Lex Medicinae

Revista Portuguesa de Direito da Saúde

Ano 21 - n.º 41 - 2024
Publicação Semestral
Edição Gratuita

Centro de Direito Biomédico

Lex Medicinae

Revista Portuguesa de Direito da Saúde

INSTITVTO IVRIDICO
FACULDADE DE DIREITO
UNIVERSIDADE DE COIMBRA

Área de investigação "Vulnerabilidade e Direito" / Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra, integrada no Projecto "Desafios sociais, incerteza e direito" (UIDB/04643/2020)

Research area "Vulnerability and Law" / Legal Institute of the Faculty of Law of the University of Coimbra, integrated in the Project "Social challenges, uncertainty and law" (UIDB/04643/2020)

FCT Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA EDUCAÇÃO E CIÊNCIA

Ficha Técnica

Propriedade da Revista (Morada da Redação)
Centro de Direito Biomédico
Faculdade de Direito da Universidade de Coimbra
3004-528 Coimbra
Telef./Fax: 239 821 043
cdb@fd.uc.pt
www.centrodedireitobiomedico.org

Editor
Instituto Jurídico | Faculdade de Direito da Universidade de Coimbra | 3004-528 Coimbra

Lex Medicinae
Revista Portuguesa de Direito da Saúde
Ano 21 - n.º 41 - janeiro/junho 2024
Publicação Semestral

Execução gráfica
Ana Paula Silva

NIPC 504 190 490
ISSN 1646-0359
N.º de Registo ERC 127770

O Centro de Direito Biomédico, fundado em 1988, é uma associação privada sem fins lucrativos, com sede na Faculdade de Direito da Universidade de Coimbra, que se dedica à promoção do direito da saúde entendido num sentido amplo, que abrange designadamente, o direito da medicina e o direito da farmácia e do medicamento. Para satisfazer este propósito, desenvolve acções de formação pós-graduada e profissional; promove reuniões científicas; estimula a investigação e a publicação de textos; organiza uma biblioteca especializada; e colabora com outras instituições portuguesas e estrangeiras.

Doutrina

SISTEMAS DE VIDEOVIGILÂNCIA EM ESPAÇOS PRIVADOS E CENTROS RESIDENCIAIS PARA IDOSOS.
QUESTÕES RELACIONADAS COM O TRATAMENTO DE DADOS PESSOAIS [1] [2]

Yolanda Bustos Moreno
Professora Titular de Direito Civil · Universidade de Alicante

1. Contextualização

O atual problema habitacional, ligado às necessidades de alojamento de determinados grupos vulneráveis[3], faz com que em muitos casos não seja possível usar todas as divisões de uma residência, sendo necessário recorrer a fórmulas ocupacionais partilhadas com outras pessoas, inclusive com o proprietário do imóvel. Noutros casos, cada vez mais frequentes devido ao envelhecimento da população, será necessário viver em "comunidade" por razões de cuidado e de dependência obrigatória de cuidados externos através de diferentes recursos, como o alojamento colaborativo ou supervisionado, ou através da admissão em centros residenciais específicos para estas situações[4].

Neste contexto, quando uma pessoa partilha a sua casa, é inevitável que surjam problemas de coabitação com interferências na sua esfera privada. Imaginemos a instalação de um sistema de videovigilância no interior de uma casa, por aparentes razões de segurança, que o proprietário decide unilateralmente antes de arrendar a habitação que continuará a ser a sua residência[5] . Como podemos antecipar, a Agência Espanhola de Proteção de Dados (AEPD) determinou que, quando se cede o uso de um anexo ou de um quarto a um terceiro, em princípio não se pode instalar uma câmara no

[1] Originalmente publicado em "Sistemas de videovigilancia en espacios privados y centros residenciales de personas mayores. Problemática en torno al tratamiento de datos personales", *El Derecho civil ante los retos actuales de la vulnerabilidad personal*, Mayor del Hoyo, M. V. y De Salas Murillo, S. (directoras), ed. Aranzadi, 2024, pp. 209-228. A versão que agora se publica foi traduzida por Diogo Soares Oliveira, Monitor na Faculdade de Direito da Universidade de Coimbra e Investigador do Centro de Direito Biomédico.

[2] Realizado no âmbito do Proyecto de Investigación del Ministerio de Ciencia e Innovación PID 2022-1398990B-100 «Nuevos desafíos del Derecho Biomédico en la protección jurídico-civil de las personas mayores», IIPP E. Algarra y J. Barceló; e do Proyecto ICAR (Centro Internacional para la Investigación del Envejecimiento) «Derecho a la salud, personas mayores y autonomía personal: las nuevas bases del consentimiento informado», IIPP E. Algarra y J. Barceló.

[3] Em relação ao conceito legal indeterminado de *vulnerabilidade* e aos grupos de pessoas cujas circunstâncias podem causar emergência ou exclusão social, beneficiários das medidas estatais previstas para o acesso à habitação, incluímos na definição daquele o "tipo de fragilidade material ou moral a que o indivíduo está exposto, que o impede de exercer adequadamente os seus direitos, ou que o coloca numa situação de inferioridade ou desequilíbrio, tornando-o merecedor de proteção". As condições de "emergência ou exclusão social" podem ser entendidas como "aquelas que podem afetar famílias com menores, idosos dependentes, pessoas com deficiência, vítimas de violência de género ou desempregados sem direito a prestações". Quanto ao primeiro conceito, NUÑEZ IGLESIAS, A., "La suspensión de los lanzamientos en la ejecución hipotecaria", *La protección del deudor hipotecario. Aproximación a la Ley de Medidas para reforzar la protección a los deudores hipotecarios, reestructuración de deuda y alquiler social*, in Núñez Iglesias, A. (dir.), Granada, Comares, 2014, p. 201. Em relação à segunda definição, ARGELICH COMELLES, C. "Acceso a la vivienda para personas vulnerables, COVID-19, Ley 4/2022 y Real Decreto-ley 3/2022: suspensión de los lanzamientos y medidas estatales y autonómicas (1)", *Actualidad Civil*, n.3, março de 2022, p. 3.

[4] Relativamente a estas modalidades de habitação partilhada, remetemos para outro trabalho que publicaremos em breve.

[5] Caso resolvido no processo n.º EXP202207199 AEPD. EXP202207199 AEPD, para o qual remetemos de *seguida*.

interior do imóvel arrendado sem que exista uma base legitimadora para tal, como o consentimento, e sem que existam razões proporcionais à finalidade de segurança contra esse tratamento invasivo, entre outras condições[6].

Por sua vez tem sido debatida a legalidade da instalação de câmaras nos locais de trabalho, diferenciando-a dos espaços que podem ser considerados excluídos devido a actividades de higiene pessoal ou de descanso, e que acabou por ser regulamentada na Lei Orgânica 3/2018, de 5 de dezembro, sobre a Proteção de Dados Pessoais e Garantia dos Direitos Digitais (doravante, LOPDPGDD) nos termos que explicaremos. No entanto, abordaremos apenas superficialmente este tipo de tratamento de dados pessoais, mais especificamente a respeito da posição dos trabalhadores durante a sua prática profissional de assistência a pessoas dependentes em centros residenciais videomonitorizados.

De um ponto de vista positivo, é verdade que o acompanhamento através das chamadas "tecnologias sociais" traz benefícios indiscutíveis no domínio da saúde e ajuda a ultrapassar a dependência. Os cuidados de saúde estão a tornar-se cada vez mais digitalizados e certos sistemas que envolvem *software* avançado (ou a utilização de inteligência artificial) permitem monitorizar a atividade, os sinais vitais ou o sono, com a ajuda da domótica, o que também facilitará a permanência dos idosos em casa. A robótica de assistência monitorizará os sinais vitais através de diferentes sensores e actuará também como um companheiro para, pelo menos, aliviar a solidão indesejada. Entre outros salientamos o desenvolvimento de cadeiras de rodas automatizadas, a vigilância por reconhecimento facial para controlo de presenças, a segurança das casas de banho ou ainda os transmissores de ordens orais para a toma de medicamentos, que são já uma realidade[7].

No entanto, esta tecnologia capta imagens e, por vezes, sons de pessoas singulares, o que pode implicar uma invasão da esfera pessoal reservada à máxima privacidade[8] mesmo quando se trata de ajudar a pessoa em caso de deficiência de memória, através de aplicações de geolocalização[9].

Desta forma, os princípios aplicáveis de prote-

[6] Pensando no desconforto que o inquilino pode sentir ao ser gravado na sua própria casa, mesmo em espaços comuns como a cozinha ou o corredor, retomamos a reflexão que INTXAURTIETA MADARIAGA nos transmite com acuidade, citando o acórdão de 15 de dezembro de 1983 do Tribunal Constitucional Federal Alemão, sobre a Lei do Recenseamento da População de 4 de março de 1982. Este autor afirma que não se trata apenas de afetar a privacidade ou a própria imagem, mas que a consciência de estar a ser gravado e observado pode afetar a vontade dos indivíduos e inibir o exercício de outros direitos, "La adaptación del tratamiento de imágenes y la videovigilancia a los principios del Reglamento General de Protección de Datos (Comentario al artículo 22 LOPDGDDD)", cap. 154, *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales*, T. II, Troncoso Reigada, A. (coord.), Cizur Menor (Navarra), Civitas Thomson Reuters, 2021, p. 3677.

