilo que é necessário. Por essas razões,

---

[51] GRAEF, Inge e VAN BERLO, Sean – "Towards Smarter Regulation in the Areas of Competition, Data Protection and Consumer Law: Why Greater Power Should come with Greater Responsibility", *in European Journal Of Risk Regulation,* 12, 2021, pp. 674-698(684), disponível em <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/towards-smarter-regulation-in-the-areas-of-competition-data-protection-and-consumer-law--why-greater-power-should-come-with-greater-responsibility/8B00EFC66EA7F599DB9B700B1720ABAD> consultado em 30.01.2023.

[52] Opinião do Advogado-Geral, Meta Plataforms*,* C-252/21, parágrafos 75-77.

[53] GT29, Diretrizes 05/2020*... cit.,* p. 11.

[54] Nesta medida, os dados pessoais funcionarão como uma verdadeira contraprestação. *Vide* HELBERG, N., ZUIDERVEEN, F e REYNA, A. – "The Perfect Match? A closer look at the relationship between EU consumer law and data protection law", *in Common Market Law Review,* LIV-5, pp. 1427-1465. Disponível em <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3048844>, consultado em 29 de janeiro de 2023.

no contexto digital promove-se o *unwitting consent*[55], pois, estando vinculados a dar o seu consentimento para a utilização da plataforma, os utilizadores simplesmente aceitam o que lhes é pedido. Conforme referido, este foi um dos motivos que levou a Autoridade da Concorrência Alemã a concluir pela violação do RGPD. Ainda assim, e como bem assinala VIKTORIA ROBERTSON, o primordial, sob o ponto de vista do direito da concorrência, é que o Facebook imponha termos de serviço que lhe permita recolher montantes excessivos de dados pessoais.[56]

Por outro lado, o consentimento terá de ser *específico,* isto é, os dados pessoais devem ser recolhidos para finalidades determinadas, o que se destina "a assegurar um certo grau de controlo do utilizador e transparência em relação ao titular dos dados"[57] (al. b) do n.º 1 do art. 5.º do RGPD). Não deixa de ser discutível que, no caso das grandes plataformas, os titulares dos dados saibam com clareza as finalidades para que serão utilizados os seus dados.

Finalmente, é necessário que este seja *informado.* Por conseguinte, determinadas informações deverão ser fornecidas, mormente: (i) a identidade do responsável pelo tratamento, (ii) a finalidade de cada uma das operações para as quais se dá o consentimento, (iii) o tipo de dados que são recolhidos e utilizados e (iv) o direito a retirar o consentimento.[58] No caso das diferentes plataformas digitais, os termos de utilização são confusos, demasiado extensos, o que implica que não haja um consentimento verdadeiramente informado, já que os termos de utilização são demasiado técnicos para que os utilizadores os consigam verdadeiramente entender.[59] Isto resulta numa situação de inevitável vulnerabilidade

[55] RICHARDS, Neil e HARTZOG, Woodrow – "The Patologies of Digital Consent", *in Washington University Law Review,* Volume 96, n. .º 6, 2019, 1461-1503(1479).

[56] ROBERTSON, Viktoria – "Excessive..." *cit,* p. 16.

[57] GT29, Diretrizes sobre o consentimento… *cit.,* p. 15.

[58] *Ibid,* p. 17.

[59] Como salientam RICHARDS, Neil e HARTZOG, Woodrow – "The pathologies…" *cit.,* 1480.

para todos aqueles que pretendem utilizar a rede social.[60]

4.2 O Cruzamento de Dados Pessoais com outros serviços

Uma das temáticas igualmente problemáticas prende-se com o facto de redes sociais como o Facebook recolherem os dados pessoais de forma quase ilimitada, procedendo ao seu cruzamento com dados provenientes de outros serviços, mormente o Whatsapp/Instagram (os quais integram o Grupo Meta), bem como outros sites da Internet. No caso do Facebook invoca-se que tal visa assegurar a personalização dos conteúdos, bem como a utilização ininterrupta dos produtos oferecidos. Ora, isto implica uma breve reflexão sobre o fundamento de licitude que pode ser invocado.

O Comité Europeu para a Proteção de Dados reconhece que a personalização do conteúdo pode ou não "ser considerada necessária para a execução do contrato com o utilizador do serviço"[61] (al. b) do n.º 1 do art. 6.º do RGPD). Para a aplicação deste fundamento de licitude é essencial que não "exista uma alternativa menos intrusiva da esfera privada do titular dos dados e haja uma ligação direta entre esse tratamento e a execução do contrato."[62] *In casu,* é discutível se existe ou não uma alternativa que seja menos intrusiva para os utilizadores. No Caso Meta Plataforms, o AG salientou que dificilmente um tratamento de dados pessoais provenientes de outros serviços poderá ser necessário para a utilização desta rede social.[63] Vemos, assim, que a execução do contrato

---

[60] Segundo BIONI, Ricardo – *Proteção de Dados Pessoais – A Função e os Limites do Consentimento,* Editoria Forense, 2019, p. 221, a sua "vulnerabilidade é maximizada por essa idiossincrasia traiçoeira do trade-off da economia informacional."

[61] CEDH, Diretrizes 2/2019 sobre o tratamento de dados pessoais ao abrigo do artigo 6.º, n.º 1, alínea b), do RGPD no contexto da prestação de serviços em linha aos titulares dos dados, Versão 2.0, 8 de outubro de 2019, p. 17 (par. 57), disponível em <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_pt.pdf> consultado em 31.01.2023.

[62] CORDEIRO, A. M. – "Artigo 6.º Licitude do Tratamento", *in* A. M. Cordeiro (Coord.) *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019,* pp. 107-120(113).

[63] Opinião AG, Caso Meta Platforms, parágrafos 56-57.

poderá não ser o fundamento mais adequado nestas situações.

Outra possibilidade passa pela invocação do interesse legítimo (previsto na al. f) do n.º 1 do art. 6.º do RGPD). Este implica o cumprimento do teste dos três passos[64]: *(i)* o interesse deverá ser legítimo[65], *(ii)* o tratamento deverá ser necessário e *(iii)* deve-se aferir se devem prevalecer os interesses ou direitos e liberdades fundamentais do titular.[66] O Facebook invoca como motivos a premência em promover a personalização da publicidade, a segurança da rede e o aperfeiçoamento do produto. Como salienta o AG, embora o marketing seja um dos fundamentos diretamente referidos no Considerando 47, não podemos deixar de ter em consideração que os dados provêm de fontes externas e, por isso, mesmo que se entenda ser necessário, será muito difícil afirmar que este interesse económico pode prevalecer sobre os interesses dos titulares dos dados.[67]

Sempre se poderá refletir sobre o facto de os interesses do Facebook serem suficientemente acautelados através do uso dos dados recolhidos na sua própria rede, sem os cruzar com os provenientes de entidades terceiras. Ainda assim, no Caso Meta-Platforms, o AG foi categórico ao considerar que, mesmo considerando-se que estas personalizações são realizadas no interesse do utilizador, parece que tal não é essencial para a utilização do serviço.[68]

---

[64] Information Commissioner's Office, *Legitimate interests – Lawful basis for processing,* p. 4., disponível em <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to--the-general-data-protection-regulation-gdpr/legitimate-interests-1-0.pdf>, p. 4.

[65] POLLICINO, Oreste, BASSINI, Marco e GREGORIO, Giovanni de – *cit.,* pp. 203-204 salientam que isto pressupõe "um interesse real e presente, algo que seja correspondente com as atividades correntes ou benefícios que poderão ser esperados no futuro próximo." (tradução nossa).

[66] CEPD, Diretrizes 8/2020 sobre o direcionamento para os utilizadores das redes sociais*,* Versão 2.0, adotada em 13 de abril de 2020, disponível em <https://edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_targeting_of_social_media_users_pt_0.pdf> consultado em 1.02.2023. *Vide*, igualmente, TJ, Fashion ID GmbH & Co. KG*,* C-40/17, 29 de julho de 2019, par. 95.

[67] Opinião do AG, C-252/21, parágrafo 64.

[68] Opinião do AG, C-252-21, parágrafos 64-66.

A este propósito, o GT29 já teve a oportunidade de demonstrar que, pese embora este fundamento de licitude possa ser usado para efeitos marketing, tal não significa que os responsáveis pelo tratamento podem "combinar uma vasta quantidade de dados pessoais de diferentes fontes que inicialmente foram recolhidas noutros contextos e para propósitos diferentes."[69] Esta problemática, conforme veremos, foi abordada no Regulamento dos Mercados Digitais.

4.3 O Direito à Portabilidade

O Direito à Portabilidade dos Dados Pessoais encontra-se previsto no art. 20.º do RPGD, permitindo-se ao titular dos dados "receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento" (n.º 1 do art. 20.º do RGPD). A sua consagração não esteve isenta de críticas[70], questionando-se a sua compatibilidade com direitos de propriedade intelectual[71], segredos de

---

[69] GT'29, Opinião 06/2014 sobre a noção de interesses legítimos do responsável pelo tratamento ao abrigo do artigo 7.º da Diretiva 95/46/EC, 9 de abril de 2014, pp. 25-26, disponível em <https://www.fia.org/sites/default/files/2019-11/Excerpts%20-%20Opinion%2006-2014%20on%20the%20notion%20of%20legitimate%20interests%20of%20the%20....pdf> consultado em 1.02.2023.

[70] FIDALGO, Vitor Palmela – "O Direito à Portabilidade dos Dados Pessoais", *in Revista de Direito e Tecnologia,* Vol. I-1, 2019, pp. 89-135(130-131) critica o direito à portabilidade por só parcialmente corresponder às expectativas, advogando que "diversas formas de tratamento lícitas de dados não são consideradas para a portabilidade", pelo que o art. 20.º "não reúne o mínimo de certeza e segurança para os interessados."

[71] *Vide* FIDALGO, Vitor Palmela – *cit.,* pp. 123-126, GEIREGAT, Simon – "Copyright Meets Consumer Data Portability Rights: Inevitable Friction between IP and the Remedies in the Digital Content Directive" *in GRUR International*, LXXI-6, 2022, pp. 495–515, disponível em <https://academic.oup.com/grurint/article/71/6/495/6576075> consultado em 1.02.2023 e GRAEF, Inge, HUSOVEC, Martin e PURTOVA, Nadezhda – "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law" *in German Law Journal,* Vol. XIX- 6, 2018, pp. 1359-1398, disponível em <https://www.cambridge.org/core/journals/german-law-journal/article/data-portability-and-data-control-lessons-for-an-emerging-concept-in-eu-law/5904FB88DDC1B9E6EC651A7F89058433>. Consultado em 01.02.2023. *Vide,* igualmente, VANBERG, Aysem Diker e ÜNVER, Mehmet – "The Right to data portability in the GDPR and EU Competition Law: odd couple or dynamic duo?" *in European Journal of Law and Technology,* Volume VIII-8, 2017, pp. 1-22(5), disponível em <https://www.ejlt.org/index.php/ejlt/article/view/546>. Consultado em 02.02.2023.

negócio, o respeito pelo "sistema de proteção de dados e o direito à autodeterminação dos dados" (72)(73) e, ainda, se tal consagração não originaria custos e esforços desproporcionais.[74] A sua possibilidade está dependente da verificação cumulativa de três requisitos, a saber: *(i)* fornecimento por parte do titular dos dados, *(ii)* que o tratamento se baseie no consentimento ou num contrato e que *(iii)* o tratamento seja realizado por meios automatizados.[75]

Este direito pode, como é evidente, apresentar a vantagem inegável de reduzir os custos associados a esta mudança, bem como diminuir os problemas de *lock-in*.[76] Todavia, existe a desvantagem de, em caso de empresas que detenham uma posição dominante, tal recusa ser suscetível de criar barreiras à entrada, o que será ainda mais evidente nas plataformas digitais. Não podemos ignorar que o modelo de negócio depende em grande medida dos dados pessoais dos seus utilizadores, daí que possa existir uma tendência para que as grandes plataformas guardem as bases de dados somente para si.[77] Tal pode ser observado numa "análise comparativa *ex post* das plataformas digitais pertencentes ao mesmo nicho de mercado"[78], podendo, em caso de recusa, haver lugar a um abuso de posição dominante.[79]

---

[72] FIDALGO, Vítor Palmela – "Artigo 20.º Direito de portabilidade dos dados", *in* A. M. Cordeiro (Coord.) *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019,* Almedina, 2021, pp. 204-213(206).

[73] *Ibid,* p. 207.

[74] VANBERG, Aysem e ÜNVER, Mehmet – *cit.,* p. 4.

[75] *Vide* GT'29 – Guidelines do direito à portabilidade, adotado em 13 de dezembro de 2016, disponível em <https://ec.europa.eu/newsroom/article29/items/611233/en> consultado em 1.02.2023.

[76] KERBER, Wolfgang e ZOLNA, Karsten – "The German Facebook Case: The Law and economics of the relationship between competition and data protection law", *in European Journal of Law and Economics,* 54, 2022, pp. 217-250(227).

[77] GRAEF, Inge – "Market Definition and Market Power in Data: The Case of Online Platforms", *in World Competition,* XXXVIII-4, 2015, pp. 473-506(479).

[78] SOUTO, Gabriel, LEMOS, Amanda e PINHEIRO, Guilherme – "O Direito à Portabilidade de Dados Pessoais e as Consequências de sua (não) implementação para o direito concorrencial", *In Revista Direito Público,* Vol. XVII-95, 2017, pp. 230-247(240), disponível em <https://blook.pt/publications/publication/111bc9bfd1a6/> consultado em 02.02.2023.

[79] VANBERG, Aysem e ÜNVER, Mehmet – *cit.,* p. 6.

De todo o modo, e como salienta a doutrina[80], existe uma diferença entre os regimes em confronto: ao passo que o RGPD exige que se verifiquem os requisitos elencados no Art. 20.º do RGPD, o campo de aplicação do art. 102.º do TFUE acaba por ser mais amplo. Nessa medida, e como salienta INGE GRAEF[81], mesmo que a recusa de portabilidade não se refira a dados pessoais de pessoas identificadas ou identificáveis, ainda assim tal poderá constituir um abuso de posição dominante, caso se verifiquem os restantes requisitos, sendo muito relevante que tal conduta seja suscetível de ter um impacto na concorrência.[82]

Recentemente, a Autoridade da Concorrência Italiana iniciou uma investigação contra a Google, pela possibilidade de ter incorrido num abuso de posição dominante. O fundamento residiu justamente no facto de a Google ter desrespeitado o direito à portabilidade dos dados, tendo recusado partilhá-los, em particular, com a Weopple APP (dirigida pela Honda). No comunicado de imprensa publicado[83], salienta-se que esta conduta não só viola o disposto no art. 20.º do RGPD, como é suscetível de ter um efeito prejudicial nos consumidores (abuso de exploração) e, ainda, é suscetível de restringir a concorrência (abuso de exclusão).

Convém, no entanto, ter em consideração aquilo que alguma

---

[80] ENGELS, Barbara – "Data Portability among online platforms" *in Internet Policy Review – Journal on Internet Regulation,* Volume V-2, 2016, pp. 1-17, disponível em <https://policyreview.info/articles/analysis/data-portability-among-online-platforms> Consultado em 02/02/2023. Igualmente GRAEF, Inge, HUSOVEC, Martin e PURTOVA, Nadezhda – *cit.,* pp. 1387-1388.

[81] GRAEF, Inge – "Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union", *in Telecommunications Policy,* Volume XXXIX-6, pp. 502-514, disponível em <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2296906> consultado em 03/fev/2023.

[82] KEMP, Katharine – "Concealed data practices and competition law: why privacy matters", *in European Competition Journal,* Vol. XVI-2/3, 2020, pp. 628-672(671), disponível em <https://www.tandfonline.com/doi/full/10.1080/17441056.2020.1839228>. Consultado em 02/02/2023. A autora realça que, sendo o objetivo do direito à portabilidade reforçar a situação dos consumidores, tal deverá ser assegurado através de mecanismos de controlo, transparência, assegurando-se, pois, que o titular dos dados é verdadeiramente soberano nessas situações.

[83] A552 – Italian Competition Authority, investigation opened against Google for abuse of dominant position in data portability, 14 de julho de 2022, disponível em <https://en.agcm.it/en/media/press-releases/2022/7/A552> Consultado em 2.02.2023.

doutrina realça: nestas grandes plataformas digitais, para a concorrência poderá ser mais útil a interoperabilidade do que a portabilidade.[84] Tal poderá ser mais crítico nas redes sociais, sendo que em caso de não funcionamento, os utilizadores ficarão inevitavelmente sujeitos a ela, não mudando mesmo que o serviço fornecido por outra seja mais atraente.[85] Ainda assim, convém ter em atenção aquilo que BARBARA ENGELS assinala: a portabilidade dos dados deve ser assegurada quando melhore a concorrência e incentive a inovação, promovendo-se um equilíbrio necessário.[86]

5. Soluções do Direito da Concorrência por violação do Direito da Proteção de Dados

A decisão da Autoridade da Concorrência Alemã gerou querelas intermináveis, não existindo consenso quanto à forma como devem estas plataformas digitais ser responsabilizadas por violação de questões relacionadas com o direito da proteção de dados. Mesmo concluindo-se que as Autoridades da Concorrência podem, embora a título incidental, aplicar o RGPD, não fica claro o tratamento a dar. Todavia, e como assinala SOFIA PAIS, "a complexidade e a novidade destas questões no plano da concorrência aconselham alguma prudência nas soluções e remédios avançados."[87] Vejamos.

5.1 Abuso de Posição Dominante

A primeira solução passará por concluir pela existência de um abuso de posição dominante (art. 102.º do TFUE). Parece ter sido essa

[84] PAIS, Sofia – "*Legal Challenges" ... cit.,* p. 24.

[85] GRAEF, Inger – "Mandanting Portability… *cit,* p. 8.

[86] ENGELS, Barbara – cit., p. 5-6.

[87] PAIS, Sofia – "Considerações de Lealdade e Equidade no Direito da Concorrência da União – Breves Reflexões", *in Revista de Concorrência e Regulação,* Ano IX, N.º 35, 2018, 123-148(142).

a solução apresentada pela Autoridade da Concorrência alemã, mas vários problemas podem emergir contra esta solução. Desde logo, a primeira dificuldade passará por definir o mercado relevante. Este é um primeiro passo essencial para que se possa avaliar se determinada empresa[88] detém ou não uma posição dominante nesse mercado. Para o efeito, devemos determinar o mercado de produto relevante, o qual "compreende todos os produtos e/o serviços considerados permutáveis ou substituíveis pelo consumidor devido às suas características, preços e utilização pretendida."[89] Adicionalmente, deverá definido o mercado geográfico relevante, o qual compreende toda a "área em que as empresas em causa fornecem produtos ou serviços, em que as condições da concorrência são suficientemente homogéneas e que podem distinguir-se de áreas geográficas vizinhas devido ao facto da concorrência ser consideravelmente diferente nessas áreas."[90]

Ora, em muitas destas situações, estamos diante um *zero price market*[91]*,* nos termos do qual não é possível encontrar uma transação financeira direta entre quem presta o serviço e que o utiliza[92]: na maioria destes casos, somente são fornecidos os dados pessoais, começando o utilizador de imediato a utilizar a rede social. Conforme salienta INGE GRAEF, nestes casos é difícil identificar um mercado relevante, já que os dados pessoais fornecidos funcionam como um mero *input of*

[88] Adota-se um conceito amplo, já que de acordo com a jurisprudência do TJ, Höfner e Fritz Elser contra Macrotron GmbH*.,* C-41/90, 23 de abril de 1991, par. 21, empresa "abrange qualquer entidade que exerça uma atividade económica, independentemente do seu estatuto jurídico e modo de funcionamento."

[89] Comunicação da Comissão relativa à definição de mercado relevante para efeitos do direito comunitário da concorrência (97/C 372/03), 9 de dezembro de 1997, par. 7.

[90] *Ibid,* par. 8.

[91] Pese embora a realidade tenha vindo a mudar, passando as redes sociais a criar as suas versões "premium", mediante o qual os utilizadores pagam determinada quantia monetária por uma versão melhorada da aplicação.

[92] PATAKYOVÁ, Maria T. – "Competition Law in Digital Era – How to Define the Relevant Market?" *in in 4th International Scientific Conference – EMAN 2020 – Economics and Management: How to Cope with Disrupted Times,* 2020, pp. 171-177(172), disponível em <https://eman-conference.org/eman-2020-171/>. Consultado em 03.02.2023.

production[93], não sendo possível identificar uma transação propriamente dita. Ademais, o autor não deixa de realçar que, ao criarem as suas contas nestas plataformas, os utilizadores não conseguem, *a priori,* controlar o tipo de informações que serão verdadeiramente recolhidas (conforme tivemos já a oportunidade de desenvolver), pelo que estas plataformas exercem um poder quase soberano no momento da sua recolha. Trata-se, pois, de uma *take-it-or-leave-it offer*.[94] Mesmo o teste SSNIP (isto é, saber se o consumidor, face a um aumento de entre 5% a 10% mudará de serviço) é de aplicação difícil, já que verdadeiramente na maioria dos casos não existe o pagamento de uma quantia monetária. Existem, por isso, vários obstáculos a encontrar o mercado relevante, o qual configura um passo essencial, já que é através dele que pode ser "apreciado o poder económico da empresa, sendo fundamental para identificar as posições concorrenciais a que está sujeita."[95]

Mesmo que seja possível ultrapassar esta barreira inegável associada às plataformas digitais da definição do mercado relevante[96], ainda assim será difícil equacionar o tipo de abuso que está em causa. Sempre se poderia argumentar, por exemplo, que casos como o do Facebook evidenciariam a existência do abuso de preço excessivo. Todavia, e como consagrado na jurisprudência do TJ United Brands[97], tal pressupõe a verificação de dois requisitos: *(i)* existência de uma desproporção excessiva entre o custo suportado e o preço efetivamente praticado e *(ii)* que se tenha imposto um preço não equitativo, seja em si mesmo, seja em comparação com os produtos concorrentes. Mais uma vez, somos confrontados com algumas dificuldades.

---

[93] GRAEF, Inge – "Market Definition and Market Power in Data: The Case of Online Platforms" *in World Competition: Law and Economics,* Volume 38, n.º 4, 2015, pp. 473-506(491).

[94] *Ibid,* p. 490.

[95] PAIS, Sofia – *Entre Inovação… cit.,* p. 453.

[96] ROBERTSON, Viktoria – "Excessiva Data…" *cit.,* pp. 7-9, defende que uma das opções poderá passar por se considerarem os mercados potenciais, considerando-se os dados pessoais como seus próprios (potenciais), mesmo quando tal não seja negociado dessa forma.

[mercado,] mesmo quando não é (atualmente) negociado como ta

[97] TJ, United Brands*,* C-27/76, 14 de fevereiro de 1978, parágrafo 252.

Em primeira linha, e tal como já assinalado a propósito da definição de mercado relevante, também aqui se coloca o problema de os dados pessoais serem usados continuamente: isto é, ao contrário das prestações pecuniárias propriamente ditas, não se esgotam numa única utilização[98], apontando-se, igualmente, que nestas situações os utilizadores não têm verdadeira noção de que aquilo constituirá um pagamento – o que não se sucede quando existe transação pecuniária envolvida. Ademais, a doutrina não deixa de apontar que tal poderá levar a que valores como a privacidade e a moralidade deixem de ser tidos em consideração quando refletimos sobre os impactos do tratamento dos dados pessoais, especialmente num contexto de internet.[99] Mais uma vez, mesmo que se conseguisse verificar o primeiro pressuposto, seria sempre difícil preencher o segundo, já que, como assinala VIKTORIA ROBERTSON, pressupõe-se um juízo de valor, devendo avaliar-se se tal seria excessivo do ponto de vista absoluto e relativo.[100] Ainda assim, e devido às dificuldades sentidas, acompanhamos a autora quando reconhece que, mesmo funcionando os dados pessoais como contraprestação, tal não quererá necessariamente dizer que eles tenham de ser equiparados a um preço excessivo.[101] Finalmente, há doutrina que reconhece que estas situações poderão ser inseridas na al. a), do art. 102.º do TFUE, isto é, condições de transações não equitativas. Tal pressuporia, pois, que os termos e condições fossem qualificados como verdadeiros termos contratuais.[102]

---

[98] BUDZINSKI, Oliver, GRUSEVAJA, Marina e NOSKOVA, Victoria – "The Economics of the German Investigation of Facebook's Data Collection" *in Market and Competition Law Review,* Volume 5, n. .º 1, 2021, pp. 43-80(64-65).

[99] ROBERTSON, Viktoria – "Excessive Data…" *cit.,* pp. 10-11.

[100] *Ibid,* p. 12.

[101] *Ibid,* p. 13.

[102] Para uma análise mais desenvolvida *vide* ROBERTSON, Viktoria – "Excessive Data…" *cit.,* 13-15.

5.2 Abuso de Dependência Económica

O Abuso de Dependência Económica é apontado como uma alternativa apta a regular este tipo de situações. Pressupõe-se, em primeira linha, que exista uma situação de dependência económica, a qual pode ser estabelecida entre duas empresas ou uma plataforma e os seus consumidores. Tal poderá, assim, ser definido como uma: "Situation of imbalance in bargaining power in the business relationship between two firms in which the larger and more powerful trading partner seeks to impose certain practices or contractual arrangements which are to their advantage in relation to a sales transaction*."*[103]

Note-se, todavia, que o conceito de dependência económica pode variar de país em país, dependendo da legislação adotada.[104] De qualquer forma, não se pressupõe a existência de uma posição dominante no mercado (e, nessa medida, algumas das dificuldades referidas anteriormente são mitigadas), pese embora, em determinadas situações, possa estar em causa o poder de mercado de um dos envolvidos.[105] O seu conceito poderá, como é salientado por alguns autores[106], ser mais flexível para sancionar condutas abusivas nos mercados digitais. Ademais, alguma doutrina tem considerado igualmente que os utilizadores se podem encontrar numa situação de *lock-in*, gerando-se um desequilíbrio acentuado entre eles e as plataformas e reforçando-se, nessa medida, a dependência existente.[107]

---

[103] PAIS, Sofia – "Big data and…" *cit.,* p. 38.

[104] Em Portugal, o art. 12.º da Lei n.º 19/2012 prevê três elementos para a verificação de abuso de dependência económica, mormente: (i) a exploração abusiva, (ii) por uma ou mais empresas, do estado de dependência económica em que se encontre relativamente a elas qualquer empresa fornecedora ou cliente, por não dispor de alternativa equivalente e (iii) que seja suscetível de afetar o funcionamento do mercado ou a estrutura da concorrência.

[105] PAIS, Sofia – "Big Data and…" *cit.,* p. 38. SCALZINI, Silvia – "Economic dependence in digital markets: EU remedies and tools" *in Market and Competition Law Review,* Volume V-1, pp. 81-103(86).

[106] SCALZINI, Silvia – "Economic dependence…" *cit.,* p. 86.

[107] PAIS, Sofia – "Big Data and…" *cit.,* p. 39 e SCALZINI, Silvia – "Economic dependence…" *cit.,* p. 86.

São apontadas duas grandes vantagens desta possibilidade: por um lado, tal pressupõe a adoção do teste das *reasonable/sufficient alternatives* e, por outro lado, diz respeito a uma relação bilateral, pelo que, conforme reiterado, pode contribuir para mitigar a dificuldade associada à definição de mercado relevante. [108]

Recentemente, o Parlamento Italiano aprovou uma reforma importante nesta matéria, dentro da qual é possível destacar o Art. 33.º da Lei n.º 118/2022[109], tendo sido introduzida uma presunção de dependência económica nas situações em que uma empresa use os serviços intermediários fornecidos por uma plataforma digital que tenha um papel essencial nos utilizadores finais ou fornecedores, também em termos de efeitos de rede ou disponibilidade de dados. Introduziu-se, além disso, uma lista de condutas que podem indiciar a dependência económica.

De qualquer forma, também este enquadramento está longe de ser unânime na doutrina.

5.3 O Regulamento dos Mercados Digitais

O Regulamento dos Mercados Digitais (doravante RMD)[110] visa assegurar uma concorrência leal nas diversas plataformas digitais, tratando-se de um mecanismo *ex ante*, ao contrário dos restantes analisados. Conforme dispõe o n.º1 do art. 1.º do RMD, este tem por finalidade "contribuir para o bom funcionamento do mercado interno mediante a previsão de regras harmonizadas que assegurem para todas as empresas a disputabilidade e equidade dos mercados no setor

[108] Como refere RINALDI, Alice – "Re-Imagining the Abuse of Economic Dependence in digital world", *in Lexxion – The Legal Publisher,* 9 de junho de 2020, disponível em <https://www.lexxion.eu/en/coreblogpost/re-imagining-the-abuse-of-economic-dependence-in-a-digital--world/> consultado em 8.02.2023.

[109] Lei n.º 118/2022, de 5 de agosto de 2022.

[110] Regulamento (UE) 2022/1925 do Parlamento Europeu e do Conselho, de 14 de setembro de 2022.

digital."[111] Note-se, todavia, que o regulamento é somente aplicável aos serviços essenciais de plataforma prestados ou propostos por *gatekeepers* (controladores de acesso).[112] O conjunto de obrigações que recaem sobre os gatekeepers não impedem, no entanto, as entidades competentes de agirem *ex post.* A este propósito, SOFIA PAIS considera que o RMD, embora possa ser visto como "uma política de concorrência, dificilmente será considerado direito da concorrência."[113]

Desde logo, prevê-se uma limitação quanto ao fundamento de licitude que os *gatekeepers* podem invocar para o tratamento dos dados pessoais. Mais importante é, todavia, a al. b), do n.º 2, do art. 5.º, o qual prevê uma proibição de combinar dados pessoais provenientes do serviço essencial da plataforma com dados provenientes de outros serviços prestados pelo *gatekeeper* ou por terceiros (a menos que tenha sido dado o consentimento pelo utilizador). Ora, sempre se poderá ver esta possibilidade como uma consequência do Caso da Autoridade da Concorrência Alemã.[114]

O Considerando 36 do regulamento evidencia que tal prática poderá constituir uma vantagem aos *gatekeepers*, através da acumulação de dados, criando-se barreiras à entrada. Ademais, o n.º 2 do art. 5.º prevê um conjunto de proibições também elas relevantes, mormente: (*i)* ligar utilizadores finais a outros serviços de controladores de acesso com o intuito de combinar dados pessoais, *(ii)* tratar, para fins de

---

[111] KONTOSAKU, Athena – "European Antitrust Enforcement in the Digital Era: How It Started, How It's Going, and the Risks Lying Ahead" *in The Antitrust Bulletin*, Volume 67, n. .º 4, 2022, pp. 522–535(526), evidencia que "DMA is expected to be used not only defensively but also offensively against "gatekeepers" by smaller competitors and aspiring future entrants."

[112] O n.º 1, do art. 3.º, elenca três requisitos: *(i)* que tenha um impacto significativo no mercado interno, *(ii)* preste um serviço essencial de plataforma que constitui uma porta de acesso importante para os utilizadores profissionais chegarem aos utilizadores finais; e *(iii)* beneficie de uma posição enraizada e duradoura nas suas operações ou se for previsível que possa vir a beneficiar de tal posição num futuro próximo.

[113] PAIS, Sofia – "A interação entre o regulamento dos mercados digitais e as regras de defesa da concorrência: breves reflexões", *in* Paulo Pinto de Albuquerque *et al* (Organização) *Estudos de Homenagem ao Professor Doutor Américo Taipa de Carvalho,* Universidade Católica Editora, 2022, pp. 415-434(433).

[114] KERBER, Wolfgang – "Taming Tech Giants: The Neglected Interplay Between Competition Law and Data Protection (Privacy) Law", *in* The Antitrust Bulletin, Vol. LXVII-2, 2022, pp. 280–301(291)

prestação de serviços de publicidade em linha, dados pessoais de utilizadores finais que utilizam serviços de terceiros que recorrem a serviços essenciais de plataforma do controlador de acesso e *(iii)* proibição de cruzamento de dados pessoais provenientes do serviço essencial de plataforma em causa com outros serviços prestados separadamente. Adicionalmente, o RMD evidencia a importância de ser tão fácil dar como retirar o consentimento (fundamento de licitude que levanta várias questões no âmbito das plataformas digitais, como vimos).

Por outro lado, prevê-se que os *gatekeepers* não poderão utilizar, em concorrência com os utilizadores profissionais, quaisquer dados não disponíveis publicamente que sejam gerados no contexto dos serviços essenciais da plataforma ou de outros serviços (n.º 2 do art. 6.º), o que poderá incluir qualquer tipo de dado gerado como "resultado das atividades comerciais dos utilizadores profissionais ou finais"[115], como por exemplo cliques ou pesquisas. Ademais, o RMD prevê uma obrigação de permitir a interoperabilidade, bem como de se assegurar a portabilidade dos dados.

Estas são apenas algumas das várias obrigações que recaem sobre os controladores de acesso. Estamos diante uma regulamentação *ex ante,* não se obviando a aplicação ulterior da Comissão Europeia. Ainda assim, dúvidas poderão surgir quanto ao conceito de *gatekeeper,* como também pode ser criticável o facto de o regulamento proibir determinadas condutas enquanto tal, sem necessidade de prova dos efeitos anticoncorrenciais, o que pode promover uma "abordagem rígida, impondo um "*one-size--fits-all*" a controladores de acesso com modelos de negócio consideravelmente diferentes."[116] Aliás, esta desconsideração dos

[115] Tradução nossa. COOPER, Dan *et. al.* – "The Digital Markets Act for Privacy Professionals", *in Covington*, 10 de outubro de 2022, disponível em <https://www.insideprivacy.com/european-union-2/the-digital-markets-act-for-privacy-professionals/>, consultado em 10.02.2023.

[116] DOS SANTOS, Miguel Máximo – "O Regulamento dos Mercados Digitais: críticas e potencial impacto negativo sobre as Pequenas e Médias Empresas (PMEs)", Sérvulo Advogados, disponível em <https://www.servulo.com/pt/investigacao-e-conhecimento/O-Regulamento-dos-Mercados-Digitais-criticas-e-potencial-impacto-negativo-sobre-as--Pequenas-e/8157/> consultado em 13.02.2023.

efeitos anticoncorrenciais produzidos no mercado é uma das razões que a doutrina aponta para o RMD não ser verdadeiramente direito da concorrência, já que "a própria Comissão Europeia reconhece o caráter diferente e complementar do regulamento."[117]

O incumprimento das obrigações previstas nos artigos 5.º, 6.º e 7.º do Regulamento poderá levar a comissão a aplicar ao controlador de acesso coimas de montante bastante elevado[118] (até 10% do volume de negócios total a nível mundial). Caso o *gatekeeper* cometa uma infração semelhante a outra que já tenha sido alvo de decisão de incumprimento nos 8 anos anteriores, poderá aí a Comissão aplicar uma coima cujo valor não deverá ser superior a 20% do seu volume de negócios total a nível mundial.[119]

6. Conclusão

Os avanços tecnológicos criaram novos desafios não só ao nível do direito da proteção de dados, como também no direito da concorrência. As principais plataformas digitais têm, ao longo dos últimos dos anos, reforçado a sua posição de primazia, adotando comportamentos que poderão ser prejudiciais não só para os utilizadores, como para novos concorrentes que pretendam entrar no mercado.

Neste sentido, numa sociedade onde os dados pessoais são vitais para a economia digital, a interligação entre ambas as áreas parece inevitável, sobretudo tendo em consideração a capacidade quase inesgotável das plataformas digitais para efetuar a recolha e o tratamento dos dados dos seus utilizadores, extravasando em muitas situações aquilo que seria estritamente essencial. Deste modo, fará sentido que uma Autoridade da Concorrência se baseie em disposições do RGPD, ainda que somente a título incidental, para justificar a existência de um comportamento

[117] PAIS, Sofia – "A Interação entre …" *cit.,* p. 432.
[118] N.º 1 do art. 30.º do Regulamento dos Mercados Digitais.
[119] N.º 2 do art. 30.º do Regulamento dos Mercados Digitais.

violador do direito da concorrência. Tal não deve, todavia, contribuir para que exista uma substituição das autoridades competentes em matéria de proteção de dados, observando-se, sempre, a cooperação necessária e nunca contrariando decisões existentes. Assim, os casos mais recentes demonstram a necessidade de existir uma visão global dos diversos problemas e não separada. Questões como o consentimento (que, na maioria das situações, não é verdadeiramente livre e esclarecido), o direito à portabilidade e o modo como os dados pessoais são utilizados, apresentam a maior relevância e evidenciam a alguns pontos de contacto entre ambas as áreas.