[7] Como refere ARIZA RODRÍGUEZ, F. "El derecho al servicio de los ciudadanos ante el desafío de la vejez y el envejecimiento", Posfacio, *Tratado de Derecho y Envejecimiento. La adaptación del Derecho a la nueva longevidad*, ROMEO CASABONA, C.M. (coord..), Fundación Mutualidad Abogacía- Wolters Kluwer, 2021, p. 936.

[8] Neste sentido, INTXAURTIETA MADARIAGA é de opinião que as possibilidades proporcionadas pelos avanços tecnológicos, bem como a progressiva implementação de um conceito cada vez mais laxista da própria privacidade, favorecem o crescimento constante e, de momento, imparável deste tipo de tratamento de dados, *op. cit.*

[9] A geolocalização, entendida como a tecnologia que permite localizar um dispositivo num ponto espacial com base na transmissão das suas coordenadas de posicionamento, implica possíveis riscos na esfera da privacidade pessoal da pessoa singular. Quando os dados de posicionamento de um terminal são ligados aos da pessoa que o possui para conhecer pormenores da vida das pessoas, criam-se assim "padrões pessoais de comportamento" que rompem as barreiras do que representa a ideia de privacidade, a partir de uma reconfiguração da identidade e da personalidade do ser humano, através de dados interligados. É por isso que a AEPD está a receber um número crescente de processos sobre a eventual violação da privacidade dos indivíduos em resultado da utilização da geolocalização. O próprio TEDH, no caso Uzún *vs* Alemanha, 2-9-2010 (processo 35625/05), concluiu que a geolocalização contínua afecta a privacidade, BATUECAS CALETRÍO, A. seguindo Barinas Ubiás, "Intimidad personal, protección de datos personales y geolocalización", *Derecho Privado y Constitución, n.* 29, janeiro-dezembro 2015, p. 50-51.

ção de dados pessoais, como a proporcionalidade, a necessidade e a intervenção mínima, entre outros, e a existência de uma base jurídica que justifique o tratamento de dados de imagem através da videovigilância são do maior interesse, na aplicação do 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 e que revoga a Diretiva 95/46/CE (doravante, RGPD) e a LOPDPGDD, como principal (mas não exclusivamente aplicável) regulamento na análise das invasões de privacidade que iremos expor. Tratam-se, na sua maioria, de casos reportados à AEPD, bem como apreciados pela *Autoridade Sueca de Proteção de Dados*, a qual, por sua vez, tem especial interesse para a *Commission Nationale de l'Informatique et des Libertés* (CNIL) francesa no sentido que passaremos a explicar[10].

Um caso particularmente problemático **é** a situação das pessoas idosas em lares residenciais. Este grupo requer garantias adicionais também no que diz respeito à proteção de dados quando vivem nestas instalações ou em centros de dia, pelo que é necessário analisar a forma de conformar as disposições do RGPD e da LOPDPGDD. Normalmente as residências têm um circuito interno de vigilância para assegurar que nada acontece nas instalações. Embora, *prima facie*, a gravação possa ser permitida nas áreas comuns, tal não será o caso em instalações privadas como casas de banho ou quartos, como explicaremos. Trata-se de um espaço privado, onde o direito à privacidade prevalece sobre as alegadas necessidades de segurança.

No entanto, na prática, surgem situações complexas, como quando os próprios familiares solicitam a instalação de sistemas de videovigilância para poderem verificar os cuidados recebidos pelos seus familiares face a suspeitas de maus tratos por parte do pessoal dos centros. Tendo em conta a mediatização destas situações relatadas em França nos lares de idosos dependentes (EHPAD), a CNIL publicou recentemente (9 de fevereiro de 2023) um projeto de recomendação sobre a instalação de dispositivos *de videovigilância nos* quartos dos lares de idosos (*Mise en place de dispositifs de vidéosurveillance au sein des chambres des EHPAD*, a seguir *Vidéosurveillance dans les chambres d'Ehpad*), documento de que daremos conta nas páginas seguintes[11] . Por outro lado, as câmaras podem destinar-se a evitar danos físicos a certas pessoas expostas a comportamentos autolesivos graves ou aos funcionários, quando este fica emocionalmente perturbado; um caso que analisaremos e que foi decidido pela *Autoridade Sueca para a Proteção de Dados*.

Estas e outras questões relacionadas são o foco central deste estudo que, no entanto, não pretende fazer uma análise exaustiva dos regulamentos de proteção de dados face a este tratamento de dados pessoais, devido a limitações óbvias de espaço. Ainda assim forneceremos informações e orientações para continuar a refletir sobre os problemas que a necessidade de habitação partilhada e de vida

[10] Como se afirma no STC 22/1984, de 17 de fevereiro, a inviolabilidade do domicílio "impõe uma extensa série de garantias e poderes, que incluem a proibição de todos os tipos de invasões, incluindo as que podem ser realizadas *sem penetração direta por meio de* dispositivos mecânicos, electrónicos e outros semelhantes", VLEX-15034676. Os itálicos são nossos.

[11] A CNIL foi convidada por várias organizações sociais e médicas a pronunciar-se sobre os problemas e a eventual legalidade da instalação de sistemas de videovigilância nos quartos dos residentes, abrindo um período de consulta pública sobre o assunto. Aguarda-se atualmente a publicação da recomendação final da CNIL, informação disponível em https://www.cnil.fr/sites/cnil/files/2023-02/projet_de_recommandation_videosurveillance_ephad.pdf. O regulamento de base é a *LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles*, e as suas sucessivas alterações, disponível em: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000037085952.

dependente continuará a gerar, devido ao aumento previsível de grupos vulneráveis que não podem suportar o custo da habitação independente e, por outro lado, ao inevitável envelhecimento da população.

No presente estudo abordamos os sistemas de videovigilância que, embora instalados *de forma contínua*[12] nestes locais, com o objetivo de garantir a segurança dessas pessoas, dos seus bens ou dos próprios edifícios, podem, no entanto, representar um atentado à privacidade ou à proteção de dados pessoais, como imagens faciais ou dados relativos à saúde, considerados "categorias especiais de dados". Para o efeito explicaremos como o "tratamento" para efeitos de videovigilância, a que se aplicam as normas de proteção de dados, será mesmo aquele em que não há conservação de dados pessoais, bastando a sua recolha ou gravação[13].

2. Regulamento

Em contraste com o crescimento da implantação social e do desenvolvimento tecnológico dos sistemas de videovigilância, a verdade é que a sua regulamentação é escassa[14]. E isto apesar de nos encontrarmos perante um dos sistemas de tratamento de dados mais invasivos e com maior impacto nos direitos humanos[15], como se detalha na secção seguinte.

Para além das implicações constitucionais, que abordamos na secção seguinte, importa referir que o artigo 22.º da Lei Orgânica n.º 3/2018, de 5 de dezembro, de Proteção de Dados Pessoais e Garantia dos Direitos Digitais (LOPDPGDD)[16], é a disposição central que visa o *tratamento para fins de videovigilância*, contendo as correspondentes referências ao Regulamento (UE) 2016/679 (RGPD), no que respeita aos requisitos para o tratamento lícito dos dados pessoais utilizados para esses fins[17]. As remissões para o RGPD, no domínio do tratamento para fins de videovigilância, ocorrem no que respeita à exceção pessoal e nacional e à aplicação do dever de informação (art. 22.º, n.ºs 4 e 5). A

[12] A definição de câmara de vigilância constante do artigo 3.º da lei sueca relativa à vigilância por câmaras, de 1 de agosto de 2018 (KBL), significa, nomeadamente, que se trata de um equipamento que, sem manobras no local, é utilizado de forma a implicar uma vigilância pessoal *permanente ou regularmente repetida*. Os itálicos são nossos.

[13] A Exposição de Motivos da Instrução da AEPD n.º 1/2006, de 8 de novembro, relativa ao tratamento de dados pessoais para fins de vigilância através de sistemas de câmaras ou de videocâmaras, aplicável na medida em que não contrarie o art. 22.º da LOPDGDD, refere que esta "visa adequar o tratamento aos critérios estabelecidos pela jurisprudência do Tribunal Constitucional ao considerar que o tratamento de dados pessoais não exige a sua conservação, sendo suficiente a sua recolha ou registo".

[14] Ao contrário do que acontece com a regulamentação da videovigilância policial, a videovigilância não policial, seja ela realizada no âmbito público ou privado, tem sido objeto de muito pouca regulamentação e de reducido alcance, o que implica um sentimento de insegurança jurídica, apesar da vontade do legislador, objeta INTXAURTIETA MADARIAGA, R., *op. cit.*, p. 3678. Vide, Lei n.º 5/2014, de 4 de abril, sobre Segurança Privada e suas disposições de aplicação, a que se refere o art. 22.º, n.º 7, da LOPDGDD.

[15] INTXAURTIETA MADARIAGA, R., *op. cit.*, p. 3677.

[16] A atual LOPDGDD é o principal regulamento interno que complementa ou desenvolve o RGPD. A referida Lei revogou a anterior LO 15/1999, de 13 de dezembro, sobre Proteção de Dados de Carácter Pessoal, decorrente da transposição para o direito espanhol da Diretiva 95/46/CE, de 24 de outubro de 1995, também revogada pelo RGPD.