Sendo este um importante ponto de partida, não ignoramos que dificuldades poderão surgir quanto ao enquadramento a dar no direito da concorrência. Parece-nos que o abuso de posição dominante tem o entrave de ser muito difícil definir qual o mercado relevante nas plataformas digitais, bem como ser difícil referir o tipo de abuso que poderá estar em causa. O Abuso de dependência económica, também assente numa perspetiva *ex post,* não é isento de dúvidas.

No nosso entendimento, o RMD é o exemplo mais recente que evidencia os diversos pontos de contacto entre ambas as áreas e que poderá contribuir para os controladores de acesso assegurarem um ambiente digital competitivo – o que pressupõe, *ex ante um* respeito pelos vários princípios do RGPD. Todavia, não podemos deixar de ter em atenção que certa doutrina chama a atenção para o facto de este não ser um verdadeiro diploma de direito de concorrência, assumindo pelo contrário um caráter complementar. Restará, pois, aferir qual o resultado da sua aplicação e, sobretudo, a capacidade da Comissão para assegurar o desígnio que prometeu.

O futuro é incerto e, no mundo tecnológico, o tempo é tudo. Reconhecendo a importância de se promover uma visão conjunta entre ambas as áreas do direito, e nunca ignorando as suas diferenças primordiais, cremos ser da mais elementar importância dar uma resposta coerente e harmonizada aos diversos problemas. Estamos longe da mera utopia e, afinal, esta interligação poderá ser a nova realidade.

The European Health Data Space and the GDPR – A problem of Compatibility for the "Donation" of Health Data

Madalena Gomes Cruz[1]
Iakovina Kindylid[2]

Abstract: The technological gap within the European Union and of the EU Single Market is hindering its economic competitiveness. To address this issue, the European Commission, has launched various regulatory initiatives aiming to promote the availability and quality of data and fostering the development and use of new technologies, such as AI, as well as the healthcare services and research in the EU. The Commission's proposal for a European health data space is an important step towards facilitating the sharing and reutilization of health and health-related data. However, the need for guidance and harmonization with the EU data protection framework must be addressed to ensure the success of the European health data space.

Keywords: *common EU health data space; personal data protection; health data sharing; data reutilization.*

Resumo: O fosso tecnológico dentro da União Europeia e do Mercado Único da UE está a dificultar a sua competitividade económica. Para contrariar esta questão, a Comissão Europeia lançou iniciativas regulamentares para promover a disponibilidade e qualidade de dados e

[1] Madalena Gomes Cruz, Associate at Vieira de Almeida & Associados; LLM in Law and Technology, Tilburg University, mgc@vda.pt

[2] Iakovina Kindylidi; International Advisor at Vieira de Almeida & Associados; PhD Candidate at NOVA School of Law; LLM International Business Law, Tilburg University imk@vda.pt

fomentar o desenvolvimento e utilização de novas tecnologias, como os sistemas de IA, bem como os serviços de saúde e a investigação na UE. A proposta da Comissão para um espaço de dados de saúde é uma iniciativa importante para facilitar a partilha e reutilização destes dados. Contudo, a necessidade de orientação e harmonização com o quadro de proteção de dados da UE devem ser endereçados para garantir o sucesso do espaço de dados de saúde.

***Palavras-Chave**: espaço europeu comum de dados de saúde; proteção de dados; partilha de dados de saúde; reutilização de dados.*

1. The Symptoms and the Diagnosis (pun intended)

The economic competitiveness of the European Single Market is a struggle that has been fought for many years and possibly for the years to come, particularly in what regards to the technological market. The challenges to the EU in this field are manifold: (*i*) to improve the economic stability; (*ii*) to become more competitive; and (*iii*) to create more and better jobs in a sustainable way.[3]

As recognised by the European Commission,[4] the business and economic growth associated with digital transformation and technological development are already moving at a rapid pace in China and in the United States. Consequently, if the European Union wishes to join the *"grown-ups'" table* of the digital and technological world, it must

[3] MONCADA.PATERNÒ-CASTELLO, Pietro; GRASSANO, Nicola; "The EU vs US corporate R&D intensity gap: investigation key sectors and firms"; Industrial and Corporate Change; volume 31; 2022, pages 19 to 38. Available at: https://www.researchgate.net/publication/340138938_The_EU_vs_US_corporate_RD_intensity_gap_Investigating_key_sectors_and_firms.

[4] European Commission; Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "A European Data Strategy"; COM(2020) 66 final; 19 February 2020; page 3.

develop its own initiatives to foster the internal market and reduce EU technology gap.[5]

In this regard, the European institutions have been working on multiple actions to encourage and promote both the commercial value of European technology companies, as well as the use of digital tools and new business models across sectors.[6] Pivotal to this end, as recognized by the Commission,[7] is the upgrade of a data-agile economy, able to simultaneously encourage the availability of large quantities of data, while ensuring their quality, trustworthiness, and reliability.

As largely highlighted in research, data are the essential tool that fosters new technologies, as a *sine-qua-non* of artificial intelligence ("AI"), Internet of Things (IoT) or cloud edge computing.[8] Thus, data is a fundamental pre-requisite for the technology development and innovation. Additionally, it is also worth pointing out that data are a great investment, as they are non-exclusive (they can be used, simultaneously, by multiple entities, independently and for different purposes) and (at least in most cases, except if contractually agreed otherwise) non-rival goods, while also being easy and cheap to replicate.

As addressed by the European Commission,[9] there are large quantities of data generated within the EU which are not utilised, particularly

---

[5] AKANDE, Adeoluwa; CABRAL, Pedro; CASTELEYN, Sven; "Assessing the Gap between Technology and the Environmental Sustainability of European Cities"; Information Systems Frontiers; 2019; Available at: https://research.unl.pt/ws/portalfiles/portal/11905837/Akande_Cabral.pdf.

[6] In this regard, multiple legislative packages and industrial incentives have been announced, namely: the Competitive Digital Markets (within the European Digital SME Alliance), the Digital Europe organization; the Digital Services Act package (comprehending the Digital Services Act and the Digital Markets Act); the Cybersecurity Strategy (comprehending the NIS 2 Directive and the Cybersecurity Act); among many others.

[7] European Commission; Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "A European Data Strategy"; COM (2020) 66 final; 19 February 2020; page 6.

[8] For instance, CURRY, Edward; SCERRI, Simon; TUIKKA, Tuomo; *Data Spaces – Design, Deployment and Future Directions*, Springer, 2022.

[9] European Commission; Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "A European Data Strategy"; COM(2020) 66 final; 19 February 2020; page 7.

due to legal, operational, and commercial barriers. Such barriers are imposed either in the relation between public entities and businesses (government-to-business) or between businesses (business-to-business).

However, before immediately considering the ways that such barriers can be minimised or even taken down, the EU standards should be taken into consideration. The EU is inextricably linked with human rights protection, which concomitantly occupy a central position within the EU legal order.[10] The European Treaties declare "that the EU is founded on respect for human rights, they give binding effect to the Charter of Fundamental Rights and Freedoms (…)".[11] Consequently, any solution founded to break through the barriers identified to the data sharing initiatives and data-driven economy must take into consideration fundamental rights protection in particular, and unavoidably, the protection of personal data, established in Art. 8 of the Charter of Fundamental Rights of the European Union.

2. The Prescription

In order to overcome the shortcomings of the lack of competitiveness of the EU economy in what regards the development and use of new technologies, the European Commission has announced several legislative initiatives:[12] *(i)* the Data Governance Act[13] (approved on the 30th May 2022), which establishes, among other topics, the conditions for the re-use, within the Union, of certain categories of data held by public bodies (Art.

[10] CRAIG, Paul and BÚRCA, Gráinne de; *EU Law – texto, cases and materials;* 6th edition, Oxford University Press, 2015.

[11] *Ibidem.*

[12] European Commission; Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "A European Data Strategy"; COM(2020) 66 final; 19 February 2020.

[13] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). Available at: https://eur-lex.europa.eu/eli/reg/2022/868/oj.

1(1)(a)); [14] *(ii)* an Implementing Act on high-value data sets, under the Open Data Directive,[15,16] which establishes a list of sectorial high-value datasets held by public bodies as well as the arrangements needed for publishing and reusing such datasets; (*iii*) the Data Act[17] approved on the [27]th November 2023 and, at the time of writing, pending publication on the Official Journal of the European Union, aiming to foster data sharing with individuals and between businesses; (*iv*) the signature of a Memoranda of Understanding with Member States on cloud federation,[18] promoting secure and competitive and secure cloud offering; and lastly the (*v*) creation of an EU (self-) regulatory cloud rulebook, to establish common grounds and standards ruling the offer and use of cloud services throughout the Union, both by public and private entities.[19]

In addition to the initiatives listed above, the Commission has also proposed the creation of multiple sectorial Data Spaces,[20] as part of the Common European Data Spaces. Data Spaces in general can be defined as "an ecosystem of data models, datasets, ontologies, data sharing contracts, and specialized data management services together with soft competencies including governance, social interactions, and business

[14] Such categories are detailed in Art. 3(1) of the Data Governance Act and include data protected on grounds of commercial and statistical confidentiality; as well as data protected under intellectual property rights of third parties and as personal data.

[15] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L1024.

[16] The Proposal for the implementing act was presented on the 21December 2022. Available here: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12111-Open-data-availability-of-public-datasets_en.

[17] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN, presented on the 23rd February 2022.

[18] Signed by the 27 Member-States on the 15 October 2020. Available at: https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe.

[19] The EU Cloud Rulebook is not yet published, but more information about it is available at: https://digital-strategy.ec.europa.eu/en/library/cloud-and-edge-computing-different-way-using-it-brochure#Rule.

[20] European Commission; Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "A European Data Strategy"; COM(2020) 66 final; 19 February 2020.

processes."[21] or as "(…) an umbrella term to an ecosystem, benefiting data sharing technologies, a suitable regulative framework, and innovative new business aspects",[22] being mainly considered, in the EU, as infrastructures that will foster data sharing and data reutilisation, without compromising the applicable legal framework.

The Commission's Strategy[23] foresees nine European Data Spaces, each governed by each one sector-specific regulation: Health, Industrial, Agriculture, Finance, Mobility, Green Deal, Energy, Public Administration and Skills. These sectors were selected due to their strategic significance for the EU Single Market but also due to their specific legal, economic, and business characteristics, risks, and requirements.

The first[24] Proposal for a Common European Data Space is the one for the Common European Health Data Space ("EHDS").[25] It should be noted that the Financial Data Spaces proposal was also originally expected in 2022,[26] while the Financial Data Spaces already mentioned as one of the strategic objectives set out in the EU Digital Finance Strategy.[27]

---

[21] CURRY, Edward; SCERRI, Simon; TUIKKA, Tuomo; *Data Spaces – Design, Deployment and Future Directions*, Springer, 2022.

[22] *Ibidem.*

[23] European Commission; Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "A European Data Strategy"; COM(2020) 66 final; 19 February 2020.

[24] And at the time of writing, the only proposal published.

[25] Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:dbfd8974--cb79-11ec-b6f4-01aa75ed71a1.0001.02/DOC_1&format=PDF.

[26] European Commission; Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "A European Data Strategy"; COM(2020) 66 final; 19 February 2020.

[27] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU, COM(2020) 591 final. Nonetheless, it should be noted that the Report on Open Finance by the Expert Group on European Financial Data Spaces was published on 24 October 2022, available here https://finance.ec.europa.eu/publications/report-open--finance_en. Therefore, some development in this field are expected in the coming months.

2.1. The Formula of the EHDS

The EHDS is described as "essential for advances in preventing, detecting and curing diseases as well as for informed, evidence-based decisions to improve the accessibility, effectiveness and sustainability of the healthcare systems".[28] With an enhanced importance after the COVID-19 public health crisis, the EHDS intends to foster data access to individuals, researchers, policy makers and innovators. As referred in this Proposal, "EHDS will create a common space where natural persons can easily control their electronic health data. It will also make it possible for researchers, innovators and policy makers to use this electronic health data in a trusted and secure way that preserves privacy".[29]

The main objectives of the EHDS, besides the ones already mentioned, are to: (*i*) contribute to a single market for digital health products and services; (*ii*) support a harmonised and common EU approach to use of electronic health data, increasing the free movement of natural persons and promote the EU a global standard in digital health; (*iii*) encourage the exchange and access to different types of electronic health data (as health records and genomics data); and (*iv*) establish mechanisms for data altruism in the sector.[30]

To achieve these goals, the Proposal for the EHDS presents nine chapters, establishing rules, common standards, practices, infrastructures, and a governance framework, both for the primary use and the reuse of "*electronic health data*".

In the first chapter, the scope and subject matter are presented, as well as the definitions. In this regard, the broad concept of *"personal electronic health data"* must be highlighted, as it includes: "(…) personal data related to the physical or mental health of a natural person, including the provision of health care services, which

[28] Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:dbfd8974--cb79-11ec-b6f4-01aa75ed71a1.0001.02/DOC_1&format=PDF.

[29] *Ibidem*.

[30] *Ibidem.*

reveal information about their health status, personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question, as well as data determinants of health, such as behaviour, environmental, physical influences, medical care, social or educational factors (…) The electronic health data concern all categories of those data, irrespective to the fact that such data is provided by the data subject or other natural or legal persons, such as health professionals, or is processed in relation to a natural person's health or well-being and should also include inferred and derived data, such as diagnostics, tests and medical examinations, as well as data observed and recorded by automatic means."[31]. All these categories of data (among others) can be processed either for (*i*) primary use – the provision of healthcare services[32] – or for (*ii*) secondary use – the purposes foreseen in Art. 34 of the Proposal.

In more detail, the primary use can be considered as the process of data to support or provide direct healthcare to the data subject, while the secondary use (or reuse) will consist of the processing of personal or non-personal data, as part of aggregated datasets or not, for research, innovation, policy making, regulatory activities or other purposes.[33]

The following chapter sets out several obligations for healthcare professionals in relation to the electronic health data. In detail, professionals are obliged to: (*i*) have access to the electronic health data of the

[31] Recital 5 of the Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:dbfd8974-cb79-11ec-b6f4-01aa75ed71a1.0001.02/DOC_1&format=PDF.

[32] Art. 2(2)(d) of the Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:dbfd8974-cb79-11ec-b6f4-01aa75ed71a1.0001.02/DOC_1&format=PDF.

[33] MARCUS, J Scott; MARTENS, Bertin; CARUGATI, Christophe; BUCHER, Anne; GODLOVITCH, Ilsa; "The European Health Data Space – Study requested by the ITRE Committee", 2022. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740054/IPOL_STU(2022)740054_EN.pdf.

patient, independent of the Member State; and (*ii*) ensure the update of the information in relation to their patients.

Furthermore, this second chapter also focus on the rights of data subjects, broadening the scope of the right to data portability, foreseen in Art. 20 of the General Data Protection Regulation ("GDPR").[34] Data portability under the GDPR consists of the right of the data subject to receive the personal data provided to the controller, as long as the processing is based on the data subject's consent or needed for the performance of a contract or for pre-contractual diligence, and only if the processing is carried out by automated means.[35] As it can be understood, the data portability right is subject to strong legal requirements under the GDPR, which are considerably reduced by the Proposal for the EHDS.

As referred in Recital 11 of the Proposal, portability under the EHDS lowers the obstacles regarding:[36] (*i*) the legal ground for processing that allows a portability request. In this case for instance, the processing can occur on the basis of compliance with a legal obligation; (*ii*) the categories of data that can be requested as to cover not only personal data directed provided to the controller by the data subject, but also inferred and indirect data; and (*iii*) the obligations of interoperability. Under the GDPR, controllers shall transmit the data when technically feasible, while under the EHDS Proposal, such technical feasibility is mandatory.

Under Art. 3(1) and 3(2) of the Proposal, all natural persons shall have the right to access and to receive an electronic copy of the electronic health data processed for primary use (the technical specifications

[34] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[35] Art. 20 of GDPR.

[36] MARCUS, J Scott; MARTENS, Bertin; CARUGATI, Christophe; BUCHER, Anne; GODLOVITCH, Ilsa; "The European Health Data Space – Study requested by the ITRE Committee", 2022. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740054/IPOL_STU(2022)740054_EN.pdf.

of the format of transmission is still to be determined by the Commission).[37] Furthermore, data subjects can also request the transmission of such data to a recipient of their choice, from the health or social security sector, "immediately, free of charge and without hindrance".[38]

Moreover, the chapter also foresees the creation of a digital health authority, which is entrusted, amongst others, with the implementation of the rights and obligations provided in the Proposal.[39] Interestingly, data subjects will also be entitled to complain to such authority, which then it shall be able to communicate with the relevant national data protection authority, if necessary, when the matter in discussion regards the protection of personal data.

Lastly, the second chapter addresses the creation of the cross-border infrastructure – MyHealth@EU – that will facilitate the exchange of the electronic health data between contact points that are nationally defined.[40] For this purpose, the Proposal establishes that in what regards this structure, the national contact points are to be qualified as joint controllers (meaning both will define together the purposes and essential means for the personal data processing), and the Commission shall be qualified as a processor (processing the personal data on the behalf of the national contact points).

Moving on to chapter three, its provision outline an essential framework for the success of the EHDS, establishing the desired interoperability and security requirements applicable to the electronic health

[37] Art. 6(1) of the Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:dbfd8974-cb79-11ec-b6f4-01aa75ed71a1.0001.02/DOC_1&format=PDF.

[38] Art. 3(8) of the Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:dbfd8974-cb79-11ec-b6f4-01aa75ed71a1.0001.02/DOC_1&format=PDF.

[39] Art. 10 of the Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:dbfd8974-cb79-11ec-b6f4-01aa75ed71a1.0001.02/DOC_1&format=PDF.

[40] Art. 12 of the Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:dbfd8974-cb79-11ec-b6f4-01aa75ed71a1.0001.02/DOC_1&format=PDF.

records systems ("EHR Systems"). Only through such requirements it is possible to ensure the efficient data sharing amongst the different systems. In this regard, the subjective scope of the chapter is mostly directed to the providers of such systems instead of the health professionals that were targeted in the previous subdivision. The Proposal's framework is mostly based on self-certification and compliance obligations for the manufacturers of EHR Systems, entrusting the oversight to the newly created market surveillance authorities, which will have the powers to oblige a certain provider to bring a system into conformity with the applicable requirements. These authorities will also be responsible for red flagging any EHR Systems which present a risk to the health or safety of natural persons or to the public interest. In addition, this chapter also provides a framework for wellness applications – which is defined as an "(…) appliance or software intended by the manufacturer to be used by a natural person for processing electronic health data for other purposes than healthcare, such as well-being and pursuing healthy life-styles" – that wish to be interoperable with the EHR Systems, regulating the use of a label for that end, issued by the manufacturer of the application. Both the EHR Systems and the wellness apps are subject to registration in the EU database.[41]

As for the fourth chapter, it is dedicated to the secondary use of electronic health data, establishing the minimum categories of data that can be reused, as well as permitted and prohibited purposes of such reutilisation. Furthermore, the chapter also provides a governance model for the secondary use, creating a health data access body which is responsible for granting the access to the data recipient entities, subject to a fee. However, these bodies are also subject to transparency measures towards data subjects, as they shall make publicly available, amongst other information, the legal basis for granting access, the security measures put in place to protect the data and the rights of the data

[41] Art. 32(2) of the Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:dbfd8974-cb79-11ec-b6f4-01aa75ed71a1.0001.02/DOC_1&format=PDF.

subjects. However, and surprisingly, these bodies do not have to comply with Art. 14 of the GDPR, thus, they do not have to inform the data subjects regarding the personal data they are receiving and sharing, as well as about the terms of the processing.

Naturally, the chapter establishes obligations towards the data holders and data recipients. In relation to the first, the obligations mainly focus on data quality and on ensuring the good faith of the *"data providers*". In relation to the latter, data recipients must prepare the application for access, including pointing out the legal grounds for processing, when needed. In this regard, also the secondary use occurring cross-borders, through the HealthData@EU infrastructure – created specifically for this purpose – and mediated by the national contact points is regulated.

In a nutshell, the process for the reuse of electronic health data will consist of:

(*i*) the entity offering healthcare services that is a holder of electronic health data will have the obligation to provide information regarding these data to the national entity acting as a health data access body;

(*ii*) the national entity will aggregate, compile and publicize a dataset catalogue that will describe the source and nature of the electronic health data, as well as the requirements of access;

(*iii*) any natural or legal person can submit an application to the national entity, requiring access to the dataset; and

(*iv*) if the conditions are fulfilled, the data permit shall be granted, in such terms that the national entity and the data user (the entity accessing the data) will be considered joint controllers, for the purposes of the GDPR.[42]

Chapter five plays a critical role in the current globalized world, as it establishes the rules governing the transfer of personal and

[42] TERZIS, Petros; "Compromises and Asymmetries in the European Health Data Space"; *European Journal of Health Law*; 29; 2022; page 1 to 19.

non-personal electronic health data to third countries. Although the transmission of personal data to third countries presents greater legal challenges due to heavy regulation in the GDPR, the transmission of non-personal data under the Proposal is also severely restricted. The primary concern is to ensure that non-personal data cannot be relinked to a specific individual, ensuring that any anonymization techniques employed are pre-approved by the Commission. Additionally, Member States are authorized to introduce further impediments to the transfer of personal data to third countries, as stipulated in Art. 9(4) of the GDPR.

The sixth chapter establishes the EHDS Board, an entity that shall facilitate the cooperation and exchange of information among Member States; while chapters seven[43], eight[44] and nine[45] deal with miscellaneous legal topics that notwithstanding their importance, are not that relevant for the present analysis.

Overall, the formula proposed by the Commission's for the EHDS is coherently structured, notwithstanding the challenges that are posed by the Data Spaces in general and to the one dedicated to the health sector in particular, resulting from the particular sensitive nature of health and health-related data.

3. The complications

As anticipated in the previous sections, the European Data Spaces face multiple challenges: technical (as the sharing design and the security of the infrastructure); business and organisational (as the dynamic

[43] This chapter concerns the delegation of powers to be conferred to the Commission, regarding specific matters that will be further regulated in the future.

[44] This chapter details that the rules on the penalties to be applied under the future Regulation are to be determined by Member States. Additionally, it also foresees an evaluation and review process, after 5 and 7 years of the entrance into force.

[45] Chapter ten details the deferred application, as not all the provisions of the Regulation would enter into force at the same time, in accordance with the Proposal.

ecosystem and skills and the trust in the information which is made available); as well as national and regional obstacles (based on local resistance to change and different workforce skills).[46] As highlighted by the European Economic and Social Committee: *"[The EESC]* calls on the Commission to clearly reflect on the pros and cons of the initiative to reduce the risks before moving forward. One must realise that there are too many challenges ahead when we talk about the Member States' health systems. There are different paces, different views about public and private health systems and citizens must realise that this proposal means investment and public policy choices*"*.[47]

Naturally, as it is possible to understand from the Proposal of the EHDS, the legal issues arising from such a disruptive initiative are multiple. More specifically, the compatibility between the obligations and rights arising from the Proposal and the legal regime applicable to data protection is particularly interesting, due to: (*i)* the strict obligations established under the GDPR for the processing of personal data; (*ii*) the conservative approach that multiple national data protection authorities have been following; and (*iii*) the fact that "electronic health data" will mostly consist, as it can be anticipated, of health and genetic data, which are special categories of personal data, that shall not be processed unless one of the (stringent) exceptions of Art. 9 of the GDPR apply. Thus, even though the Explanatory Memorandum of the Proposal claims that *"*Considering that a substantial amount of electronic data to be accessed in the EHDS are personal health data relating to natural persons in the EU, the proposal is designed in full compliance (…) with the GDPR (…)*"*, it is possible to highlight several pertinent inconsistencies and obstacles.

The first challenge is the one stemming from Art. 51 of the Proposal and is posed by the qualification of national body controlling the access

[46] CURRY, Edward; SCERRI, Simon; TUIKKA, Tuomo; *Data Spaces – Design Deployment and Future Directions*, Springer, 2022.

[47] European Economic and Social Committee; Opinion of the European Economic and Social Committee on the Communication from the Commission to the European Parliament and the Council – A European Health Data Space: harnessing the power of health data for people, patients and innovation; COM(2022) 196 final; 21 December 2022.

to health data and data users as joint controllers for secondary use. First of all, the qualification of the parties involved in a data processing activity should be determined considering the facts and the effective control over the decisions underlying the processing.[48] Even though one can also argue that such control can be inferred or directly established in legal provisions (as it would be the case), a relationship between joint controllers has multiple consequences which can hinder the goals of the EHDS. Firstly, joint controllers shall determine and agree on the terms that rule their relationship,[49] especially regarding the data subjects' rights and the provision of information under Art. 13 and Art. 14 of the GDPR. This document has not been drafted yet.[50] However, its scope cannot prejudice the data users' interests, an aspect that would prove particularly challenging, since one of the controllers is a public entity. Secondly, national authorities are not bound by the roles attributed to each joint controller under the referred agreement.[51] Concomitantly, there is a risk that different national data protection authorities may have different deliberations in this matter, undermining the harmonised approach and EU-wide data-agile objective of the EHDS. This risk may be further aggravated considering that specific measures in relation to the health and health-related data may be in place subject to sector--specific national laws as well as due to possible specific provisions included in the GDPR national implementation laws.[52] The fact that

[48] European Data Protection Board; Guidelines 07/2020 on the concepts of controller and processor in the GDPR; 2 September 2020; Available at: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf.

[49] Art. 25 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[50] Art. 51(2) of the Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:dbfd8974-cb79-11ec-b6f4-01aa75ed71a1.0001.02/DOC_1&format=PDF.

[51] European Data Protection Board; Guidelines 07/2020 on the concepts of controller and processor in the GDPR; 2 September 2020; Available at: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf.

[52] For instance, this is the case in Portugal were specific technical and organisational measures are posed in Art. 29 of Law 58/2019 of 8 August, and Law 12/2005 of 26 January, as amended.

each of the joint controllers is also liable for the activities of the other controller[53] may also present high risk to entities who could be potentially interested in reusing the data, especially due to the volume and sensitivity of the personal data processed in this context.

In light of the above, it is also relevant to highlight the lawful bases for processing of personal data that can be used under the EHDS Proposal, in particular for the secondary use. In accordance with Recital 37, a data user will request access to the electronic health data (when applying for a permit) based on Art. 6(1)(e) or Art. 6(1)(f) of the GDPR, thus, either considering that processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or that processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

In what regards the first lawful basis, it is doubtful if it is applicable to private entities that do not have public authority powers. In this regard, it should be noted that that it is the prevailing opinion that *"*Article 6(1)(e) deals with data protection in the context of the performance of intrinsically state or public functions *(...)"*[54], and as such it has an extremely reduced scope. Following the case law of the Court of Justice of the European Union, the processing has to be necessary in the sense that it should facilitate activities that are foreseen in the law, in the public interest.[55] Therefore, data users should rely mainly on Article 6(1)(f) GDPR for the processing of personal data in this context. This

[53] MILLARD, Christopher; KAMARINOU, Dimitra; "Article 26 – Joint Controllers"; *The EU Data Protection Regulation – A Commentary;* Oxford University Press; 2020; pages 582 to 588.

[54] KOTSCHY, Waltraut; "Article 6 – Lawfulness of Processing"; *The EU Data Protection Regulation – A Commentary;* Oxford University Press; 2020; pages 321 to 344.

[55] Court of Justice of the European Union, Case C-524/06, REFERENCE for a preliminary ruling under Article 234 EC from the Oberverwaltungsgericht für das Land Nordrhein-Westfalen (Germany), made by decision of 15 December 2006, received at the Court on 28 December 2006; Heinz Huber v Bundesrepublik Deutschland; 16 December 2008.

will pose many obstacles to the flexible and easy process that underlined the draft of the EHDS Proposal. More specifically, a balancing exercise that must be performed by the data controller before the beginning of the processing activity. Notwithstanding Recital 37 of the Proposal establishes that "If the lawful ground for processing by the user is Art. 6(1), point (f), of Regulation (EU) 2016/679, in this case it is this Regulation that provides the safeguards.". However, this statement does not appear sufficient in fulfilling the balancing obligation, since it does not provide any guidance regarding the obligation of carrying a balancing test. It should be noted that such test must be tailor-made to the processing activity evaluated and should be documented by the controller. In particular, the balancing test should take into account:[56] (*i*) an assessment of the legitimacy of the interest of the controller which in this case and considering the purpose limitation for reuse of the electronic health data[57] may be possible; (*ii*) an assessment on the impact of the processing activities for the data subjects which can be particularly difficult to establish for secondary use, especially considering the amount of personal data processed and the sensitivity of the health and health-related data which is required; (*iii*) a provisional balance; and (*iv*) additional safeguards applied to mitigate the impact for data subjects. Therefore, such exercise may create an additional compliance obstacle to the secondary use provided in the EDHS Proposal.

The second problem posed with using Art. 6(1)(f) as a lawful basis for the processing related to the right to object, established in Art. 21 GDPR (which applies when the legal ground for processing is either line (e) or (f) of Art. 6). The data subjects must be able to object to the processing activity that may only continue if the data controller is able

[56] Article 29 Data Protection Working Party; Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC; 9 April 2014. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

[57] As detailed before, the EHDS Proposal determines the purposes that can be pursued by electronic health data reutilisation, under Art. 34(1).

to demonstrate compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject or for the establishment, exercise, or defence of legal claims. However, the data subjects will not be informed by the data access body of the processing activity under Art. 38(2) of the Proposal (which exempts these entities of the obligation to inform) and the data user may not be able to provide the required information (which would also be exempt under Art. 14(5)(b) GDPR). This means that the data subjects may lose power over their personal data, in such way that is inconsistent with the GDPR.[58]

Furthermore, besides the legal ground for processing, there is also a challenge in the restrictions established in Art. 9 GDPR. In accordance with this Article, special categories of personal data – as health data – shall not be processed, unless one of the conditions foreseen in Art. 9(2) GDPR applies. In this regard, the Proposal lists several exclusions that may be appropriate in the context of EDHS.[59] Firstly, Art. 9(2)(g) GDPR applies when processing is necessary for reasons of substantial public interest as long as it is based in law and that such law is proportionate for the specific purposes pursued while respecting the right to data protection and providing suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. To be able to use such exception for secondary use, the data user will be required to perform a balancing test, between the substantial public interest pursued and the risks for data subjects. Such analysis is not carried in the Proposal. Thus, it will be up to each data user to perform it.

The second exception listed is Art. 9(2)(h) allows processing of special categories of data, if necessary, for the purposes of preventive

[58] As noted by the European Data Protection Board and the European Data Protection Supervisor in their Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, 12 July 2022, available at https://edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202203_europeanhealthdataspace_en.pdf, in some topics the Proposal weakens the protection of the rights to privacy and data protection.

[59] Recital 37 of the Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:dbfd8974-cb79-11ec-b6f4-01aa75ed71a1.0001.02/DOC_1&format=PDF.

or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of law or pursuant to contract with a health professional. This exception will certainly be extremely useful for processing for the primary use of health data. However, this exception may not always be applicable for secondary use.

Furthermore, the third listed exception mentioned in Art. 9(2)(i) GDPR is probably the most useful for secondary uses. This exception allows the processing of health data, if necessary, for reasons of public interest in the area of public health, for instance to fight serious cross-border threats to health or to ensure high standards of quality and safety of health care and of medicinal products or devices on the basis of law, provided that such law offers suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy. Nonetheless, it is doubtful whether the Proposal is a sufficient basis to trigger the application of this exception, especially considering the strict interpretation of this Article and the lack of clarity of the Proposal to this effect.

Lastly, the fourth and last exception to be taken into consideration is Art. 9(2)(j), allowing processing, if necessary, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Art. 89(1) GDPR, based on law and provided that it is proportionate for the objectives pursued and as long as it provides for safeguards to the fundamental rights and the interests of the data subject, including data protection. Once again, the text of the Proposal will have to pass the strict test of the legal interpretation. Even if such test is successfully passed, this exception will serve innovators and researchers, however, it may be difficult to apply to commercial entities, in general.

Naturally, and even though the European Data Protection Board ("EDPB") and the European Data Protection Supervisory ("EDPS") have correctly stated that several of the permitted purposes for the

secondary use are included in one of the mentioned exceptions,[60] such exclusions must be interpreted objectively and narrowly. As such, additional difficulty and risks for data users arise. For instance, the use of secondary health data for training AI systems by commercial and profit-seeking entities[61] will be difficult to frame within the mentioned exceptions.

Furthermore, it should be noted that the Proposal does not oblige the data user to disclose to the national data access body what is the exception under Art. 9(2) of the GDPR it is relying on for the processing. Considering the sensitivity of the data reuse and following the same rationale that obliges the data user to disclose the legal ground of Art. 6 GDPR in the data permit application, the exception in which the data user is relying when requiring access to personal health data (or to other special categories of data) shall also be disclosed to and taken into consideration by the national data access body when deciding to grant, or not, the permit.[62]

Another important data protection topic impacted by the Proposal for the EHDS related to the data subjects' information rights. As established in Art. 38(2) of the Proposal, the national data access bodies are not obliged to provide the information foreseen in Art. 14(1) GDPR to data subjects in what regards the use of their data for projects subject to a data permit. This means that, in practice, data subjects will not be informed of the processing of their sensitive personal data, since data users will, most likely, rely on the exception foreseen in Art. 14(5)(b)

[60] European Data Protection Board and the European Data Protection Supervisor in their Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, 12 July 2022, available at https://edpb.europa.eu/system/files/202207/edpb_edps_jointopinion_202203_europeanhealthdataspace_en.pdf.

[61] As foreseen in Art. 34(1)(g) of the Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:dbfd8974-cb79-11ec-b6f4-01aa75ed71a1.0001.02/DOC_1&format=PDF.

[62] European Data Protection Board and the European Data Protection Supervisor in their Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, 12 July 2022, available at https://edpb.europa.eu/system/files/202207/edpb_edps_jointopinion_202203_europeanhealthdataspace_en.pdf.

GDPR, due to the absence of a method to inform these data subjects and because the process for notifying the data subject would be disproportionally difficult. As the EDPB and the EDPS have mentioned, this derogation undermines the powers of the data subjects.[63] Furthermore, it is not clear, and the Proposal does not address this matter, if such derogation is indeed necessary and proportionate for the purposes of the Proposal.

Finally, there are multiple challenges that will be posed at a national level, in particularly due to: (*i*) national laws and specific provisions applicable to the processing of health and health-related data; and (*ii*) the relationship between the national authorities and bodies involved in the EHDS. In what regards the first point, the GDPR specifically foresees, in Art. 9(4), that Member States are free to introduce additional conditions and restrictions to the processing of health data. Naturally, considering that there is some fragmentation already in this regard from a GDPR perspective, further tension is expected with Proposal for the EHDS.[64] Such fragmentation in implementation may also hinder the objectives of the cross-border infrastructures foreseen in the Proposal (as MyHealth@EU and HealthData@EU). In what regards the relationships among different national bodies and authorities, the Proposal foresees the creation of national digital health authorities, market surveillance authorities and health data access bodies, that will have to coexist with the national data protection authorities (among others that exist to regulate and supervise the health sector). The potential overlap of functions and inconsistencies amongst these entities and the possible tensions in their relationship with the various relevant stakeholders will be an additional challenge, aggravated by the possible fragmentation amongst the different Member States substantially hindering the objectives of the EHDS.

[63] *Ibidem.*
[64] *Ibidem.*

4. A Full Recovery?

The EHDS, as presented, has undoubtedly merit and may significantly contribute in boosting the competitiveness of the EU data-driven and technology economy, by addressing:[65] (*i*) the increased focus on public health, particularly due to the COVID-19 crisis; (*ii*) the desire to expand data subject's rights in the health sector, taking into account the limitations still applicable under the GDPR; (*iii*) the necessity of making a large volume of data available for commercial and non-commercial purposes, especially for AI training; and (*iv*) the fact that voluntary--based programs were insufficient to promote the data-agile economy in the sector.