[17] A Convenção Europeia dos Direitos do Homem, em 1950, apenas reconheceu genericamente (art. 8.1) o respeito pela vida privada e familiar: "toda a pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência". Posteriormente, a Convenção n.º 108 do Conselho da Europa, de 28 de janeiro de 1981 (e o seu Protocolo Adicional de 8 de novembro de 2001), relativa à proteção das pessoas singulares no que diz respeito ao tratamento automatizado de dados pessoais, veio reconhecer a proteção dos dados pessoais. A Carta dos Direitos Fundamentais da UE já reconhece separadamente o direito de cada pessoa "ao respeito pela sua vida privada e familiar" (art. 7.º) e o direito "à proteção dos dados pessoais que lhe digam respeito" (art. 8.º), uma evolução que se reflecte em MEGIAS QUIROS, J.J., "Actividades personales y domésticas excluidas del ámbito de aplicación (comentario al artículo 2.2.c) RGPD y al artículo 2.2.A) LOPDGDD , T. I, Troncoso Reigada, A. (coord.), Cizur Menor (Navarra), Civitas Thomson Reuters, 2021 p. 356, nota 2. 356, nota 2; ÁLVAREZ ALVITE, A. "El derecho a la vida privada en la doctrina del Tribunal Europeo de Derechos Humanos: un largo camino por recorrer", *Revista Aranzadi Unión Europea*, n. 5/2022

sua aplicação será direta e integral, na medida em que as imagens (e os dados de saúde) quando tratadas por meio de videovigilância devem cumprir os princípios e requisitos determinados pelo Regulamento (UE) para serem lícitas[18].

Concretamente, o art. 22º da LOPDGDD estipula que:

"1) As pessoas singulares ou colectivas, públicas ou privadas, podem proceder ao tratamento de imagens através de sistemas de câmaras ou de câmaras de vídeo, a fim de preservar a segurança das pessoas e dos bens e das suas instalações.

2) Só podem ser captadas imagens da via pública na medida em que tal seja indispensável para o efeito referido no número anterior.

No entanto, deve ser possível captar uma área maior da via pública quando tal for necessário para garantir a segurança de bens ou instalações estratégicas ou de infra-estruturas relacionadas com os transportes, mas em caso algum pode implicar a captação de imagens do interior de uma casa particular.

3. Os dados serão apagados no prazo máximo de um mês a contar da sua captação, exceto se tiverem de ser conservados para provar a prática de actos que ameacem a integridade de pessoas, bens ou instalações. Neste caso, as imagens serão colocadas à disposição da autoridade competente no prazo máximo de setenta e duas horas a contar do conhecimento da existência da gravação.

A obrigação de bloqueio prevista no artigo 32º da presente lei orgânica não se aplica a estes tratamentos.

4. O dever de informação previsto no artigo 12.º do Regulamento (UE) 2016/679 considera-se cumprido mediante a afixação de um dispositivo de informação num local suficientemente visível que identifique, pelo menos, a existência da operação de tratamento, a identidade do responsável pelo tratamento e a possibilidade de exercer os direitos previstos nos artigos 15. º a 22.º do Regulamento (UE) 2016/679. Pode também ser incluído no dispositivo de informação um código de ligação ou um endereço Internet para esta informação. Em qualquer caso, o responsável pelo tratamento de dados deve manter as informações referidas no regulamento acima mencionado à disposição das pessoas em causa.

5. Nos termos do artigo 2.º, n.º 2, alínea c), do Regulamento (UE) 2016/679, considera-se excluído do seu âmbito de aplicação o tratamento, por uma pessoa singular, de imagens que apenas captem o interior da sua própria casa.

Esta exclusão não abrange o tratamento efectuado por uma organização de segurança privada que tenha sido contratada para a vigilância de um domicílio e que tenha acesso às imagens.

6. O tratamento de dados pessoais provenientes de imagens e sons obtidos através da utilização de câmaras e de câmaras de vídeo pelas Forças e Órgãos de Segurança e pelos organismos responsáveis pela vigilância e controlo nos estabelecimentos prisionais e pelo controlo, regulação, fiscalização e disciplina do trânsito rege-se pela legislação que transpõe a Diretiva (UE) 2016/680, quando

[18] Anteriormente, por imposição comunitária, a via escolhida foi a já revogada Diretiva 95/46/CE, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais. No entanto, a diferença no tipo de regulamento escolhido não só tem consequências na aplicação direta do seu conteúdo em todos os Estados, como também na eventual interpretação, no nosso caso importante, da exceção pessoal e doméstica, que poderá ser feita nos casos controversos que aqui analisamos. A Comissão Europeia alertou para o facto de a interpretação do RGPD ser da responsabilidade das instâncias jurisdicionais europeias (tribunais nacionais e, em última instância, o Tribunal de Justiça da União Europeia) e não dos legisladores dos Estados-Membros, cabendo ao *Comité Europeu para a Proteção de Dados* (CEPD), sucessor do GT 29, emitir os pareceres adequados quando necessário (Comunicação COM (2018) 43 final, p. 10), como bem nota MEGÍAS QUIRÓS, J. J., *op. cit.*, p. 357.

o tratamento se destine à prevenção, investigação, deteção ou repressão de infracções penais ou à aplicação de sanções penais, incluindo a proteção e prevenção contra ameaças à segurança pública. Fora destes casos, o tratamento será regido pela respetiva legislação específica e, além disso, pelo Regulamento (UE) 2016/679 e pela presente Lei Orgânica.

7. O disposto no presente artigo entende-se sem prejuízo do disposto na Lei n.º 5/2014, de 4 de abril, sobre Segurança Privada e respectivas disposições de aplicação.

8. O tratamento pela entidade patronal dos dados obtidos através de sistemas de câmaras ou de câmaras de vídeo está sujeito ao disposto no artigo 89.º da presente Lei Orgânica".

3. Tratamento de imagens por meio de videovigilância para fins de segurança e outros fins de assistência. Respeito pelo direito à privacidade, à inviolabilidade do domicílio e ao tratamento de dados pessoais.

Art. 22.1. A LOPDPGDD começa por determinar que: "as pessoas singulares ou colectivas, públicas ou privadas, podem realizar o tratamento de imagens através de sistemas de câmaras ou de câmaras de vídeo com a *finalidade de preservar a segurança* das pessoas e dos bens, bem como das suas instalações"[19]. O art. 1.2. do RGPD determina que: "O presente regulamento protege os direitos e liberdades fundamentais das pessoas singulares e, em especial, o seu direito à proteção dos dados pessoais". E o art. 1.b) da LOPDPGDD estabelece que o objetivo desta lei orgânica é: "b) garantir os direitos digitais dos cidadãos, de acordo com o mandato estabelecido no artigo 18.4 da Constituição". O facto é que nos movemos naquilo a que se tem chamado um especial *teste de equilíbrio* entre a *privacidade e a segurança*, bem como entre esta última e o direito fundamental à própria imagem do artigo 18.1 CE[20]. Estamos, portanto, num terreno de possível afetação de direitos fundamentais, embora nem sempre de incompatibilidade[21]. Assim, para que se alcance a *legalidade* na implementação de sistemas de vigilância, normalmente justificados sob o objetivo dissuasor de prevenir a prática de agressões ou outros actos externos ilícitos[22], devem ser tomadas certas precauções na sua instalação, dado que a sua presença pode colidir com outros direitos fundamentais em jogo, de acordo com a AEPD (*ex* art. 5.º e 6.º RGPD)[23] .

Do mesmo modo, partindo do ambiente de cuidados de pessoas admitidas em centros residenciais, constatamos que algumas não estão conscientes dos seus actos (veja-se o caso sueco de auto-mutilação[24]) e com a possibilidade de poderem ferir

[19] Os itálicos são nossos.

[20] Como poder de impedir a sua captação ou difusão por terceiros com os limites derivados de outros direitos ou interesses públicos prevalecentes, BALLESTEROS MOFFA, L.A. *Las fronteras de la privacidad. El conflicto entre seguridad pública y datos personales en una sociedad amenazada y tecnológica*, Granada, Comares, 2020, p. 165.

[21] Assim, na exposição de motivos da Instrução 1/2006, de 8 de novembro, da AEPD, foi salientado que: "a segurança e a vigilância, elementos presentes na sociedade atual, não são incompatíveis com o direito fundamental à proteção da imagem enquanto dado pessoal, o que, consequentemente, impõe o respeito pelas normas de proteção de dados existentes...".

[22] A presença deste tipo de dispositivos no interior de habitações afasta-se da finalidade de proteção da propriedade, para se tornar uma medida coerciva de controlo excessivo da privacidade e/ou dos dados dos utilizadores, que não podem circular livremente no espaço alugado para o efeito como atividade de lazer, turística ou recreativa, etc., de acordo com a AEPD, Processo n.º: EXP202209840 AEPD.

[23] Processo n. em que o senhorio foi multado pela instalação "por aparentes razões de segurança de uma câmara que afectava a zona privada do inquilino, afectando assim os seus dados pessoais". N.º. EXP202207199.

[24] Consta do processo da Autoridade Sueca de Supervisão que, durante a primeira estadia da pessoa sob vigilância e admitida no esta-

outros residentes, incluindo os funcionários[25]. Note-se que a instalação destes dispositivos de vigilância, sobretudo se forem de carácter permanente, pode constituir uma violação dos direitos constitucionais, como adverte a CNIL francesa (*Vidéosurveillance dans les chambres d'Ehpad)*[26], nos casos em que são tratadas imagens de pessoas singulares, nomeadamente nos quartos destes residentes em organizações de cuidados[27].