Moreover, the EHDS represents the first attempt to establish a European framework for the secondary use of health data.[66] It imposes obligations on healthcare providers and EHR Systems to contribute and collaborate towards this goal, and as such significantly departing from other voluntary initiatives.[67]Despite the potential benefits and positive outcomes of the EHDS, the Proposal still presents legal challenges, as outlined above. One of the main obstacles in reusing electronic health data is establishing the legal basis for processing such data, particularly regarding the balancing test required when basing data processing on the controller's legitimate interests. Additionally, Art. 9 of the GDPR presents difficulties for processing activities that underpin each of the permitted purposes of secondary use. These issues, although not addressed currently in the Proposal, can still be addressed in its final text by including further details on the applicability of the exceptions listed in Art. 9(2) of the GDPR and on the obligation of the data users

[65] MARCUS, J Scott; MARTENS, Bertin; CARUGATI, Christophe; BUCHER, Anne; GODLOVITCH, Ilsa; "The European Health Data Space – Study requested by the ITRE Committee", 2022. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740054/IPOL_STU(2022)740054_EN.pdf

[66] TERZIS, Petros; "Compromises and Asymmetries in the European Health Data Space"; *European Journal of Health Law*; 29; 2022; page 1 to 19.

[67] *Ibidem.*

to inform the national data access bodies of the applicable condition.[68] This will ensure that the legal provisions of the Proposal meet the requirements established in Art. 9 (2): (*i*) proportionality when considering the objectives pursued, (*ii*) respect of the data protection right, and (*iii*) appropriate and specific measures to safeguard the fundamental rights and interests of the data subjects.

In addition to the challenges already mentioned, there are further legal obstacles that should be addressed to ensure the success of the EHDS. One of the main concerns is the derogation to the information obligations provided for in Art. 38(2) of the Proposal. To overcome this issue, alternative solutions such as limiting the derogation to specific situations or enhancing transparency obligations may be considered. Additionally, mechanisms to facilitate the exercise of the right of access under Art. 15 of the GDPR could be created to ensure data subjects have access to relevant information about the processing of their personal data.

Furthermore, it is crucial to establish a uniform understanding among all the national data protection supervisory authorities (existing and created based on EHDS) regarding the EHDS and its data protection implications to ensure its success. Uncertainty surrounding the approach of different authorities and possible fragmented implementation may deter data users from participating in the EHDS, ultimately hindering its goals, in particular due to the high fines that data users may face subject to the GDPR.

In conclusion, the legal obstacles and challenges presented in the EHDS Proposal must be addressed to create a better and more effective EHDS Regulation. Overcoming these obstacles will not only contribute to the success of the EHDS but also to the development of robust European Data Spaces, creating technological opportunities and

[68] As suggested by the EDPB and the EDPS, in European Data Protection Board and the European Data Protection Supervisor in their Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, 12 July 2022, available at https://edpb.europa.eu/system/files/202207/edpb_edps_jointopinion_202203_europeanhealthdataspace_en.pdf

offering a competitive advantage to EU companies, especially start-ups and SMEs in line with the EU´s strategic objectives.

A investigação clínica na era do altruísmo dos dados: algumas considerações em torno da proteção de dados pessoais

Elisabete Castela[1]
Tiago Branco da Costa[2]

Resumo: A investigação clínica contribui para a melhoria significativa do conhecimento científico, e, por conseguinte, potencia a melhoria da qualidade e da eficácia dos cuidados de saúde. No entanto, por contender com a tutela oferecida pelo quadro legal atinente à proteção de dados pessoais, é necessário encontrar o ponderado equilíbrio entre o respeito pela privacidade e autodeterminação dos sujeitos com a necessidade premente e cada vez mais global de procurar mais e melhores soluções ao nível da prestação e da gestão dos cuidados de saúde.

Palavras-chave: *Dados pessoais; Investigação clínica; Licitude; Proteção de dados.*

Abstract: Clinical research contributes to the significant improvement of scientific knowledge, and, therefore, promotes the improvement of the quality and effectiveness of health care. However, as it contends with the protection offered by the legal framework on the protection of personal data, it is necessary to find the right balance between the respect for the subjects' privacy and self-determination and the pressing

[1] Encarregada da Proteção de Dados do Centro Hospitalar Universitário de Santo António, E.P.E.; Administradora Hospitalar no Centro Hospitalar Universitário de Santo António, E.P.E., elisabete.castela@chporto.min-saude.pt.

[2] Assistente convidado na Escola de Direito da Universidade do Minho; Doutorando em Ciências Jurídicas Privatísticas na Escola de Direito da Universidade do Minho e Bolseiro da Fundação para a Ciência e Tecnologia; tiagobrancodacosta@direito.uminho.pt.

and increasingly global need to seek more and better solutions in the provision and management of health care.

Keywords: *Personal data; Clinical research; Lawfulness; Data protection.*

1. Considerações introdutórias

A investigação clínica assume um papel primordial no setor da saúde, na medida em que contribui para a melhoria significativa do conhecimento científico, e, por conseguinte, potencia a melhoria da qualidade e da eficácia dos cuidados de saúde, bem como uma maior eficiência na gestão dos recursos[3].

Por outro lado, atento o domínio em que a mesma se desenvolve, a investigação clínica representa um risco acrescido para a esfera de privacidade e de autodeterminação dos participantes nos estudos clínicos, daí que o interesse e o bem-estar do ser humano devam prevalecer perante os interesses da sociedade ou da ciência[4].

A par disto, a legislação atinente à proteção de dados pessoais consagra, como regra geral, a proibição de tratamento de dados pessoais de categorias especiais, como sejam os dados relativos à saúde. No entanto, encontram-se previstas várias exceções que legitimam o tratamento desses dados especiais, designadamente para efeitos de investigação

[3] Cfr. MARTÍN URANGA, Amelia, "Protección de datos y fomento de la investigación científica: la necesidad de un equilíbrio adecuado (comentario al artículo 9.2.j) RGPD)", in *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales*, Tomo I, Thomson Reuters, 2021, 1219-1248, p.1219, "El desarrollo de la Ciencia tiene como objetivo fundamental llevarnos a conocer mejor el mundo en el que vivimos. El derecho a la investigación científica viene a ser una proyección del derecho a la creación científica, con el que se atende a los interesses del investigador y también a los colectivos de promover el progresso científico en beneficio de la sociedad".

[4] Assim se prescreve no art. 2.º da Convenção para a Proteção dos Direitos do Homem e da Dignidade do Ser Humano face às Aplicações da Biologia e da Medicina.

científica. Se, por um lado, este regime de proteção de dados pessoais é caracterizado por um elevado nível de exigência e de responsabilidade em relação ao tratamento de dados pessoais que seja levado a cabo pelo responsável pelo tratamento, por outro lado, oferece-se um espaço privilegiado à investigação científica, na medida em que a mesma impõe, ao longo do diploma, várias exceções e derrogações ao regime geral[5], conforme teremos oportunidade de analisar adiante com mais pormenor.

Ademais, o contexto pandémico que desafiou a Europa e o Mundo destacou a relevância do acesso seguro e protegido aos dados de saúde pública e de cuidados de saúde para além das fronteiras de cada Estado, e colocou em causa, de algum modo, a perspetiva individual e egoísta dos dados que temos vindo a acolher. Nesta senda, o novo Espaço Europeu de Dados de Saúde[6], anunciado em maio de 2022, apresenta-se como um espaço comum onde as pessoas singulares poderão controlar facilmente os seus dados de saúde eletrónicos, e onde os investigadores, os inovadores, os decisores políticos e as entidades reguladoras poderão aceder a dados de saúde eletrónicos, com o intuito de promover um melhor diagnóstico, tratamento e bem-estar das pessoas singulares e implementar políticas mais adequadas e bem fundamentadas.

Procuraremos, assim, caracterizar o contexto jurídico em que se desenvolve a investigação clínica, compreender como a mesma se concilia com a proteção de dados pessoais e como se insere na estratégia europeia para os dados e no espaço europeu de dados de saúde (EEDS), recentemente anunciado pela Comissão Europeia, que apela a um altruísmo ao nível europeu.

[5] *Vd.* MONGE, Cláudia, "Acesso à informação de saúde e à informação genética", in *O acesso à informação administrativa*, Almedina, 2021, p.549-649, p.575.

[6] Disponível em https://ec.europa.eu/commission/presscorner/detail/pt/ip_22_2711.

2. A investigação clínica: conceitos e princípios basilares

A investigação clínica[7] consiste, nos termos do disposto no art. 1.º da Lei da Investigação Clínica (LIC)[8], no estudo sistemático destinado a descobrir ou a verificar a distribuição ou o efeito de fatores de saúde, de estados ou resultados em saúde, de processos de saúde ou de doença, do desempenho e/ou segurança de intervenções ou da prestação de cuidados de saúde.

O citado diploma legal opera, por conseguinte, algumas distinções quanto ao objeto, aos sujeitos intervenientes, à finalidade e amplitude e ao objeto do estudo que se pretende levar a cabo, caracterizando: o «estudo clínico»[9], que inclui o «estudo clínico de regimes alimentares»[10] e o «estudo clínico de terapêutica não convencional»[11], o «estudo multicêntrico»[12], o «estudo clínico sem intervenção»[13], o «estudo clínico com intervenção»[14], o «estudo clínico de dispositivo médico»[15] e o «estudo clínico de produtos cosméticos e de higiene corporal»[16].

Note-se, no entanto, que este agrupamento, que tem por base os diferentes critérios consagrados na lei, não é estanque, mas permite

[7] O CEPD assinala que o RGPD não avança com uma definição de «investigação científica», mas que a mesma corresponde ao seu significado comum, isto é, "projeto de investigação criado de acordo com as normas metodológicas e éticas aplicáveis em cada setor, em conformidade com as boas práticas" – cfr. COMITÉ EUROPEU PARA A PROTEÇÃO DE DADOS, *Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679*, 04 de maio de 2020, p. 35. No entanto, não podemos deixar de considerar a amplitude que é conferida pelo RGPD ao conceito de investigação clínica, quando no considerando 159 se diz que o mesmo "deverá ser entendido em sentido lato, abrangendo, por exemplo, o desenvolvimento tecnológico e a demonstração, a investigação fundamental, a investigação aplicada e a investigação financiada pelo setor privado", e que deve contemplar ainda os "estudos de interesse público realizados no domínio da saúde pública".

[8] Lei n.º 21/2014, de 16 de abril, cuja última alteração foi introduzida pela Lei n.º 49/2018, de 14 de agosto.

[9] Cfr. alínea p) do art. 2.º da LIC.

[10] Cfr. subal. i) da alínea p) do art. 2.º da LIC.

[11] Cfr. subal. ii) da alínea p) do art. 2.º da LIC.

[12] Cfr. al. q) do art. 2.º da LIC.

[13] Cfr. al. r) do art. 2.º da LIC.

[14] Cfr. al. s) do art. 2.º da LIC.

[15] Cfr. al. t) do art. 2.º da LIC.

[16] Cfr. al. u) do art. 2.º da LIC.

apenas compreender a diversidade da investigação clínica[17]. Por outro lado, esta cisão releva para efeitos de determinação do regime legal aplicável, tendo em conta que, consoante a natureza, a extensão e as finalidades do estudo, o risco a que o indivíduo se submete é, consideravelmente, diverso, e, por essa razão, nos termos da lei da investigação clínica, diversas são também as obrigações que impendem sobre os diversos sujeitos intervenientes no estudo.

Embora não se pretenda com o presente estudo escalpelizar os diferentes tipos de estudos consagrados no identificado diploma legal, é relevante assinalar que o «estudo clínico» é entendido como o estudo sistemático, conduzido no ser humano, ou a partir de dados de saúde individuais, que tem como desiderato descobrir ou verificar a distribuição ou o efeito de fatores de saúde, de estados ou resultados em saúde, de processos de saúde ou de doença, do desempenho e/ou segurança de intervenções ou serviços de saúde, através de aspetos biológicos, comportamentais, sociais ou organizacionais[18]. Como tal, há que assinalar que o conceito de ensaio clínico preconizado pela lei da investigação clínica[19] deve ser entendido como uma modalidade de estudo clínico, que é conduzido no ser humano e que compreende a utilização de medicamentos.

Deste modo, sem prejuízo das distinções operadas, cremos estar em condições de fazer uma primeira constatação: todos os tipos de estudos elencados envolvem, em maior ou menor grau, o tratamento de dados pessoais e, portanto, a ingerência na esfera de privacidade e de

[17] A título de exemplo, um estudo clínico de dispositivo médico pode ser considerado um estudo com intervenção (cfr. al. s) do art. 2.º, quando se diz "com a finalidade de descobrir ou verificar efeitos na saúde, incluindo (…) a utilização de dispositivos médicos" e desde que o mesmo preconize a referida alteração, influência ou programação dos cuidados de saúde, dos comportamentos ou dos conhecimentos dos participantes ou cuidadores) e, num outro contexto, um estudo sem intervenção (cfr. al. r) do art. 2.º, quando se estabelece como condição "(i) os medicamentos sejam prescritos ou os dispositivos médicos sejam utilizados de acordo com as condições previstas na autorização de introdução no mercado ou no procedimento de avaliação de conformidade, respetivamente").

[18] Cfr. alínea p) do art. 2.º da LIC.

[19] Cfr. alínea n) do art. 2.º da LIC.

autodeterminação do indivíduo[20]. Por essa razão, devemos atender a um conjunto geral de princípios basilares que se aplicam a todas as modalidades de estudos que acabamos de elencar, que tenham por base o tratamento de dados pessoais.

O primeiro princípio a merecer destaque neste contexto é o princípio da dignidade da pessoa humana, que deve nortear a atuação dos vários atores envolvidos na investigação clínica, no sentido em que os estudos clínicos, em nome do avanço científico e do interesse da sociedade, jamais poderão colocar em causa a dignidade da pessoa humana e a sua autodeterminação. Pese embora se reconheça, sobejamente, a relevância do progresso dos cuidados de saúde em geral, a lei não deixa de o colocar num segundo plano, quando colocado em perspetiva com a dignidade da pessoa humana e com os seus direitos fundamentais[21].

Sob a égide do primado da pessoa humana[22], o legislador, embora pudesse tê-lo reconduzido ao conteúdo dos direitos fundamentais, previu, expressamente, o dever de respeito pelo direito à privacidade do indivíduo, bem como o dever de respeito e de minimização de riscos relativamente aos direitos de personalidade do indivíduo e à sua integridade física e mental[23].

Seguidamente, há destaque para o princípio das boas práticas clínicas[24], impondo-se a conceção, a realização, o registo, a notificação e a revisão e divulgação de resultados de acordo com os princípios das

---

[20] *Vd.*, entre outros, IGLÉSIAS, Filipa; PEREIRA, André Dias, "O uso secundário de dados pessoais de saúde na investigação científica: legislação e práticas no ordenamento jurídico português"; *Lex Medicinae*, Ano 18, n.º 35, 2021, 15-27, https://www.centrodedireitobiomedico.org/publica%C3%A7%C3%B5es/publica%C3%A7%C3%B5es-online/revista-portuguesa-de-direito-da-sa%C3%BAde-lex-medicinae-ano-18-n%C2%BA35, p.27, "A investigação clínica é um terreno fértil de recolha e criação de informação e dados de saúde, cada vez mais estruturados em repositórios e bases de dados eletrónicas, com amplo potencial de partilha e interconexão".

[21] Cfr. n.º 2 do art. 3.º da LIC.

[22] DUARTE, Tatiana, "Anotação ao artigo 9.º", in Comentário ao Regulamento Geral de Proteção dados, Almedina, 2018, p. 236-334, p. 304 "o princípio do primado do indivíduo que participa na investigação modela o conteúdo, os procedimentos e as metodologias aplicáveis à investigação científica em seres humanos".

[23] Cfr. n.º 3 do art. 3.º da LIC.

[24] Cfr. art. 4.º da LIC.

boas práticas clínicas. As boas práticas clínicas referem-se a critérios de natureza ética e científica, internacionalmente reconhecidos, que deverão aplicar-se aos estudos clínicos que envolvam a participação de seres humanos[25].

A investigação clínica parece também estar subordinada ao princípio da proporcionalidade, na medida em que se condiciona a realização dos estudos clínicos a uma ponderação custo-benefício entre o almejado avanço científico e os riscos e inconvenientes que do estudo possam resultar[26]. Esta ponderação é assegurada pelas comissões de ética, nos termos da lei da investigação clínica[27].

Não podemos olvidar que o regime jurídico da investigação clínica é, em rigor, fruto da influência de diversos diplomas legais que coabitam no ordenamento jurídico português e no contexto europeu. Por essa razão, importa também considerar, para o presente estudo, entre outros: a Lei de Bases da Saúde[28], a Lei relativa à informação genética pessoal e informação de saúde[29], o Regulamento relativo aos dispositivos médicos[30], o Regulamento Geral sobre a Proteção de Dados (RGPD)[31] e a Lei de Execução do RGPD (LERGPD)[32].

Destarte, a Lei de Bases da Saúde contempla na base 2, que é responsável por estabelecer os direitos e deveres das pessoas, a proteção da saúde com respeito, entre outros, pelos princípios da confidencialidade e da privacidade. Ademais, a base 4 refere-se à política de saúde tendo por fundamento as pessoas como elemento central na conceção,

---

[25] Cfr. alínea f) do art. 2.º da LIC.

[26] Cfr. art. 5.º da LIC.

[27] *Ibidem*.

[28] Lei n.º 95/2019, de 04 de setembro.

[29] Lei n.º 12/2005, de 26 de janeiro, cuja última alteração foi introduzida pela Lei n.º 26/2016, de 22 de agosto.

[30] Regulamento (UE) 2017/745, do Parlamento Europeu e do Conselho, de 5 de abril de 2017, relativo aos dispositivos médicos, OJ L 117, 5.5.2017, p.1-175.

[31] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, OJ L 119, 4.5.2016, p.1-88.