Imaginemos que existem indícios da prática de um ato ilícito por parte de um trabalhador do centro de acolhimento (situações que foram denunciadas em França). O art. 89.1 segundo parágrafo da LOPDGDD estabelece que: "No caso de ter sido captado o flagrante da prática de um ato ilícito por parte de trabalhadores ou funcionários públicos, o dever de informação entender-se-á cumprido quando existir, pelo menos, o dispositivo referido no art. 22.4 da presente lei orgânica", referindo-se ao cartaz informativo. Concretamente, a AEPD considerou compatível com as finalidades da videovigilância a cedência a terceiros das imagens captadas para efeitos de processo judicial penal ou civil, desde que a visualização se limite às imagens indispensáveis para esse efeito[28]. Por sua vez, o art. 22.º, n.º 3, da LOPDGDD determina, como exceção à eliminação dos dados captados, que estes sejam conservados "para comprovar a prática de actos que atentem contra a integridade de pessoas, bens ou instalações. Neste caso, as imagens devem ser colocadas à disposição da autoridade competente no prazo máximo de setenta e duas horas a contar do conhecimento da existência da gravação".

Para tal, há que distinguir entre a captação de imagens pelo legítimo proprietário do seu próprio domicílio, no âmbito da sua esfera familiar, e os casos em que a atividade envolve terceiros. Assim, enquanto no primeiro caso não haveria grande problema, uma vez que está excluído do âmbito de aplicação das normas de proteção de dados (art. 22.º, n.º 5, da LOPDGDD e art. 2.º, n.º 2, alínea c), do RGPD)[29], nas hipóteses em que são afectados dados pessoais (como a imagem de outra pessoa singular que não o responsável pelo tratamento), deve garantir-se o respeito pelos direitos e liberdades das pessoas potencialmente afectadas. A este respeito, recorde-se que a imagem como di-

belecimento LSS, havia três membros do pessoal de serviço, mas em várias ocasiões tanto o residente como o pessoal foram feridos. Estes incidentes foram tão graves que a vida do residente esteve seriamente em perigo. A organização decidiu então instalar a câmara, após formação e orientação do pessoal. Os funcionários notaram que, quando o residente ficava ansioso e dava sinais de querer fazer mal a si próprio, aos funcionários ou à propriedade, o seu estado voltava ao normal mais rapidamente quando ficava sozinho no seu quarto. Dizem que, desde que a câmara foi instalada, não se registaram incidentes graves quando ele estava no quarto. Isto significa que os funcionarios podiam perceber rapidamente o que ele estava a fazer sem ter de o incomodar e perturbar entrando no quarto e que a instalação da câmara não tinha levado a uma redução do número de funcionários, que era sempre o dobro do pessoal de serviço 24 horas por dia. Além disso, a câmara só era utilizada em tempo real para observar o estado do residente e não havia qualquer gravação áudio. E que, quando o residente solicitava a presença de um funcionário no seu quarto, este vinha e a câmara não era utilizada. No entanto, o caso foi resolvido como tratamento ilegal e a instalação do sistema de videovigilância foi sancionada, como se explica a *seguir*. Decisão completa disponível em: https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-gnosjo-2020-11-25.pdf

[25] Como se refere no Processo n.º E/02273/2016 AEPD, relativo à legalidade da instalação de câmaras de videovigilância em áreas comuns pelas necessidades de vigilância de um lar de idosos dependentes, não só devido à falta de consciência dos seus actos mas também pelos perigos da permanência fora das áreas de segurança ou do acesso de estranhos às instalações

[26] Informações disponíveis em https://www.cnil.fr/sites/cnil/files/2023-02/projet_de_recommandation_videosurveillance_ephad.pdf.

[27] Na sua decisão a *Autoridade Sueca para a Proteção de Dados* (APD) conclui que a videovigilância em questão, que monitoriza as pessoas no seu ambiente doméstico, é particularmente sensível do ponto de vista da privacidade. Por este motivo, a DPA impõe uma coima de 300 000 coroas suecas à empresa imobiliária https://edpb.europa.eu/news/national-news/2020/300000-sek-fine-against-housing-company_en.

[28] Relatório jurídico sobre o interesse legítimo, https://www.aepd.es/sites/default/files/2019-09/informe-juridico-rgpd-interes-legitimo.pdf.

[29] Referimo-nos à exceção "pessoal ou doméstica", que é discutida na secção seguinte.

reito de personalidade está ligada à imagem como dado, sendo protegida através do tratamento automatizado a que se refere o art. 18.º, n.º 4, CE (art. 1.º, alínea b), da LOPDGDD)[30].

Em todo o caso, como se disse, os direitos à honra, à reserva da intimidade da vida privada e familiar e à própria imagem juntam-se à proteção dos dados pessoais, que protege a utilização desses dados por terceiros sem o consentimento do titular, o que configura o conceito mais amplo de privacidade, podendo estes direitos ser violados de forma independente ou simultânea, já que se integram uns nos outros[31].

Note-se que esta questão está relacionada com o direito fundamental à privacidade (n.º 1 do artigo 18.º da Constituição Espanhola), com a inviolabilidade do domicílio (n.º 2 do artigo 18.º) e, por força do n.º 4, com a proteção das pessoas singulares relativamente ao tratamento de dados pessoais, direito fundamental protegido pelo n.º 4 do artigo 18.º da Constituição espanhola[32]. Este último direito tem por objetivo proteger o indivíduo contra qualquer invasão da sua vida pessoal e familiar. No que diz respeito à questão em apreço, garante também a não ingerência nos espaços físicos onde se desenrolam os aspectos da sua vida mais íntima, como é o caso dos quartos das pessoas em centros de cuidados ou habitações partilhadas, que se tornam a casa dos senhorios e, ao mesmo tempo, dos inquilinos, mesmo que estes apenas usufruam parcialmente da propriedade. Tal como a autoridade sueca para a proteção de dados decidiu, a vigilância das pessoas no seu ambiente doméstico é particularmente sensível do ponto de vista da privacidade[33].

A este respeito a AEPD afirma[34] que o Supremo Tribunal assume a definição de "privacidade" de forma ampla, reconhecendo assim a existência do espaço de privacidade, cuja exclusão do conhecimento de outras pessoas constitui uma faculdade de cada indivíduo. Consequentemente, a proteção do domicílio é apenas um aspeto da proteção da privacidade que serve o livre desenvolvimento da personalidade. Também neste sentido o Tribunal Constitucional afirma no STC 22/1984, de 17 de fevereiro de 1984, que "a inviolabilidade do domicílio, que constitui um autêntico direito fundamental do indivíduo, estabelecido, como dissemos, para garantir a esfera de privacidade deste no espa-

[30] VELASCO NÚÑEZ, E., "Derecho a la imagen: tratamiento procesal penal", *Diario La Ley*, n. 8595, 1-9-2015, p. 2. Recordemos que a Lei Orgânica de Proteção Civil do Direito à Honra, à Privacidade Pessoal e Familiar e à Imagem Pessoal (LOPC), considera a captação e publicação de imagens de pessoas privadas, contra a sua vontade, como uma "ingerência ilícita". Neste sentido, BELLO JANEIRO, D. "Responsabilidad civil y derechos de la personalidad", *Cuestiones clásicas y actuales del Derecho de daños. Estudios en homenaje al profesor Dr. Roca Guillamón*, T.I, Madrid, Thomson Reuters Aranzadi, 2021, p. 690; MORENO MARTÍNEZ, explicando a possível coordenação entre esta Lei e o regulamento sobre o tratamento de dados pessoais, "El impacto del Reglamento General de Protección de Datos en el régimen de responsabilidad civil (art. 82 RGPD)", cap. 101, *Cuestiones clásicas y actuales del Derecho de daños. Estudios en homenaje al profesor Dr. Roca Guillamón*, T.III, Madrid, Thomson Reuters Aranzadi, 2021, pp. 515-567.

[31] GIL ANTON, A. "Redes sociales y privacidad del menor: un debate abierto", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, n. 36,2014, pp. 7-8, seguido de CREMADES GARCÍA, P. "Protección de la imagen del menor y sociedad de la información", cap. 39, *Cuestiones clásicas y actuales del Derecho de daños. Estudios en homenaje al profesor Dr. Roca Guillamón*, T.I, Madrid, Thomson Reuters Aranzadi, 2021, pp. 1692-1693. Ver também o número de ficheiro: EXP202209840 AEPD.

[32] Deste modo, a nossa Constituição foi pioneira no reconhecimento do direito fundamental à proteção de dados pessoais ao estipular que "a lei limitará a utilização da informática para garantir a honra e a intimidade pessoal e familiar dos cidadãos e o pleno exercício dos seus direitos". Fazia assim eco dos trabalhos desenvolvidos desde o final dos anos 60 no Conselho da Europa e das poucas disposições legais adoptadas nos países vizinhos, refere o preâmbulo da LOPDGDD. Referências constitucionais também citadas no Dossier n. EXP202207199 AEPD.

[33] Resolução de 14 de dezembro de 2020, DI-2020-4534. Resumo disponível em: https://edpb.europa.eu/news/national-news/2020/300000-sek-fine-against-housing-company_en; https://www.imy.se/en/news/300000-sek-fine-against-housing-company/.