[32] Lei n.º 58/2019, de 08 de agosto, que assegura a execução, na ordem jurídica nacional, do Regulamento Geral sobre a Proteção de Dados.

organização e funcionamento de estabelecimentos, serviços e respostas de saúde, mas, concomitantemente, o incentivo à investigação em saúde, como motor da melhoria da prestação de cuidados, bem como o reconhecimento da saúde como um investimento que beneficia a economia e a relevância económica da saúde. Não obstante, a informação de saúde continua a ser considerada propriedade da pessoa, pelo que a sua circulação deve ocorrer em respeito pela segurança e proteção dos dados pessoais e da informação de saúde e pelo princípio da intervenção mínima (cfr. base 15).

O primado da pessoa humana é, como referimos supra, a linha mestra[33]. Em matéria de tecnologia e de inovação, e com especial interesse para o nosso estudo, prescreve-se, em sintonia com o atrás referido relativamente à base 4, que as mesmas sejam utilizadas de forma a reforçar a humanização e a dignidade da pessoa[34]. Aliás, a investigação deve ser norteada pelo princípio ético orientador do respeito pela vida humana e deverá observar um conjunto de condições, especialmente quando a mesma se baseie na experimentação em seres humanos e em ensaios clínicos – *respeito pela dignidade e pelos direitos fundamentais, segurança e bem-estar dos participantes, cumprimento das regras da boa prática de investigação, inexistência de contrapartidas para os participantes*[35].

No mesmo sentido vai a Lei da informação genética pessoal e informação de saúde, que reclama a proteção da confidencialidade da informação de saúde[36]. Com mais propriedade, o RGPD e a LERGPD definem um conjunto alargado de princípios que deve nortear qualquer operação de tratamento de dados pessoais, e, portanto, mobilizável no domínio da investigação científica, cuja análise faremos de seguida.

---

[33] *Vd.* Convenção sobre os Direitos do Homem e a Biomedicina, aprovada, para ratificação, pela Resolução da Assembleia da República n.º 1/2001, de 03 de janeiro.

[34] Cfr. n.º 2 da base 17 da Lei de Bases da Saúde.

[35] Cfr. n.º 3 da base 31 da Lei de Bases da Saúde.

[36] Cfr. art. 4.º da Lei da informação genética pessoal e informação de saúde.

3. Os dados pessoais objeto de tratamento na investigação clínica

A investigação clínica alimenta-se de dados pessoais e, em especial, de dados de categorias especiais, como é o caso dos dados relativos à saúde, dos dados genéticos e dos dados biométricos.

Quando nos referimos a dados pessoais estamos a aludir a toda a informação relativa a uma pessoa singular identificada ou identificável, sendo certo que é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular[37].

Por sua vez, quando nos referimos aos dados de categorias especiais estamos a mencionar os dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa[38].

Os «dados relativos à saúde» dizem respeito aos dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde[39].

Os «dados genéticos» também são particularmente relevantes neste contexto, já que dizem respeito aos dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular

[37] Cfr. n.º 1 do art. 4.º e Considerandos 26, 27, 30, 34 e 35 do RGPD.

[38] Cfr. n.º 1 do art. 9.º do RGPD.

[39] Cfr. n.º 15 do art. 4.º e considerando 35 do RGPD. Cfr. Tribunal de Justiça da União Europeia, Processo C-101/01, Göta hovrätt (Suécia) contra Bodil Lindqvist, 06 de novembro de 2003.

que oferecem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta, designadamente, de uma análise de uma amostra biológica proveniente da pessoa singular em causa[40].

Do mesmo modo, especial tutela merecem os «dados biométricos», na medida em que abrangem os dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitem ou confirmam a identificação única dessa pessoa singular[41].

Para além destes, os dados pessoais de categorias gerais, como o género, a morada, a idade, entre outros, poderão também interessar para o estudo em questão, sendo certo, contudo, que o regime aplicável será diverso, no que concerne à proteção de dados pessoais. Com efeito, a distinção entre dados pessoais de categorias gerais e dados de categorias especiais resulta, em bom rigor, da diferente disciplina consagrada no RGPD para o tratamento de dados pessoais de cada uma das categorias em apreço. Sem prejuízo da citada diferença de regime, que adiante apreciaremos, em ambos os casos serão aplicáveis os princípios gerais a que alude o art. 5.º do RGPD.

Note-se, todavia, que em vários diplomas da União, mormente aqueles que regulam os diferentes aspetos atinentes ao mercado único digital e ao mercado de dados, são empregues conceitos como "dados", "dados não pessoais" ou, ainda, "dados de saúde eletrónicos não pessoais", "conjunto de dados" e "catálogo de conjuntos de dados". O conceito de "dados" definido no Regulamento Governação de Dados[42] refere-se a qualquer representação digital de atos, factos ou informações e qualquer compilação desses atos, factos ou informações. Por sua vez, o conceito de dados não pessoais, também definido no mesmo diploma legal, refere-se a "dados que não sejam

[40] Cfr. n.º 13 do art. 4.º do RGPD.

[41] Cfr. n.º 14 do art. 4.º do RGPD.

[42] Regulamento (UE) 2022/868 do Parlamento Europeu e do Conselho de 30 de maio de 2022 relativo à governação europeia de dados e que altera o Regulamento (UE) 2018/1724 (Regulamento Governação de Dados), PE/85/2021/REV/1, OJ L 152, 3.6.2022, p.1-44.

dados pessoais", isto é, dados que não caibam na definição do ponto 1, do art. 4.º, do RGPD.

Os dados de saúde eletrónicos não pessoais, definidos na Proposta de Regulamento EEDS[43], dizem respeito aos dados relativos à saúde e aos dados genéticos em formato eletrónico, que não caibam na definição de dados pessoais avançada pelo RGPD. O "conjunto de dados" diz respeito ao conjunto estruturado de dados de saúde eletrónicos e, por sua vez, o catálogo de conjuntos de dados representa uma compilação de descrições de conjuntos de dados, organizada de forma sistemática e constituída por uma parte pública orientada para o utilizador, em que as informações relativas aos parâmetros individuais dos conjuntos de dados estão acessíveis por meio eletrónicos através de um portal em linha[44].

Ora, nestes universos convivem, como se compreende, dados pessoais e não pessoais, sem que se consiga, a maior parte das vezes, assegurar a separação de uns e de outros. Nesses casos, em que os dados não pessoais e os dados pessoais estiverem «indissociavelmente ligados», os direitos e obrigações em matéria de proteção de dados decorrentes do RGPD deverão aplicar-se, plenamente, a todo o conjunto misto de dados, mesmo que os dados pessoais representem apenas uma pequena parte desses conjuntos de dados[45].

A este respeito, não é despiciendo trazer à colação as preocupações sobre a anonimização de dados e a reversibilidade dessas medidas, na medida em que tal poderá condicionar, em cada caso em concreto, a classificação dos dados como pessoais ou não pessoais.

---

[43] Proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao Espaço Europeu de Dados de Saúde, COM/2022/197 final, disponível em https://health.ec.europa.eu/publications/proposal-regulation-european-health-data-space_en.

[44] Cfr. Alíneas b), ab) e ac) do n.º 2 do art. 2.º da Proposta de Regulamento EEDS.

[45] Cfr. KUNER, Christopher, et. al., *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford University Press, 2020, p.112-113.

4. Os princípios norteadores do tratamento de dados no contexto de investigação clínica

O RGPD estabeleceu no seu art. 5.º os princípios gerais pelos quais se deve pautar o tratamento de dados pessoais – *princípio da licitude, lealdade e transparência, princípio da limitação das finalidades, princípio da minimização dos dados, princípio da exatidão, princípio da limitação da conservação, princípio da integridade e da confidencialidade e princípio da responsabilidade*[46].

O princípio da licitude traduz-se na necessidade de reconduzir o tratamento de dados a uma condição de licitude prevista na lei, seja entre as várias opções oferecidas pelo art. 6.º do RGPD, quando esteja em causa o tratamento de dados pessoais de categorias gerais, seja entre o leque apresentado pelo n.º 2 do art. 9.º, quando esteja em causa o tratamento de dados pessoais de categorias especiais.

Por seu turno, o princípio da lealdade impõe o conhecimento pelo titular dos dados dos riscos, regras, garantias e direitos associados ao tratamento dos seus dados pessoais, bem como dos meios disponíveis para o exercício dos seus direitos. Os deveres de informação que recaem sobre o responsável pelo tratamento representam, em bom rigor, um desdobramento do princípio da lealdade, o qual no contexto particular da investigação clínica reveste particular importância. Em linha com este, o princípio da transparência exige a facilidade de acesso e de compreensão das informações e comunicações relacionadas com o tratamento de dados pessoais. O investigador, na qualidade de responsável pelo tratamento de dados, está obrigado a informar o participante no estudo dos seguintes elementos, consoante o caso (art. 13.º do RGPD): (i) identidade e contactos do responsável pelo tratamento; (ii) contactos do encarregado da proteção de dados; (iii) finalidades do

[46] Para mais desenvolvimentos, *vd.*, entre outros, PINHEIRO, Alexandre Sousa; GONÇALVES, Carlos Jorge, "Anotação ao artigo 5.º", in *Comentário ao Regulamento Geral de Proteção de Dados*, Almedina, 2018, p.204-212; MONIZ, Graça Canto, *Manual de Introdução à Proteção de Dados Pessoais*, Almedina, 2023, p.65-132.

tratamento a que os dados pessoais se destinam e fundamento jurídico; (iv) interesses legítimos do responsável pelo tratamento ou de um terceiro; (v) destinatários ou categorias de destinatários dos dados pessoais; (vi) intenção de transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas; (vii) prazo de conservação dos dados pessoais ou respetivos critérios de definição; (viii) existência do direito de solicitar ao responsável pelo tratamento o acesso aos dados pessoais que lhe digam respeito, bem como a sua retificação ou o seu apagamento, e a limitação do tratamento no que disser respeito ao titular dos dados, ou do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados; (ix) se o tratamento dos dados tiver por base o consentimento do titular dos dados, a existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado; (x) direito de apresentar reclamação a uma autoridade de controlo; (xi) se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados; e (xii) existência de decisões automatizadas, incluindo a definição de perfis. A esta informação soma-se a origem dos dados pessoais e, eventualmente, se provêm de fontes acessíveis ao público, quando os dados não sejam recolhidos junto do titular dos dados (art. 14.º do RGPD).

Em suma, o tratamento de dados será transparente quando o participante no estudo conheça e bem entenda todas as informações relativas ao tratamento dos seus dados, assim como todas as comunicações que lhe sejam dirigidas a este respeito.

Um outro princípio que, no nosso modesto entendimento, merece particular destaque neste domínio é o princípio da limitação das finalidades, que exige que o tratamento de dados levado a cabo pelo

investigador respeite finalidades (i) determinadas, (ii) explícitas e (iii) legítimas. As finalidades deverão ser (i) determinadas na medida em que sejam devidamente fixadas, antes do processo de tratamento iniciar; (ii) explícitas na medida em que sejam "definidas sem espaço para ambiguidades"[47] e "informadas aos e conhecidas dos interessados"[48]; e (iii) legítimas na medida em que respeitem as normas vigentes.

No domínio do EEDS e, em particular, no que concerne à utilização primária de dados e à utilização secundária de dados, este princípio da limitação das finalidades poderá vir a sofrer uma compressão no novo espaço comum de dados, sem prejuízo daquela que já sofre no RGPD, no domínio da investigação científica[49].

De qualquer modo, no que respeita à determinação das finalidades, não podemos ignorar a prerrogativa estabelecida a propósito de um tratamento que vá além das finalidades previamente determinadas, nos termos e para os efeitos previstos no n.º 4 do art. 6.º do RGPD[50]. Este alargamento do tratamento de dados pessoais depende, contudo, do preenchimento de alguns requisitos legais, a saber: (i) o tratamento de dados deve prosseguir um fim distinto daquele para o qual os dados pessoais do titular foram inicialmente recolhidos; (ii) não haja consentimento do titular para esse tratamento para outros fins; (iii) o tratamento para outros fins não seja operado com base em disposições do direito da União ou dos Estados-Membros, que constituam uma medida necessária e proporcionada numa sociedade democrática para salvaguardar os objetivos referidos no n.º 1 do art. 23.º do RGPD; e (iv) compatibilidade entre o tratamento para outros fins e a finalidade para a qual os

---

[47] MONIZ, Graça Canto, *Manual de Introdução à Proteção de Dados Pessoais*, *op. cit.*, p.109.

[48] CORDEIRO, A. Barreto Menezes, *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019, op. cit.*, p.104.

[49] Costa, Tiago Branco da, "O altruísmo (económico?) de dados: breves considerações sobre o espaço europeu de dados de saúde e a proteção de dados pessoais", em Oliveira, A. Sofia Pinto & Jerónimo, Patrícia (Coord.), *Liber Amicorum Benedita Mac Crorie*, Volume II, Braga, Uminho Editora, 2022, 613-622, pp. 635-642.

[50] Sobre esta possibilidade, *vd.*, entre outros, KUNER, Christopher, et. al., *The EU General Data Protection Regulation…, op. cit.*, p.326-327.

dados pessoais foram inicialmente recolhidos[51]. Note-se, no entanto, que neste exercício de ponderação, deve atender-se a uma ligação entre a finalidade para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior; ao contexto em que os dados pessoais foram recolhidos; à natureza dos dados pessoais, em especial se as categorias especiais de dados pessoais forem tratadas nos termos do art. 9.º; às eventuais consequências do tratamento posterior; e à exigência de salvaguardas adequadas.

Todavia, com maior relevância no contexto da investigação clínica, não podemos deixar de sublinhar que o tratamento posterior para fins de investigação científica ou histórica ou para fins estatísticos não é considerado incompatível com as finalidades iniciais (em conformidade com as garantias e derrogações previstas no n.º 1 do art. 89.º do RGPD)[52]. Porém, sem prejuízo desta compatibilidade *ex lege*, o responsável pelo tratamento de dados poderá ver-se confrontado com a necessidade de encontrar um novo fundamento legal para o tratamento de dados, quando as operações de tratamento que queira levar a cabo não caibam no fundamento inicialmente encontrado para o efeito, isto é, quando o(s) fundamento(s) daquele tratamento de dados passe a ser, exclusiva ou maioritariamente, outro que não a investigação clínica *de per si*. Como é evidente, os sujeitos intervenientes na investigação clínica não poderão servir-se da presumível compatibilidade dos fins da investigação clínica com os fins inicialmente determinados para efeito de tratamento de dados, quando, na verdade, pretendam, dessa forma, camuflar outras intenções que não sejam aquelas que se reportam estritamente ou maioritariamente à investigação clínica.

---

[51] *Vd.* Tribunal de Justiça da União Europeia, Processo C77/21, Digi Távközlési és Szolgáltató Kft. Contra Nemzeti Adatvédelmi és Információszabadság Hatóság, 20 de outubro de 2022.

[52] Cfr. al. b), *in fine*, do n.º 1 do art. 5.º do RGPD. Cfr. COMITÉ EUROPEU PARA A PROTEÇÃO DE DADOS, *EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research*, 02 de fevereiro de 2021, p.4, onde o CEPD entendeu que, no quadro do RGPD, o consentimento ético que seja recolhido para a participação no estudo pode ser entendido como uma das garantias adequadas contempladas pelo n.º 1 do artigo 89.º.

Ademais, os dados pessoais que sejam objeto de tratamento devem ser adequados, pertinentes e limitados ao que é necessário, relativamente à finalidade do tratamento. O legislador empregou, a respeito do princípio da minimização dos dados, os conceitos «adequado», «pertinente» e «necessário», que nos recordam o princípio da proporcionalidade, e que se referem à necessidade da medida a adotar; à adequação da medida adotada à prossecução do fim; e à menor ingerência ou desvantagem possível, isto é, ao juízo de ponderação necessário entre o resultado obtido e a sua onerosidade[53].

Uma vez mais, a este respeito, não podemos deixar de assinalar que o EEDS, sob a capa da utilização secundária de dados parece admitir a compressão deste princípio, desde logo ao fixar um conjunto alargado de dados que devem ser registados e partilhados, que, note-se, é mais extenso do que aquele que se encontra fixado para a utilização primária, ou seja, para efeitos de prestação de cuidados de saúde.

Uma vez que concretiza o princípio da minimização dos dados, bem como os princípios da integridade e da confidencialidade, convém lembrar, a este respeito, que o legislador nacional veio a consagrar, no domínio do acesso aos dados de saúde e aos dados genéticos, o princípio da necessidade de conhecer a informação[54]. Por essa razão, A. Barreto menezes cordeiro assinala que "a sua positivação não era necessária, ele seria sempre aplicável"[55], uma vez que apenas se reforça a ideia já plasmada de que apenas devem ter acesso aos dados, neste contexto, os sujeitos intervenientes na investigação, que tenham a necessidade de os conhecer (e nessa exata medida). Atendendo à natureza dos dados pessoais em apreço, "quanto maior for o leque de pessoas que acedem a dados de saúde, maiores são os riscos para a segurança, integridade e confidencialidade desses dados"[56].

---

[53] A este respeito, *vd.* Tribunal de Justiça da União Europeia, Processo C268/21, Norra Stockholm Bygg AB contra Per Nycander AB, 02 de março de 2023.

[54] Cfr. n.º 1 do artigo 29.º da LERGPD.

[55] Cfr. CORDEIRO, A. Barreto Menezes, *Direito da Proteção de Dados – À luz do RGPD e da Lei n.º 58/2019,* Almedina, 2020*,* p.253.

[56] Cfr. COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS, Parecer n.º 20/2018, Processo n.º 6275/2018, 02 de maio de 2018, p.29.

O princípio da exatidão exige que os dados pessoais objeto de tratamento, em atenção à finalidade para a qual são tratados, sejam corretos e atuais, pelo que, quando assim não seja, devem ser adotadas as medidas necessárias ao seu apagamento ou à sua retificação. Contudo, este princípio deve ser interpretado com alguma parcimónia no que concerne ao conceito de «dados atuais», na medida em que, no contexto particular da saúde e da investigação clínica, o histórico clínico do paciente assume particular relevância para o diagnóstico, para o tratamento e para a investigação que se pretenda levar a cabo. Por essa razão, a informação que, *prima facie*, poderia ser considerada desatualizada, pode, na verdade, ser bastante relevante no contexto da investigação clínica.

Por outro lado, os dados pessoais devem ser conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais os dados são tratados. É nisto que se traduz o princípio da limitação da conservação que se interseta com o princípio da minimização dos dados, sobretudo quando reclama a aplicação do princípio da proporcionalidade.

Os dados pessoais devem também ser tratados de forma segura, devendo o responsável pelo tratamento de dados assegurar a proteção dos dados dos participantes no estudo contra o tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental. Cabe-lhe, casuisticamente, adotar medidas técnicas ou organizativas adequadas à garantia da segurança dos dados, atendendo às técnicas mais avançadas, aos custos de aplicação e à natureza, ao âmbito, ao contexto, às finalidades do tratamento, à natureza dos dados, bem como aos riscos, de probabilidade e gravidade variável, para os direitos e liberdades dos pacientes. Assim, deverá o responsável pelo tratamento de dados incluir nas medidas a adotar: (i) a pseudonimização e encriptação dos dados pessoais; (ii) a capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento; (iii) a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico; (iv) um processo para testar, apreciar e

avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

O último princípio que cumpre assinalar é o da responsabilidade. Sobre o responsável pelo tratamento de dados recaem especiais deveres e responsabilidades, pelo que este sujeito será, assim, responsável pelo cumprimento pontual de todos os princípios elencados no n.º 1 do art. 5.º do RGPD, bem como pela comprovação desse mesmo cumprimento (cfr. art. 24.º do RGPD), sendo certo que, em caso de incumprimento dos deveres a que se encontra adstrito, o responsável pelo tratamento de dados poderá ver a sua responsabilidade acionada nos termos do disposto nos art. 79.º e 82.º do RGPD, quando o participante no estudo entenda ter havido uma violação à lei e tenha sofrido danos decorrentes dessa violação[57].

5. A licitude do tratamento de dados na investigação clínica

Conforme enunciámos supra, a respeito do princípio da licitude, o tratamento de dados pessoais no contexto da investigação clínica deve ter por base uma condição de licitude que o legitime[58]. Como tal, o art. 6.º do RGPD, elenca as diferentes condições de licitude aplicáveis ao tratamento de dados pessoais, a saber: (i) consentimento do titular dos dados para o tratamento de dados para uma ou mais

[57] A este respeito não é despiciendo recordar que, nos termos da alínea e) do n.º 1 do artigo 6.º da LIC, uma das condições mínimas de proteção dos participantes nos estudos clínicos é a existência de um seguro que cubra a responsabilidade civil do promotor e do investigador, que respondem solidariamente, e independentemente de culpa, pelos danos patrimoniais e não patrimoniais que o estudo possa causar ao participante. Ora, não vemos razões para excluir deste regime os eventuais danos causados por violação das regras atinentes ao regime da proteção de dados pessoais, pese embora o regime de responsabilidade consagrado no RGPD não corresponda *ipsis verbis* ao regime adotado pela LIC (designadamente no que concerne à culpa e à obrigatoriedade de subscrição de um seguro). Vd. ainda Tribunal de Justiça da União Europeia, Processo C-300/21, UI contra Österreichische Post AG, 04 de maio de 2023

[58] Cfr. COMITÉ EUROPEU PARA A PROTEÇÃO DE DADOS, *Diretrizes 03/2020 sobre o tratamento de dados relativos à saúde para efeitos de investigação científica no contexto do surto de COVID-19*, 21 de abril de 2020, p.6.

finalidades específicas; (ii) necessidade do tratamento de dados para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados; (iii) necessidade do tratamento de dados para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; (iv) necessidade do tratamento para efeitos de defesa de interesses vitais do titular dos dados ou de outra pessoa singular; (v) necessidade do tratamento de dados para efeitos de exercício de funções de interesse público ou de exercício da autoridade pública de que está investido o responsável pelo tratamento; (vi) necessidade do tratamento para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros.

Contudo, o art. 9.º do RGPD estabelece um regime diverso daquele que se encontra previsto no art. 6.º[59], contendo no n.º 1 a regra geral da proibição de tratamento destes dados de categorias especiais e no seu n.º 2 um conjunto de exceções a essa regra, a saber: (i) consentimento explícito do titular dos dados; (ii) necessidade do tratamento de dados para o cumprimento de obrigações e para o exercício de direitos do responsável pelo tratamento de dados ou do titular dos dados em matéria de legislação laboral, segurança social e de proteção social; (iii) proteção de interesses vitais do titular dos dados ou de outra pessoa singular, no caso de o titular estar física ou legalmente incapacitado de dar o seu consentimento; (iv) se o tratamento for efetuado no âmbito das atividades legítimas e mediante garantias adequadas por uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais; (v) os dados

[59] *Vd.* DUARTE, Tatiana, "Anotação ao artigo 9.º" in *Comentário ao Regulamento Geral de Proteção de Dados*, Almedina, 2018, p.236-334, p.244, "no âmbito do tratamento de dados sensíveis, o consentimento assume duas feições: a de fundamento jurídico e a de condição de licitude de tratamento. (…) Algumas das exceções à proibição do tratamento de dados sensíveis consagradas no n.º 2 do artigo 9.º do RGPD constituem o resultado de ponderação do legislador comunitário entre direitos, ou interesses juridicamente relevantes e o risco implicado no tratamento destas categorias especiais de dados. Essas ponderações, resolvidas a favor do tratamento de dados, em virtude da preponderância de um direito ou interesse em face do risco inerente ao tratamento, constituem fundamento de licitude".

pessoais tenham sido tornados públicos pelo seu titular; (vi) se o tratamento de dados for necessário à declaração, exercício ou defesa de um direito num processo judicial ou sempre que os tribunais atuem no exercício da sua função jurisdicional; (vii) se o tratamento for necessário por motivos de interesse público importante; (viii) se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistema e serviços de saúde ou de ação social; (ix) se o tratamento for necessário por motivos de interesse público no domínio da saúde pública; (x) se o tratamento for necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos.

Do elenco apresentado, destacamos as condições de licitude que no contexto particular da investigação clínica poderão aplicar-se com mais frequência, quer em relação aos dados pessoais de categorias gerais, quer relativamente aos dados pessoais de categorias especiais: consentimento do titular dos dados, exercício de funções de interesse público («importante» ou «no domínio da saúde pública») e interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiro. Contudo, é necessário sublinhar que todas estas condições de licitude que acabamos de identificar apresentam fragilidades.

O consentimento do titular dos dados não basta que seja explícito, pois terá de respeitar todas as demais condições gerais que se encontram fixadas no n.º 11 do art. 4.º e no art. 7.º do RGPD, tendo, portanto, de corresponder a uma declaração de vontade livre, específica, informada, inequívoca e explícita[60]. Contudo, atenta a natureza desigual da relação jurídica em apreço, o estado de saúde do titular e as demais circunstâncias, poderá questionar-se (com frequência) se a declaração de

[60] CORDEIRO, A. Barreto Menezes, *O consentimento do titular dos dados no RGPD*, Blook, disponível em https://blook.pt/publications/fulltext/e772e2d8f7b4/, p.23.

vontade do titular é, efetivamente, livre e informada[61]. A este respeito, o extinto Grupo de Trabalho de Proteção de Dados do artigo 29.º (GT29) avançou, precisamente, com o exemplo do consentimento no contexto médico, demonstrando que o mesmo não pode ser livre se for obtido mediante a ameaça de não tratamento ou de tratamento de menor qualidade[62].

De qualquer modo, da leitura dos vários diplomas legais mobilizáveis, e sem prejuízo de não se verificar uma correspondência entre os conceitos de consentimento informado no contexto da investigação clínica (como condição de validade da participação) e de consentimento nos termos do RGPD (enquanto condição de licitude para o tratamento de dados), é evidente o respeito pela autodeterminação informativa, no contexto da investigação clínica[63]. Veja-se, a título de exemplo, o disposto no art. 4.º da Lei da informação genética pessoal e informação de saúde que faz depender a utilização da informação de saúde pelo sistema de saúde da autorização escrita do seu titular, e que apenas admite o acesso para fins de investigação quando a informação seja

---

[61] Cfr. COMITÉ EUROPEU PARA A PROTEÇÃO DE DADOS, *Diretrizes 05/2020 relativas ao consentimento…, op. cit.*, p.8-19. *Vd.* Tribunal de Justiça da União Europeia, Processo C129/21, Proximus NV contra Gegevensbeschermingsautoriteit, 27 de outubro de 2022; Processo C61/19, Orange Romania SA contra Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), 11 de novembro de 2020; Processo C673/17, Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV contra Planet49 GmbH, 01 de outubro de 2019; e Processo C40/17, Fashion ID GmbH & Co. KG contra Verbraucherzentrale NRW eV, 29 de julho de 2019. Sobre a questão do dever de informação, da iliteracia e da racionalidade limitada, *vd.* entre outros, DUCATO, Rossana, "Data protection, scientific research, and the role of information", *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 2020, disponível em https://doi.org/10.1016/j.clsr.2020.105412, p.13-14.

[62] Cfr. GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29.º, *Documento de trabalho sobre o tratamento de dados pessoais ligados à saúde em registos de saúde eletrónicos (RSE)*, 15 de fevereiro de 2007, p.9, "O recurso ao consentimento deve limitar-se a casos em que a pessoa em causa tenha uma liberdade de escolha genuína e possa subsequentemente retirar o consentimento sem correr riscos".

[63] No mesmo sentido, *vd.* DUARTE, Tatiana, "Anotação ao artigo 9.º" in Comentário ao Regulamento *op. cit.*, p.244, "o consentimento constitui o fundamento residual para o tratamento de dados sensíveis (…). E bem se entende que assim seja, na medida em que o consentimento se assume como a manifestação mais perfeita – por comparação às demais alternativas previstas no n.º 2 do artigo 9.º – do direito à autodeterminação".

anonimizada, ou seja, quando deixe de ser considerada um dado pessoal. Do mesmo modo, o art. 31.º da LERGPD dedica o seu n.º 4 ao consentimento relativo ao tratamento de dados para fins de investigação científica e aconselha a anonimização ou a pseudonimização dos dados sempre que os fins visados pela investigação possam ser atingidos por uma dessas vias.

5.1. Diferenças entre entidades públicas e entidades privadas?[64]

O interesse público poderá figurar como condição de licitude do tratamento de dados, embora o texto legal empregue, a respeito do tratamento de dados de categorias especiais, o conceito de «interesse público importante» e, numa outra condição, circunscreva o interesse público ao domínio da saúde pública.

No que respeita aos interesses legítimos, quando estejam em causa interesses legítimos sobreponíveis aos direitos fundamentais dos titulares de dados, suscitam-nos as maiores reservas quando os mesmos pertençam a terceiros, concretamente a entidades privadas com escopo lucrativo (*v.g.* farmacêuticas, fabricantes de dispositivos médicos), pese embora não possamos deixar de admitir (em tese) a sua invocação em determinados casos[65].

Deste modo, após tecermos várias considerações de caráter genérico relativamente às condições de licitude do tratamento de dados pessoais usualmente empregues no contexto da investigação clínica, cremos que se afigura conveniente clarificar algumas ideias relativamente à sua aplicabilidade concreta, no sentido de podermos responder

[64] Sobre a temática, em particular sobre a divergência de regime entre os diferentes Estados-Membros, *vd.* IGLÉSIAS, Filipa; PEREIRA, André Dias, "O uso secundário de dados pessoais de saúde…, *op. cit.*, p.23-24; e ainda MARTÍN URANGA, Amelia, "Protección de datos y fomento de la investigación científica…, *op. cit.*, p.1227-1228.

[65] Sobre as dificuldades na admissão desta condição de licitude, *vd.*, entre outros, QUINN, Paul, "Research under the GDPR – a level playing field for public and private sector research?", *Life Sciences, Society and Policy*, 17:4, 2021, disponível em https://doi.org/10.1186/s40504-021-00111-z, p.27-29.

à seguinte questão: a investigação clínica levada a cabo por pessoas de direito privado desenvolve-se nos mesmos moldes que a investigação clínica realizada por pessoas de direito público (sobretudo pelos interesses que estão presentes num e noutro caso)?

Em primeiro lugar, o tratamento de dados pessoais no âmbito da investigação clínica por cumprimento de obrigação legal, pelas pessoas de direito privado, parece, em abstrato, consubstanciar uma ingerência eventualmente excessiva do legislador na esfera jurídica das mesmas, colocando em causa a livre iniciativa económica e a autonomia privada que as caracteriza[66].

Em segundo lugar, as pessoas de direito privado não prosseguem, por natureza, o interesse público. Por esta razão, quando procuramos enquadrar o tratamento de dados nas condições de licitude elencadas no art. 6.º, teremos de excluir, por princípio, a aplicabilidade da alínea e)[67]. Restam, assim, as hipóteses elencadas nas alíneas a), b), d) e f).

No entanto, quando estivermos perante um tratamento de dados de categorias especiais e, portanto, perante a necessidade de preencher uma

---

[66] A nossa afirmação é dirigida ao estudo/investigação propriamente dita e às respetivas operações de tratamento que lhe estão associadas, e não às obrigações procedimentais prescritas por lei, que decorrem da concretização/operacionalização do estudo, onde, obviamente, o cumprimento de uma obrigação legal poderá servir de fundamento a tal operação de tratamento. No entanto, esse fundamento (cumprimento de obrigação legal) não servirá de base às demais operações de tratamento levadas a cabo nesse estudo.

Neste sentido, *vd.* COMITÉ EUROPEU PARA A PROTEÇÃO DE DADOS, *Diretrizes 05/2020 relativas ao consentimento…, op. cit.*, p.35, onde se assinala que "O artigo 6.º, n.º 1, alínea c), também pode ser aplicável a partes das operações de tratamento especificamente exigidas por lei". Veja-se, a título de exemplo, o que acontece no domínio dos ensaios clínicos, no que concerne nomeadamente às obrigações de comunicação relevantes para a segurança dos participantes no ensaio (artigo 53.º do Regulamento Ensaios Clínicos). No mesmo sentido, *vd.* CALDEIRA, Cristina, "A proteção de dados pessoais, a investigação científica e as transferências internacionais: os códigos de conduta e procedimentos de certificação", in *Direito da Sociedade do Conhecimento*, Volume I: Estudos na Área do Direito, Universidade Europeia, 2019/2020, 284-319, disponível em https://www.europeia.pt/resources/media/documents/direito_da_sociedade_do_conhecimento_vol1.pdf, p.296.

[67] A regra que aqui enunciamos considera a natureza destas entidades, embora não se deva ignorar a possibilidade de estas poderem, em determinados contextos, contribuir para a realização do interesse público, designadamente através das parcerias público-privadas.

condição de licitude do art. 9.º, não encontramos disposições semelhantes às previstas nas alíneas b) e f) do n.º 1 do art. 6.º.

Neste contexto em particular, apenas vislumbramos possível lançar mão, consoante o caso, das hipóteses previstas nas alíneas a), c)[68], e) e j) do n.º 2 do art. 9.º, porquanto as restantes alíneas não se mostram compatíveis com o âmbito da investigação clínica. A título excecional, a aplicação das alíneas g) e i) também poderá mostrar-se adequada, quando as entidades públicas, a quem por natureza e por princípio incumbe a prossecução do interesse público, tenham legitimado tal tratamento pelas pessoas de direito privado, uma vez que o conceito de interesse público não pode, no nosso modesto entendimento, ser preenchido e determinado pelas pessoas de direito privado.

No entanto, quando a investigação clínica seja desenvolvida por pessoas de direito público, que estejam incumbidas de desenvolver atividades de investigação, formação e ensino, o leque de condições de licitude que poderão justificar o tratamento de dados pessoais, de categorias gerais e de categorias especiais, será mais abrangente, já que incluirá também, por princípio, as hipóteses previstas na alínea c) e e) do n.º 1, do art. 6.º, bem como as alíneas g) e i) do n.º 2 do art. 9.º, que atrás excluímos (em termo gerais) do contexto de tratamento de dados levado a cabo por pessoas de direito privado. No entanto, temos de excluir a alínea f) do n.º 1 do art. 6.º (quando esteja em causa a atuação de uma autoridade pública), nos termos do disposto no art. 6.º, *in fine*, bem como a alínea b).

[68] Sobre o conceito de interesses vitais, *vd.* GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29.º, *Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/CE*, 844/14/EN, WP217, 09 de abril de 2014. Em particular neste contexto da investigação clínica, poderá questionar-se se o perigo para os interesses vitais é emergente ou não. Acompanhamos de perto a leitura preconizada por DUARTE, Tatiana, "Anotação ao artigo 9.º" in *Comentário ao Regulamento op. cit.*, p.255, no sentido de se considerar quer um perigo imediato, quer um perigo previsível (com um grau de probabilidade relevante).

5.2. O "consentimento ético" vs. o consentimento para efeitos de tratamento de dados

A lei da investigação clínica refere-se, frequentemente, ao conceito de «consentimento informado»[69], sendo que o mesmo representa nesse contexto, "a decisão expressa de participar num estudo clínico, tomada livremente por uma pessoa dotada de capacidade de o prestar ou, na falta desta, pelo seu representante legal, após ter sido devidamente informada sobre a natureza, o alcance, as consequências e os riscos do estudo, bem como o direito de se retirar do mesmo a qualquer momento, sem quaisquer consequências, de acordo com as orientações emitidas pela Comissão de Ética Competente (CEC), que devem incluir a definição do meio adequado de o prestar, o qual deve ser escrito, sempre que aplicável"[70].