Conteúdo integral da resolução em https://www.imy.se/globalassets/dokument/beslut/2020-12-14-beslut-tillsyn-uppsalahem.pdf.

[34] Processo N.º EXP202209840 AEPD ; Processo N.º EXP202209842 AEPD.

ço escolhido pelo próprio indivíduo e que se deve caraterizar precisamente por ser isento ou imune a invasões ou agressões externas, de outras pessoas ou da autoridade pública"[35]. Paralelamente, em apoio desta argumentação, a AEPD invoca a sentença do Tribunal Superior de Justiça da Catalunha, Câmara do Contencioso, de 2 de julho de 2020[36] que afirma: "a norma constitucional que proclama a inviolabilidade do domicílio e a proibição de entrada e buscas no domicílio (art. 18.2 CE), apesar da autonomia que a Constituição espanhola reconhece a ambos os direitos, constitui uma manifestação da norma anterior (art. 18.1 CE) que garante o direito fundamental à intimidade pessoal e familiar. Assim, se o direito proclamado no art. 18.1 CE visa proteger uma área reservada da vida das pessoas, excluída do conhecimento de terceiros, sejam eles autoridades públicas ou particulares, contra a sua vontade[37], o direito à inviolabilidade do domicílio protege "uma área espacial específica", dado que é nela que as pessoas exercem a sua liberdade mais íntima, livre de qualquer sujeição aos costumes e convenções sociais, sendo o objeto de proteção deste direito tanto o espaço físico em si mesmo considerado mas também o que nele emana da pessoa e da sua esfera privada. Por esta razão, temos afirmado que a proteção constitucional da casa é uma proteção instrumental, que defende as esferas em que se desenvolve a vida privada da pessoa"[38] .

Sem prejuízo da instalação de câmaras em centros de saúde e hospitais com a finalidade - mais utilizada e exposta - de garantir a segurança, a captação e gravação de imagens poderá ser utilizada com o objetivo de garantir um tratamento de saúde adequado, como seria o caso da monitorização de doentes em unidades de cuidados intensivos ou da telemedicina, como alerta a AEPD[39].

4. Âmbito da videovigilância. Delimitação da atividade exclusivamente pessoal ou doméstica.

Centrando-nos no problema principal que aqui abordamos e que, com algumas particularidades, é partilhado por habitações colectivas, espaços de convívio ou estabelecimentos de prestação de cuidados, reside na existência de compartimentos reservados a uma maior privacidade (que nem sempre podem ser classificados como vedados de terceiros) junto a áreas comuns.

O artigo 22.5 da LOPDGDD exclui do âmbito de aplicação do RGPD o tratamento por uma pessoa singular de imagens que apenas captam o

[35] VLEX-15034676.

[36] N.º 2923/2020. Seguem-se os acórdãos do TC 10/2002 de 17 de janeiro e 22/2003 de 10 de fevereiro.

[37] Sobre a relação entre os dados pessoais e o direito à vida privada, ver BELLO JANEIRO, D., *op.cit.,* pp. 683-692.

[38] Por outro lado, no Processo nº: EXP202208420, é também acrescentado como argumentação o Julgamento Criminal Nº. 147/2021, Tribunal Provincial de Huelva, Secção 1, Rec 298/2021 de 29 de junho de 2021: ""No que diz respeito às violações dos direitos fundamentais que se diz terem sido cometidas pela representação de Constantino, em relação à inviolabilidade do domicílio, a proteção constitucional do domicílio no artigo 18.2 da Constituição é especificada em duas normas diferentes, a primeira refere-se à proteção da sua inviolabilidade como garantia de que esta esfera espacial de privacidade da pessoa por ela escolhida está "isenta de" ou "imune a" qualquer tipo de invasão ou agressão externa por parte de outras pessoas ou da autoridade pública, incluindo aquelas que podem ser realizadas sem penetração física na mesma, mas através de dispositivos mecânicos, electrónicos ou outros semelhantes (STC 22/1984 de 17 de fevereiro, e a segunda, como especificação da primeira, estabelece a interdição de duas das formas possíveis de ingerência no domicílio, ou seja, a entrada e as buscas, estipulando que, salvo em caso de flagrante delito, só são constitucionalmente legítimas a entrada ou as buscas efectuadas com o consentimento do proprietário ou resolução judicial, pelo que a menção das excepções a esta interdição, admitidas pela Constituição, tem carácter taxativo (CCT 22/1984, de 17 de fevereiro de 1984 e 136/2000, de 29 de maio de 2000)".

[39] AEPD: "Guía sobre el uso de videocameras para seguridad y otras fines de la AEPD", https://www.aepd.es/documento/guia-videovigilancia.pdf, p. 44. Referimo-nos a estas funcionalidades mais avançadas na primeira secção do presente documento.

interior da sua própria casa[40]. O artigo 2.2.c) do RGPD estabelece que "o presente regulamento não se aplica ao tratamento de dados pessoais: efectuado por uma pessoa singular no exercício de actividades *exclusivamente pessoais ou* domésticas"[41] ; formulação que tem sido interpretada em sentido restritivo, por um lado porque as limitações às garantias dos direitos fundamentais à privacidade e à proteção dos dados pessoais nunca devem ir além do estritamente necessário e, por outro, porque o próprio texto regulamentar utilizou o termo *exclusivamente* para dissipar quaisquer dúvidas que pudessem surgir sobre a questão[42].

Por outro lado, a utilização de câmaras por particulares para fins de vigilância na via pública, independentemente do meio utilizado para o efeito (bicicleta, drone, correndo, etc.), não estaria abrangida pela referida exceção, pelo que se aplicariam as normas de proteção de dados. Importa ter em conta que a vigilância do comportamento de terceiros através de câmaras não é uma circunstância que possa ser subsumida no âmbito privado, familiar ou de amizade, razão pela qual se aplicará, logicamente, a norma aqui tratada, daí a proibição de captar imagens da via pública, salvo se for imprescindível para efeitos de preservação da segurança, nos termos previstos no art. 22.º, n.º 2, da LOPDGDD[43]. Esta exclusão também não abrangeria o tratamento efectuado por uma entidade de segurança privada que tenha sido contratada para a vigilância de uma residência e que tenha acesso às imagens[44].

No que respeita à instalação de câmaras em zonas comuns de uma comunidade de proprietários (ou zonas balneares como piscinas ou balneários)[45], a LPH prevé a maioria necessária para a sua aprovação[46] e a própria AEPD publicou algu-

[40] Os itálicos são nossos. Art. 22.º, n.º 5, da LOPDGDD: "Nos termos do artigo 2.º, n.º 2, alínea c), do Regulamento (UE) 2016/679, considera-se excluído do seu âmbito de aplicação o tratamento, por uma pessoa singular, de imagens que apenas captem o interior do seu próprio domicílio". Art. 2.2. LOPDGDD: "A presente lei orgânica não é aplicável:

a) Os tratamentos excluídos do âmbito de aplicação do Regulamento Geral de Proteção de Dados pelo seu artigo 2.2, sem prejuízo do disposto nos números 3 e 4 do presente artigo". A nova LOPDGDD não reproduz a exceção com as mesmas palavras que o RGPD, como acontecia na anterior Lei 15/1999, mas regula-a fazendo referência direta a este último. A única diferença a destacar é que o novo artigo 22.º exclui expressamente o tratamento efectuado por uma pessoa singular na atividade de videovigilância do domicílio familiar, tratamento que já tinha sido considerado excluído do âmbito de aplicação da lei, MEGIAS QUIRÓS, J.J., *op. cit*., p. 358.

[41] Os itálicos são nossos.

[42] Como refere MEGIAS QUIRÓS, a propósito do acórdão do TJUE de 6 de novembro de 2003, processo C-101/01. Pedido de decisão prejudicial apresentado pelo *Göta hovrätt (*Suécia): Bodil Lindqvist (ECLI:EU:C:2003:596), *op. cit*., pp. 369-370.

[43] Tanto assim é que, quando se realiza afectando a via pública, é da responsabilidade das Forças e Corpos de Segurança, como assinala a Agência Basca de Proteção de Dados, parecer CN 16-022.

[44] Cf. Lei n.º 5/2014, de 4 de abril, sobre Segurança Privada e respectivas normas de execução. Como se deixou claro, é notório que a videovigilância policial ligada à segurança pública e à prevenção e repressão da criminalidade tem uma regulamentação detalhada que estabelece um regime de autorização prévia, que carece de parecer favorável da Comissão de Videovigilância. Este órgão é presidido pelo Tribunal Superior de Justiça da Comunidade Autónoma correspondente, ao passo que a videovigilância não policial, seja ela realizada no âmbito público ou privado, tem sido objeto de uma regulamentação muito escassa e de reduzido alcance normativo (Lei de Segurança Privada e instruções das autoridades de controlo em matéria de proteção de dados), INTXAURTIETA MADARIAGA, R., *op. cit*., p. 3678. A este respeito, ver também RODRÍGUEZ AYUSO, J.F., *Protección de datos. Estudio conforme al Esquema de Certificación de Delegados de Protección de Datos (AEPD-DPD)*, Valencia, Tirant lo blanch, 2023, p. 294. Ver, para mais informações, o Relatório Jurídico da AEPD N/REF: 010308/2019, https://www.aepd.es/documento/2019-0031.pdf.

[45] Art. 17.3 LPH: "A criação ou supressão de portaria, porteiro, vigilância ou outros serviços comuns de interesse geral, quer impliquem ou não alteração do título constitutivo ou dos estatutos, carece do voto favorável de três quintos do número total de condóminos que, por sua vez, representem três quintos das quotas de participação". Sobre a instalação nas zonas comuns das associações de moradores e zonas balneares, ver o Guia da AEPD sobre a utilização de câmaras de vídeo para segurança e outros fins, https://www.aepd.es/documento/guia-videovigilancia.pdf p. 35-36, 40; https://www.aepd.es/documento/informe-juridico-rgpd-camaras-en-spas.pdf

[46] Uma vez aprovado pela comunidade de proprietários, não será necessário o consentimento do titular dos dados ou da pessoa afetada pelo tratamento dos dados pessoais, uma vez que o interesse público é o fundamento que legitima o tratamento, na opinião da GIL MEMBRADO, C., *Videovigilancia y protección de datos*, *especial referencia a la gra-*

mas fichas técnicas sobre os requisitos necessários para a instalação de videovigilância, bem como sobre a forma de captação de imagens de pessoas no exterior de uma habitação (entradas, espaços comuns, muros de separação, etc.)[47]. Por sua vez na Suécia foi aplicada uma coima (300 000 SEK) a uma *empresa de habitação* porque, num edifício de apartamentos, a área de vigilância abrangia duas portas de apartamentos, uma pertencente ao queixoso e a outra a um residente que tinha sido sujeito a incómodos e assédio[48].

Passando ao caso do interior de uma residência privada, devemos considerar que a exceção "pessoal e doméstica" à videovigilância em habitações privadas desaparece quando o uso e gozo temporário da habitação é cedido a um terceiro, quer por força de uma modalidade contratual (contrato de alojamento ou arrendamento turístico[49]), quer por um direito real de habitação. E isto mesmo que a utilização da casa não seja total mas partilhado com outras pessoas, como o proprietário[50]. Neste caso, o espaço estará abrangido pelas normas de proteção de dados, tornando-se num lugar reservado à privacidade pessoal e familiar desse possuidor legal. Consequentemente, a recolha e o tratamento de dados pessoais não serão em regra permitidos, a menos que exista um fundamento legítimo e os requisitos para que o tratamento esteja em conformidade com o regulamento *ad hoc* sejam cumpridos.

Da mesma forma, o controlo do trabalho no domicílio através de vídeo de quem possa realizar tarefas de limpeza ou de cuidado de menores ou pessoas dependentes foi protegido pela AEPD e por força do art. 20.3 do Estatuto dos Trabalhadores[51] . Tal como no caso dos trabalhadores dos

bación de la vía pública desde el espacio privado Madrid, La Ley, 2019, p. 153. No entanto, baseando-se na Diretiva 95/46/CE revogada, o TJUE de 11 de dezembro de 2019, *TK/Asociația de Proprietari bloc M5A-ScaraA*, Processo C-708/18, n.º 49, declarou que a colocação de um sistema de videovigilância assentava no "interesse legítimo", Documento EU-R-Lex 62018CJ0708, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A62018CJ0708. Para mais informações sobre este caso, ver MARTÍNEZ LÓPEZ-SÁEZ, Mónica: "A vueltas con la ponderación de derechos en materia de videovigilancia. Interés legítimo, seguridad privada, régimen vecinal y protección de datos", *Revista de Derecho Civil*, ISSN 2341-2216, Vol. 9, Nº. 4, 2022, pp. 351-375.

47 Disponível em: https://www.aepd.es/areas-de-actuacion/videovigilancia#:~:text=Saber%20a%20trav%20C3%A9s%20da%20nossa%20habitação%20ou%20um%20estabelecimento%20comercial

48 Foi declarado que, mesmo que a empresa tivesse um *interesse legítimo* na videovigilância, este era ultrapassado pelo direito dos residentes à privacidade, Resolução de 14 de dezembro de 2020, DI-2020-4534. Resumo disponível em: https://edpb.europa.eu/news/national-news/2020/300000-sek-fine-against-housing-company_en; https://www.imy.se/en/news/300000-sek-fine-against-housing-company/ Conteúdo integral da decisão em https://www.imy.se/globalassets/dokument/beslut/2020-12-14-beslut-tillsyn-uppsalahem.pdf.

49 Em relação a um apartamento turístico onde tinha sido instalado "um sistema de acesso que tirava fotografias com a aproximação à porta", a AEPD determina que: "Qualquer pessoa que alugue um apartamento turístico goza de plena proteção do direito à privacidade pessoal e/ou familiar, bem como da proteção dos seus dados pessoais contra a presença de dispositivos que possam afetar espaços "reservados" onde o indivíduo leva uma vida, mesmo que temporária, pessoal e familiar, excluída tanto do conhecimento como da intromissão de terceiros. N.º do processo: EXP202209840.

50 A este respeito, a AEPD afirma que: "é irrelevante que, no presente caso, a parte requerida viva com o requerente nessa habitação, uma vez que, em qualquer caso, continua a constituir o seu próprio domicílio, mesmo que seja partilhado", Processo n.º EXP202208420.

51 No que diz respeito aos sistemas de *geolocalização,* o art. 90º da LOPDGDD estabelece: "Direito à privacidade na utilização de sistemas de geolocalização no local de trabalho.

1. A entidade empregadora pode proceder ao tratamento dos dados obtidos através de sistemas de geolocalização para o exercício das funções de controlo dos trabalhadores ou dos funcionários públicos previstas, respetivamente, no n.º 3 do artigo 20.º do Estatuto dos Trabalhadores e na legislação da função pública, desde que essas funções sejam exercidas no seu quadro legal e com os limites que lhe são inerentes. 2 - As entidades empregadoras devem informar previamente, de forma expressa, clara e inequívoca, os trabalhadores ou os funcionários públicos e, se for caso disso, os seus representantes, da existência e das características desses dispositivos. Devem igualmente informá-los do possível exercício dos direitos de acesso, retificação, limitação do tratamento e eliminação".

BATUECAS CALETRÍO, assinala que uma elevada percentagem de casos referentes à utilização da geolocalização no ambiente de trabalho, como a instalação em viaturas da empresa, foram sancionados pela AEPD, por violação do art. 5.º da LOPDGDD, quando o empregador não informou os trabalhadores sobre a sua instalação ou quando, tendo-os informado, utilizam os dados de localização para um fim diferente daquele para que foram informados, *op. cit*.

centros residenciais, a exclusão da videovigilância dos locais de descanso deve ser aplicada (art. 89.2 LOPDGDD[52]) mas não nas funções de controlo do cumprimento das suas obrigações laborais (art. 89.1 LOPDGDD)[53]. Como referiu a *Commission Nationale de l'Informatique et des Libertés* francesa, embora o poder de vigilância do empregador seja legítimo na medida em que o leva a controlar o trabalho prestado, a avaliá-lo e a dar instruções sobre o trabalho a realizar, este poder tem limites no que toca à transparência da medida, à sua legitimidade e à sua proporcionalidade em relação ao objetivo prosseguido. A vigilância *contínua* dos trabalhadores no seu local de trabalho ou durante a sua atividade profissional constituiria uma infração deste tipo, a menos que sejam demonstradas circunstâncias especiais que justifiquem a mesma[54] .

Por seu lado, nos centros de cuidados destinados a pessoas idosas dependentes, o problema da instalação de sistemas de videovigilância nos locais mais sensíveis à privacidade dos doentes internados, os *quartos*, surgiu recentemente em França, face a alegados maus tratos por parte do pessoal contratado (*Vidéosurveillance dans les chambres d'Ehpad*), como já referimos. Distinguindo os diferentes espaços, a CNIL indica que a instalação de câmaras em *locais abertos ao público*, como as zonas de entradas e saídas de uma organização social ou médico-social, é, em princípio, autorizada, desde que o tratamento esteja em conformidade com o RGPD (e a lei francesa de proteção de dados) e que seja apresentado um pedido de autorização à prefeitura onde o sistema vai ser instalado[55]. De referir que a AEPD teve oportunidade de se pronunciar sobre um caso relativo à instalação de câmaras de videovigilância nas áreas comuns de um lar de idosos, concluindo que os princípios da qualidade, proporcionalidade e finalidade do tratamento não foram violados, de acordo com a revogada Instrução 1/2006[56].