Com efeito, estabelece-se como condição mínima de proteção dos participantes no estudo clínico, entre outras, a obtenção pelo investigador do consentimento informado[71]. Este consentimento prestado pelo participante pode, contudo, ser revogado a qualquer momento, sem necessidade de observar qualquer forma especial (podendo ser expressa ou tácita) e sem que desse ato possa resultar qualquer responsabilidade do participante. Não obstante, nos estudos clínicos sem intervenção prevê-se a possibilidade de a CEC, a título excecional e de forma fundamentada, vir a dispensar o consentimento[72], inclusive

---

[69] *Vd.*, entre outros, OSSWALD, Walter, "Limites do Consentimento Informado", in *Estudos de Direito da Bioética*, Almedina, 2009, p.151-160, p.153, que se refere ao consentimento informado especificamente no domínio da prestação de cuidados de saúde, mas que tem aplicação direta neste contexto da investigação clínica, no sentido em que o consentimento informado "respeita a dignidade individual, afasta os riscos de fraude ou influência indevida, estimula a adoção de uma atitude racional (…) e se aproxima do ideal de participação plena". Por outro lado, o mesmo autor afirma ainda, na p.160, que "tal como outro precioso bem, a liberdade, a autonomia tem as suas limitações e será tanto mais respeitada quanto mais racional e ponderadamente for utilizada".

[70] Cfr. alínea l) do art. 2.º da LIC.

[71] Cfr. alínea d) do n.º 1 do art. 6.º e alínea c) do art. 10.º da LIC. Sobre a participação de menores e outros participantes especialmente vulneráveis, cfr. artigos 7.º e 8.º da LIC.

[72] Cfr. n.º 2 do art. 6.º da LIC.

nos casos em que participem menores ou maiores que não se encontrem em condições de prestar o seu consentimento[73]. Do ponto de vista procedimental, a CEC assume um papel de destaque no que respeita à verificação do cumprimento dos pressupostos de validade do estudo, de entre os quais consta, naturalmente, a obtenção do consentimento informado.

Nesta senda, é de sublinhar que "a realização de estudo clínico sem que o participante tenha sido previamente informado dos objetivos, riscos, inconvenientes do estudo clínico e condições em que este é realizado ou prestado o consentimento informado" constitui uma contraordenação, nos termos do disposto no art. 45.º da LIC[74].

No que respeita ao consentimento para efeitos de tratamento de dados pessoais, devemos começar por esclarecer o que se entende por consentimento nesse contexto: "manifestação de vontade, livre, específica, informada e inequívoca, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento"[75].

O consentimento figura, desde logo, como uma declaração ou ato positivo, no sentido de que deve corresponder a um comportamento ativo do titular dos dados. O silêncio ou a omissão por parte do titular dos dados não releva, assim, para este efeito, isto é, do comportamento

[73] Cfr. n.º 3 do art. 7.º e n.º 4 do art. 8.º da LIC.

[74] Note-se que da definição de consentimento informado, oferecida pela LIC, o consentimento prestado pelo participante pressupõe uma fase prévia na qual o investigador presta informações sobre a natureza, o alcance, as consequências e os riscos do estudo, e ainda sobre o direito de se retirar do mesmo a qualquer momento, sem quaisquer consequências. Pese embora a formulação legal da prescrição contraordenacional não seja totalmente coincidente com o texto da definição de consentimento informado, cremos que está presente a intenção de punir a obtenção do consentimento do participante nos casos em que não tenham sido prestadas, previamente à sua obtenção, todas as informações necessárias para que se possa considerar o mesmo verdadeiramente informado, bem como a falta de obtenção (pela forma prescrita) do consentimento ainda que tenham sido prestadas as informações necessárias ao participante.

[75] Cfr. n.º 11 do art. 4.º do RGPD. Sobre as críticas que podem ser erigidas ao consentimento para o tratamento de dados, *vd.* CORDEIRO, A. Barreto Menezes, *O consentimento do titular(...)*, *op. cit.*, p.3-5.

passivo do titular não se pode retirar a ilação de que a sua vontade é consentir no tratamento dos seus dados pessoais[76].

Em segundo lugar, o consentimento deve ser livre, ou seja, o titular dos dados deve poder decidir se o presta ou não, sem que a sua decisão possa, de algum modo, ser manipulada ou influenciada. Conforme reconhece o Comité Europeu para a Proteção de Dados (CEPD): "Regra geral, o RGPD prevê que se o titular dos dados não puder exercer uma verdadeira escolha, se sentir coagido a dar o consentimento ou sofrer consequências negativas caso não consinta, então o consentimento não é válido"[77].

Em terceiro lugar, para que o consentimento seja específico, deverá respeitar-se a(s) finalidade(s) para a(s) qual(is) o mesmo é recolhido[78]. Este requisito de validade do consentimento reclama, contudo, prudência. Senão vejamos: de acordo com o CEPD, o responsável pelo tratamento de dados deve procurar a (i) especificação em função da finalidade como salvaguarda contra o desvirtuamento da função, (ii) a granularidade nos pedidos de consentimento, e (iii) a separação clara entre as informações relacionadas com a obtenção de consentimento para atividades de tratamento de dados e as informações sobre outras questões[79]. Por outro lado, não raras vezes, no contexto da investigação clínica, o responsável pelo tratamento de dados não se encontra, *ab initio*, ciente da totalidade das finalidades do tratamento de dados pessoais[80], sobretudo pela complexidade ou pela novidade do objeto de estudo, pelo

[76] Cfr. Considerando 32 do RGPD, "O consentimento pode ser dado validando uma opção ao visitar um sítio web na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento."

[77] COMITÉ EUROPEU PARA A PROTEÇÃO DE DADOS, *Diretrizes 05/2020 relativas ao consentimento…, op. cit.*, p.8.

[78] Cfr. Considerando 32 do RGPD, "O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. (…) Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins."

[79] COMITÉ EUROPEU PARA A PROTEÇÃO DE DADOS, *Diretrizes 05/2020 relativas ao consentimento…, op. cit.*, p.15 e ss.

[80] Cfr. Considerando 33 do RGPD.

surgimento de novos desenvolvimentos ao longo do estudo, pela descoberta de outros interesses em virtude do avanço alcançado até então, entre outras causas. Atenta essa realidade, a LERGPD previu, no n.º 4 do art. 31.º, a possibilidade de o titular dos dados oferecer o seu consentimento para determinadas áreas de investigação ou partes de projetos. Ainda assim, esta possibilidade não deve ser encarada como um desvio ao princípio da limitação das finalidades, sob pena de se defraudar as legítimas expectativas do titular dos dados, razão pela qual o critério da granularidade assume particular destaque neste contexto[81].

Em quarto lugar, o consentimento deve ser informado, o que faz recair sobre o responsável pelo tratamento de dados um dever de informação prévia (completa, verdadeira, atual, clara e objetiva[82]) sobre os termos em que se processará o tratamento de dados pessoais.

Em quinto lugar, o consentimento deve traduzir-se numa declaração de vontade inequívoca, ou seja, "tem de ser óbvio que o titular dos dados deu o consentimento para o tratamento em causa"[83], embora tal requisito nem sempre exija que o consentimento seja expresso.

Ademais, o legislador europeu, ciente dos riscos (para os direitos e liberdades fundamentais do titular dos dados) a que se encontram expostos alguns tipos de dados pessoais, atenta a sua natureza sensível, consagrou um regime diferenciado, mais exigente e mais específico, relativamente àquele que é conferido aos dados pessoais em geral, adicionando um requisito de validade ao consentimento – *o caráter*

---

[81] *Vd.* COMITÉ EUROPEU PARA A PROTEÇÃO DE DADOS, *Diretrizes 05/2020 relativas ao consentimento…, op. cit.*, p.36, "Considerando as condições apertadas do artigo 9.º do RGPD, relativo ao tratamento de categorias especiais de dados, o CEPD refere que, quando as categorias especiais de dados são tratadas com base no consentimento explícito, a aplicação da flexibilidade do considerando 33 ficará sujeita a uma interpretação mais restritiva e exigirá um nível mais elevado de escrutínio. Quando considerado no seu todo, o RGPD não pode ser interpretado como um ato que permite a um responsável pelo tratamento contornar o princípio-chave da especificação das finalidades em relação às quais solicita o consentimento do titular dos dados."

[82] CORDEIRO, A. Barreto Menezes, *O consentimento do titular…*, *op. cit.*, p.20.

[83] *Vd.* COMITÉ EUROPEU PARA A PROTEÇÃO DE DADOS, *Diretrizes 05/2020 relativas ao consentimento…, op. cit.*, p.20.

explícito[84]. É precisamente o que se verifica com os dados de categorias especiais – aqueles que habitualmente suscitam maior interesse no domínio da investigação clínica. Nestes casos será necessário que o titular expressamente manifeste a sua vontade de consentir no tratamento dos seus dados pessoais[85].

Atento o exposto, o "consentimento ético" exigido no âmbito da investigação clínica não se confunde com o consentimento exigido para efeitos de tratamento de dados no âmbito do RGPD[86], pese embora a sua convivência seja possível e desejável em várias situações. Ainda assim, estes consentimentos não se substituem entre si, mas nada obsta a que, por exemplo, desde que devidamente individualizados e formalizados, possam figurar num mesmo documento escrito disponibilizado ao titular dos dados com toda a informação necessária à formulação e posterior manifestação de uma vontade de consentir na participação no estudo clínico e no tratamento de dados pessoais necessário para o efeito.

6. A compressão dos direitos dos titulares dos dados no contexto da investigação clínica

Conforme assinala Graça Canto Moniz[87], "É inegável que a vontade do titular dos dados ocupa um lugar de relevo (…). Reflexo disso é o princípio, não enunciado no artigo 5.º do RGPD, da *participação* do titular dos dados nos tratamentos".

O art. 12.º do RGPD é responsável por definir as regras e limites gerais atinentes ao exercício dos direitos dos titulares dos dados. Não

[84] COMITÉ EUROPEU PARA A PROTEÇÃO DE DADOS, *Diretrizes 03/2020 sobre o tratamento de dados relativos à saúde…*, *op. cit.,* p.7.

[85] Como é consabido, o caráter expresso da declaração de vontade de consentir não tem, necessariamente, de se traduzir numa declaração escrita. A este respeito, *vd.* COMITÉ EUROPEU PARA A PROTEÇÃO DE DADOS, *Diretrizes 05/2020 relativas ao consentimento…, op. cit.*, p.23-25.

[86] *Ibidem*, p.35.

[87] MONIZ, Graça Canto, *Manual de Introdução à Proteção de Dados Pessoais*, *op. cit.*, p.169.

obstante, estando em causa o tratamento de dados pessoais para fins de investigação clínica, os direitos dos titulares poderão sofrer limitações específicas, plasmadas nos art. 14.º, 15.º, 17.º e 21.º do RGPD.

O considerando 62 e a alínea b) do n.º 5 do art. 14.º compreendem um enfraquecimento da obrigação de prestar informação ao titular dos dados, nomeadamente quando esteja em causa um tratamento para fins de investigação científica, considerado o número de titulares de dados, a antiguidade dos dados e as devidas garantias que tenham sido adotadas.

O n.º 4 do art. 15.º salvaguarda os direitos e liberdades de terceiros, na medida em que prevê a possibilidade de se vedar ao titular o direito de obter uma cópia dos dados que se encontrem em fase de tratamento.

Por sua vez, a alínea d) do n.º 3 do art. 17.º prevê a compressão do direito ao apagamento dos dados, quando tal se afigure impossível ou prejudique gravemente a obtenção dos objetivos desse tratamento.

Por fim, o n.º 6 do art. 21.º, relativo ao direito de oposição, impõe limites à oposição quando a investigação tenha em vista a prossecução do interesse público.

Para além das situações aqui elencadas, que na verdade resultam do texto legal do RGPD, o legislador europeu concedeu aos Estados Membros a possibilidade de estabelecerem derrogações aos direitos dos titulares de dados, previstos nos art. 15.º, 16.º, 18.º e 21.º, ainda que sob a reserva das condições e garantias previstas no n.º 1 do art. 89.º, para os casos em que tal exercício seja suscetível de tornar impossível ou de prejudicar gravemente a realização dos fins em apreço. A LERGPD consagrou, assim, no seu n.º 2 do art. 31.º uma referência à limitação destes direitos. No entanto, conforme assinala Francisco Paes Marques[88], "A lei apenas se limita a prever o mínimo denominador comum em matéria de derrogações (…) admitidas nos n.os 2 e 3 do art. 89.º do RGPD,

[88] Cfr. MARQUES, Francisco Paes, "Anotação ao artigo 31.º da LERGPD", in *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, Almedina, 2021, p.627-629, p.628.

não estabelecendo as diferenciações contidas nessas normas. O legislador renuncia à competência que lhe é conferida, inibindo-se de aprovar normas específicas que traduzam uma ponderação dos fins em causa e dos direitos dos titulares dos dados".

De qualquer modo, toda a limitação aos direitos dos titulares implicará uma maior responsabilidade para o responsável pelo tratamento de dados.

7. Síntese conclusiva

A investigação clínica, que tem como desiderato descobrir ou a verificar a distribuição ou o efeito de fatores de saúde, de estados ou resultados em saúde, de processos de saúde ou de doença, do desempenho e/ou segurança de intervenções ou da prestação de cuidados de saúde, assume um papel primordial no setor da saúde. No entanto, é imperioso conjugar os diplomais legais responsáveis por regular os termos em que a investigação clínica é efetuada com aqueles que pugnam pela proteção de dados pessoais. O exemplo mais recente e desafiante no contexto europeu é a criação do Espaço Europeu de Dados de Saúde.

Do quadro legal referente à proteção de dados pessoais resulta a regra geral da proibição de tratamento de dados pessoais de categorias especiais, como sejam os dados relativos à saúde. No entanto, uma vez que a investigação clínica se alimenta de dados pessoais e, em especial, de dados de categorias especiais, encontram-se previstas várias exceções que autorizam o tratamento desses dados pessoais, designadamente para efeitos de investigação científica, embora em moldes diversos. De qualquer modo, em ambos os casos serão aplicáveis os princípios gerais a que alude o art. 5.º do RGPD, que impõem que o tratamento de dados pessoais seja realizado de forma lícita, leal e transparente, para finalidades determinadas, explícitas e legítimas, seguro e baseado em dados adequados, pertinentes e limitados ao necessário, exatos e atualizados e conservados limitadamente.

No que concerne às condições de licitude do tratamento de dados (gerais e especiais) no contexto da investigação clínica torna-se necessário conjugar a aplicação do art. 6.º com a aplicação do art. 9.º do RGPD, a qual é fortemente influenciada pela natureza das entidades que levam a cabo tais atividades de investigação. Das condições de licitude que no contexto particular da investigação clínica poderão aplicar-se com mais frequência, quer em relação aos dados pessoais de categorias gerais, quer relativamente aos dados pessoais de categorias especiais destacam-se o consentimento do titular dos dados, o exercício de funções de interesse público («importante» ou «no domínio da saúde pública») e os interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiro. Contudo, todas estas condições de licitude apresentam fragilidades.

O tratamento de dados pessoais no âmbito da investigação clínica por pessoas de direito privado poderá basear-se nas alíneas a), b), d) e f) do art. 6.º, assim como nas alíneas a), c), e) e j) do n.º 2 do art. 9.º. A alínea c) do art. 6.º embora não sirva de base ao estudo propriamente dito, poderá no âmbito da sua realização impor-se relativamente a determinadas operações de tratamento que decorrem da concretização/operacionalização do estudo. Por seu turno, as alíneas g) e i) poderão também aplicar-se, ainda que a título excecional, quando as entidades públicas tenham legitimado tal tratamento pelas pessoas de direito privado, uma vez que o conceito de interesse público não pode, no nosso modesto entendimento, ser preenchido e determinado pelas pessoas de direito privado.

No entanto, quando a investigação clínica seja desenvolvida por pessoas de direito público, que estejam incumbidas de desenvolver atividades de investigação, formação e ensino, o leque de condições de licitude que poderão justificar o tratamento de dados pessoais, de categorias gerais e de categorias especiais, será mais abrangente, já que incluirá também, por princípio, as hipóteses previstas na alínea c) e e) do n.º 1, do art. 6.º, bem como as alíneas g) e i) do n.º 2 do art. 9.º. No entanto, temos de excluir a alínea b), bem como a alínea f) do n.º 1 do art. 6.º (quando esteja em causa a atuação de uma autoridade pública) nos termos do disposto no art. 6.º, *in fine*.

No que concerne concretamente ao consentimento, impõe-se a distinção clara entre o "consentimento ético" exigido no âmbito da investigação clínica e o consentimento exigido para efeitos de tratamento de dados no âmbito do RGPD, pese embora a sua convivência seja possível e desejável em várias situações. Estes consentimentos não se substituem entre si, mas nada obsta a que possam figurar num mesmo documento, de forma clara e individualizada, disponibilizado ao titular dos dados, com toda a informação necessária à formulação e posterior manifestação de uma vontade de consentir na participação no estudo clínico e no tratamento de dados pessoais necessário para o efeito.

O regime legal da proteção de dados pessoais prevê ainda a compressão de alguns direitos dos titulares dos dados: limites gerais que resultam do art. 12.º do RGPD e limites específicos plasmados nos art. 14.º, 15.º, 17.º e 21.º do RGPD. Concomitantemente, o legislador europeu concedeu aos Estados Membros a possibilidade de estabelecerem derrogações aos direitos dos titulares de dados, previstos nos art. 15.º, 16.º, 18.º e 21.º, ainda que sob a reserva das condições e garantias previstas no n.º 1 do art. 89.º, para os casos em que tal exercício seja suscetível de tornar impossível ou de prejudicar gravemente a realização dos fins em apreço. Não obstante, a LERGPD apesar de se referir, no n.º 2 do art. 31.º, à limitação destes direitos, fá-lo sem concretizar, adequadamente, a medida e os termos dessa compressão.

Em suma, a adoção do Regulamento Geral sobre a Proteção de Dados representou uma reviravolta significativa nos quadros jurídicos que regulam a proteção de dados, o que contribuiu para o reforço da confiança e segurança dos cidadãos na União. No entanto, a aspiração da União em participar no mercado digital, por um lado, e a relevância do acesso seguro e protegido aos dados de saúde pública e de cuidados de saúde para além das fronteiras de cada Estado, por outro lado, conduziram a União a apresentar uma proposta de criação de um espaço europeu de dados de saúde. Todavia, sem se perceber se norteada pelo altruísmo ou se antes pelo economicismo dos dados, a União Europeia

parece vacilar quanto introduz, nas linhas de atuação voltadas para o contexto do mercado único de dados, uma ideia de utilização massiva de dados de saúde.