No entanto, a instalação de câmaras nos *quartos* das pessoas que vivem em lares de idosos levanta uma série de questões legais e éticas que foram recentemente abordadas pela Autoridade Francesa de Proteção de Dados[57], antecipando a este respeito que: "tal sistema é suscetível de violar os direitos tanto dos empregados como dos residentes, para quem o quarto é o único local de privacidade onde

[52] Art. 89.º, n.º 2, da LOPDGDD: "Em caso algum será permitida a instalação de sistemas de gravação de som ou de videovigilância em locais destinados ao repouso ou ao lazer dos trabalhadores ou dos funcionários públicos, tais como vestiários, casas de banho, cantinas e similares". Sobre a coima de 50.000 euros aplicada pela AEPD a uma empresa por violação das normas de proteção de dados ao instalar câmaras de videovigilância no refeitório dos empregados, veja-se o comentário em: https://maserlegal.es/actualidad-lopd/videovigilancia-y-proteccion-de-datos/

[53] Para uma síntese da regulamentação a aplicar, ver a Ficha práctica de videovigilancia por cámaras para el control laboral, https://www.aepd.es/documento/fichas-videovigilancia-6-camaras-control-laboral.pdf. Sobre a visualização destas câmaras como meio de prova em processos de despedimento, ver PRAT RAMÓN, M.I., "Las cámaras de videovigilancia como medio de prueba en el proceso laboral", *Diario La Ley*, n. 10263, 10 de abril de 2022, *La Ley* 1290/2023. Sobre o cumprimento do dever de informação e a instalação de câmaras ocultas no âmbito do poder de controlo empresarial, para a análise do processo SSTEDH López Ribalda I (9 de janeiro de 2018) e II (17 de outubro de 2019), ver ÁLVAREZ ALVITE, A., *op. cit.*; PASCUAL, J., "López Ribalda II, la utilización de cámaras de video-vigilancia en las relaciones laborales: ¿se puede prescindir del deber de información?", *Diario La Ley*, n. 9555, 17 de janeiro de 2020, *La Ley* 15597/2019.

[54] Acrescentando que os sistemas de videovigilância no local de trabalho, que são legítimos se o seu objetivo for garantir a segurança dos bens e das pessoas no local de trabalho, devem garantir que não se infringem *de forma desproporcionada* os direitos e liberdades fundamentais dos trabalhadores, informação disponível em https://www.cnil.fr/sites/cnil/files/2023-02/projet_de_recommandation_videosurveillance_ephad.pdf.

[55] Desde que os trabalhadores ou os residentes não estejam sob vigilância constante, declarou a autoridade de controlo francesa, remetendo mais pormenores para o guia https://www.cnil.fr/fr/technologies/videosurveillance-videoprotection).

[56] Processo N. E/02273/2016. Os sistemas de videovigilância estavam localizados no hall de entrada, na sala de estar principal, nos corredores, na cozinha e na sala de jantar.

[57] CNIL: "Vidéosurveillance dans les chambres d'Ehpad", informação disponível em https://www.cnil.fr/sites/cnil/files/2023-02/projet_de_recommandation_videosurveillance_ephad.pdf.

podem desenvolver a sua vida emocional e familiar". Com base nesta premissa e conforme detalhado na secção seguinte, a recomendação inicial conclui que a vigilância permanente destes espaços privados constitui, de facto, uma violação dos seus direitos fundamentais.

Na Suécia, em 2020, a Autoridade Nacional de Proteção de Dados aplicou uma coima administrativa de 200 000 coroas suecas ao município de *Gnosjö* por vigilância vídeo ilegal numa habitação pública ou residência LSS para pessoas com determinadas deficiências funcionais. Foi possível demonstrar que os requisitos legais para o tratamento de dados pessoais de um residente, que foi vigiado no seu quarto em violação do RGPD e da lei sueca sobre videovigilância, não foram cumpridos, entre outros motivos, porque não foram previamente equacionadas medidas alternativas menos invasivas. Em particular, o seu quarto estava sob vigilância constante de câmaras. Por conseguinte, concluiu-se que se tratava de um "tratamento de dados pessoais muito sensível à privacidade, que implicava a vigilância do residente na esfera mais privada da sua casa. A Inspeção de Dados avalia que a vigilância por câmara implicou uma intrusão significativa na integridade pessoal do residente"[58] .

5. Tratamento de sistemas de videovigilância em residências e lares de idosos

5.1. Categorias especiais de dados e respetivo tratamento

Centrando-nos nesta última secção no problema dos centros residenciais para idosos, seria apropriado começar por recordar que a imagem física de uma pessoa, de acordo com o artigo 4.1 do RGPD, é um dado pessoal e a sua proteção é, portanto, objeto deste Regulamento, de acordo com a AEPD[59]. No entanto, esta afirmação requer mais desenvolvimento. Os dados obtidos por gravação ou filmagem não estão sempre sujeitos à atenção do RGPD, sendo objeto do mesmo apenas quando podem fornecer informações sobre uma pessoa singular *identificada ou identificável*, que é então designada por "pessoa em causa", art. 4.º, n.º 1, do RGPD. Como bem se disse[60], a relevância do tratamento efectuado através das câmaras de videovigilância não reside em si mesmo nas imagens mas nos dados que elas contêm, sobretudo porque captam a *imagem facial* das pessoas e esta revela o seu sexo, a sua origem racial ou étnica, a sua religião… Assim, os dados objeto de tratamento são convertidos em *dados biométricos*, por força da definição do art. 4. 14 RGPD[61] . Com base neste postulado, devem ser considerados uma *categoria especial de dados*, como é justamente confirmado, sem prejuízo da sua consideração como dados, os relativos *à saúde*, que são

[58] Resolução "Tillsyn enligt EU:s dataskyddsförordning 2016/679 - kamerabevakning på ett LSSboende", 2020-11-24 DI-2019-7782, disponível em: https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-gnosjo-2020-11-25.pdf. Informação resumida disponível em: https://edpb.europa.eu/news/national-news/2020/gdpr-fine-unlawful-video-surveillance-lss-housing_es.

[59] EXPEDIENTE N.º: EXP202208420, datado de 12/07/2022, deliberação do procedimento sancionatório.

[60] PARDO MARQUINA, V., *op. cit.*, p. 4.

[61] Considerando (14): "dados biométricos", dados pessoais obtidos a partir de um tratamento técnico específico, relativos às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitem ou confirmam a identificação única dessa pessoa, tais como imagens faciais ou dados dactiloscópicos".

obtidos no domínio hospitalar e assistencial, art. 4. 15 RGPD[62]. Resulta destas disposições que esta formulação inclui não só a saúde efectiva de uma pessoa, mas também informações sobre o "estado de saúde" (considerando 35)[63]. Esta qualificação como "categorias especiais de dados" implica, em princípio, uma consequência importante, ou seja, a proibição de tratamento (considerando 51 e n.º 1 do artigo 9.º do RGPD)[64]. Será este o caso a menos que exista um motivo que o justifique, em conformidade com o artigo 9.º, n.º 2, do RGPD, e que quanto ao tema em apreço poderá indicar-se o *interesse público* (artigo 9.º, n.º 2, alínea g), do RGPD) ou a necessidade do tratamento para a prestação de serviços *de assistência sanitária ou social* (artigo 9.º, n.º 2, alínea h), do RGPD) ou ainda para a proteção dos *interesses vitais* da pessoa em causa, como no caso das unidades de cuidados intensivos (artigo 9.º, n.º 2, alínea c), do RGPD)[65].

De facto, este é um dos casos classificados como de *maior risco de* acordo com a LOPDPGDD, razão pela qual os responsáveis pelo tratamento de dados e os subcontratantes são obrigados a cumprir as obrigações previstas no art. 28.º do RGPD, sendo também articuladas medidas técnicas e organizativas especiais "quando o tratamento de dados for efectuado sobre grupos em situação de especial vulnerabilidade e, em especial, sobre menores e pessoas com deficiência", art. 28.º, n.º 2, alínea e), da LOPDGDD[66], juntamente com os requisitos que passamos a explicar.

[62] Art. 14.15 do RGPD: "dados relativos à saúde", 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".

[63] Considerando (35) do RGPD: "Os dados pessoais relativos à saúde devem incluir todos os dados relativos ao estado de saúde da pessoa em causa que forneçam informações sobre a sua saúde física ou mental passada, presente ou futura. Incluem-se aqui as informações sobre a pessoa singular recolhidas por ocasião do seu registo para efeitos de cuidados de saúde, ou por ocasião da prestação desses cuidados, em conformidade com a Diretiva 2011/24/UE do Parlamento Europeu e do Conselho (1); qualquer número, símbolo ou dado atribuído a uma pessoa singular que a identifique de forma inequívoca para efeitos de saúde; informações obtidas a partir de testes ou exames de uma parte do corpo ou de uma substância corporal, incluindo informações provenientes de dados genéticos e amostras biológicas, e quaisquer informações relacionadas, a título de exemplo, com uma doença, deficiência, risco de doença, historial médico, tratamento clínico ou estado fisiológico ou biomédico da pessoa em causa, independentemente da sua fonte, por exemplo, um médico ou outro profissional de saúde, um hospital, um dispositivo médico ou um teste de diagnóstico in vitro". Para uma visão geral da proteção de dados de saúde no RGPD, ver ÁLVAREZ RIGAUDIAS, C.: "Tratamiento de datos de salud", cap. XI, em *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, Piñar Mañas, J.L. dir, Reus, Madrid, 2016, pp. 171-185.

[64] Para uma melhor compreensão do tratamento de categorias especiais de dados pessoais, remetemos para PUYOL MONTERO, J. "Los principios del derecho a la protección de datos", Cap. IX, in *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, Piñar Mañas, J.L. dir, Reus, Madrid, 2016, pp. 45-148.

[65] No que respeita ao reconhecimento facial utilizado para a videovigilância, é de notar que tem sido controverso em que circunstâncias pode ser considerado como tratamento de dados de categoria especial**.** De acordo com o artigo 4.º do RGPD, pode interpretar-se que o conceito de dados biométricos incluiria tanto a identificação como a verificação/autenticação dos dados. No entanto, em geral, os dados biométricos só serão considerados como uma categoria especial de dados nos casos em que estejam sujeitos a um tratamento técnico destinado à identificação biométrica (um para muitos) e não no caso de verificação/autenticação biométrica (um para um). A este respeito, o Comité Europeu para a Proteção de Dados, nas suas "Orientações 3/2019 sobre o tratamento de dados pessoais através de dispositivos de vídeo", considera a utilização da videovigilância com reconhecimento facial como uma categoria especial de dados ao abrigo do artigo 9. Por conseguinte, para que o tratamento de dados biométricos por sistemas de reconhecimento facial integrados num sistema de videovigilância seja lícito, deve ser cumprida uma das exceções que levantam a proibição de tratamento[1], de acordo com o artigo 9.º, n.º 2, do RGPD, SÁNCHEZ, I., "Videovigilancia y control de reconocimiento facial", 7 de julho de 2022, https://eiposgrados.com/blog-dpo/compliance/videovigilancia-y-control-de-reconocimiento-facial/. Ver também o Relatório Jurídico 2019 da AEPD, disponível em: https://www.aepd.es/documento/2019-0031.pdf.

[66] No entanto, o considerando 75 do RGPD, ao exemplificar situações especiais de risco, refere-se a casos em que são tratados dados pessoais de pessoas vulneráveis, mencionando, em particular, apenas crianças. Por seu lado, o considerando 38 do RGPD refere que: As crianças merecem uma proteção específica dos seus dados pessoais, uma vez que podem estar menos conscientes dos riscos, consequências, garantias e direitos relativos ao tratamento de dados pessoais. Essa proteção específica deve aplicar-se, em particular, à utilização de dados pessoais de crianças para fins de marketing, de definição de perfis de personalidade ou de utilizadores, bem como à recolha de dados pessoais relativos a crianças quando utilizam serviços que lhes são oferecidos diretamente. O consentimento do titular das responsabilidades

5.2. Requisitos para a legalidade do tratamento de dados pessoais

O artigo 4.º, n.º 2, do RGPD define o conceito de "tratamento" de dados pessoais. Assim, "tratamento" é qualquer operação ou conjunto de operações efectuadas sobre dados pessoais ou conjuntos de dados pessoais, com ou sem meios automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, a supressão ou a destruição"[67]. O artigo 5.1.a) do RGPD estabelece que "os dados pessoais devem ser: (a) tratados de forma lícita, leal e transparente em relação à pessoa em causa ("licitude, lealdade e transparência")". E o n.º 1 do artigo 6.º do RGPD determina a lista de "condições" para que *o tratamento* seja *lícito* (considerando 40 do RGPD)[68].

Na hipótese principal analisada nesta secção, a admissão por razões de saúde em estabelecimentos residenciais, *prima facie,* parece que a base legitimadora deve ser o tratamento necessário para proteger um *interesse vital* da pessoa em causa (art. 6.1 d. e secção 4. c. RGPD). A este respeito, a AEPD[69] estabeleceu que, sem prejuízo da instalação de câmaras em centros de saúde e hospitais com o objetivo de garantir a *segurança de pessoas, bens e instalações* (*interesse público*, art. 6.º, n.º 1, alínea e), do RGPD)[70] , "a captação e gravação de imagens pode ser utilizada para garantir um tratamento *de saúde* adequado, como seria o caso do acompanhamento de doentes em unidades de cuidados intensivos ou da telemedicina", ou seja, para proteger um "interesse vital" da pessoa em causa[71].

Por conseguinte, por um lado, no caso de centros de saúde ou de cuidados públicos (tal como listados no sítio Web do Ministério da Saúde da Comunidade Valenciana)[72] ou na Suécia (Comité

parentais ou da tutela não deve ser exigido em contexto de serviços preventivos ou de aconselhamento oferecidos diretamente às crianças.

67 No que diz respeito à recolha de fotografias dos quartos dos residentes para publicitar uma residência, se apenas for mostrado mobiliário, tal não será abrangido pela proteção de dados pessoais. No entanto, se for possível identificar objectos pessoais que permitam a identificação do proprietário, o estabelecimento deverá solicitar o consentimento da pessoa em causa antes de a colocar num sítio Web ou de a publicitar, https://protecciondatos-lopd.com/empresas/residencias-ancianos-rgpd/#Se_pueden_publicar_fotografias_de_las_habitaciones_de_los_residentes_para_publicitar_la_Residencia.

68 Considerando (40) do RGPD: "Para que o tratamento seja lícito, os dados pessoais devem ser tratados com o consentimento da pessoa em causa ou com outro fundamento legítimo previsto por lei, quer no presente regulamento, quer noutra legislação da União ou de um Estado-Membro referida no presente regulamento, incluindo a necessidade de cumprir uma obrigação jurídica aplicável ao responsável pelo tratamento ou a necessidade de executar um contrato no qual a pessoa em causa é parte, ou para efetuar diligências a pedido da pessoa em causa antes da celebração de um contrato".

69 AEPD: "Guía sobre el uso de videocameras para seguridad y otras fines de la AEPD", https://www.aepd.es/documento/guia-videovigilancia.pdf p. 44.

70 Mais amplamente, sobre o "interesse público" e o exercício de poderes públicos como base legítima para o tratamento de imagens, ver INTXAURTIETA MADARIAGA, R., *op. cit.*, p. 3689. Sobre o conceito de "interesse público" no domínio da investigação biomédica sobre a utilização de dados de saúde sem consentimento, ver BARREDA, I., "Big Data / Utilização de dados de saúde sem consentimento na investigação biomédica", *ADS*, n.º 268, março de 2019, pp. 235-240.

71 Sobre esta base de legitimação do tratamento de imagem, embora não seja a mais comum mas tenha um carácter residual, será aplicável aos casos que aqui analisamos e que INTXAURTIETA MADARIAGA descreve como sendo os de controlo em unidades de reanimação, instalação de sistemas de vídeo que permitem o acompanhamento contínuo de doentes afectados por determinadas doenças com o objetivo de vigiar a sua saúde e preservar o seu interesse vital ou a instalação de câmaras de vídeo nas portas de saída de um lar de idosos, assegurando o interesse vital de pessoas que facilmente se poderiam desorientar, *op. cit. cit*, p. 3689.

72 Considera-se que, nos centros e instalações do Ministério Regional da Saúde Universal e Saúde Pública, a base legitimadora é constituída pelo caso previsto no art. 6.1.e) RGPD, ou seja, para garantir a segurança de pessoas, bens e instalações. As finalidades do tratamento seriam a deteção de incidentes de segurança; o controlo e vigilância do acesso aos centros e instalações do Ministério Regional da Saúde Universal e Saúde Pública através do tratamento de imagens ou sons captados com sistemas de videovigilância e que a categoria de dados seria de natureza identificadora: imagem/voz. Informação disponível em:

dos Assuntos Sociais), a base jurídica aplicável ao tratamento monitorizado do residente é considerada como o cumprimento de uma tarefa realizada no *interesse público*, tal como previsto no Art. 6(1)(e) do RGPD, na medida em que a organização de cuidados de saúde que instalou a câmara de vídeo era de natureza pública no caso apresentado neste trabalho[73] .

No entanto, a AEPD também considera outras bases legitimadoras[74]. Assim, refere que neste caso da utilização de câmaras para fins de saúde e sendo os dados de saúde considerados categorias especiais de dados, a legitimação dar-se-ia da seguinte forma: em primeiro lugar, com base no artigo 9.º, n.º 2, alínea c), do RGPD, uma vez que "o tratamento é necessário para proteger *os interesses vitais* do titular dos dados ou de outra pessoa singular, se o titular dos dados não for física ou legalmente capaz de dar o seu consentimento". Em segundo lugar, com base no artigo 9.º, n.º 2, alínea h), do RGPD, uma vez que o tratamento é necessário para efeitos de medicina preventiva, diagnóstico médico, *prestação de cuidados de saúde* ou tratamento com base na legislação da União Europeia ou de um Estado-Membro ou no âmbito de um contrato com um profissional de saúde e sujeito às condições e garantias referidas no artigo 9.

É questionável se o consentimento[75] é necessário no caso de videovigilância por razões de *interesse público* (art. 9.2.g) do RGPD)[76]; para a proteção de *interesses vitais* (art. 9.2.c) do RGPD), bem como por razões de gestão de sistemas e serviços *de saúde e assistência social* (art. 9.2.h) do RGPD)[77]. Geralmente este pedido é feito para dar maiores garantias ao tratamento ou como último recurso, embora como salientámos o art. 6.1.a) do RGPD estabeleça que "o tratamento é lícito se se verificar pelo menos uma das seguintes condições:", onde se inclui, como uma das alternativas, o consentimento dado pelo titular dos dados, sem prejuízo do disposto no art. 9.2.a) do RGPD.

Em todo o caso exige-se que, uma vez dado o consentimento, este seja expresso, não sendo válido o consentimiento tácito (art. 4.11 do RGPD[78]).

https://www.san.gva.es/documents/337738/3057540/7.+Videovigilancia.pdf/42f53e87-99a9-a395-c8f7-6bda9acb459a?t=1676549412795.

[73] A decisão completa está disponível em: https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-gnosjo-2020-11-25.pdf.

[74] AEPD: "Guía sobre el uso de videocameras para seguridad y otras fines de la AEPD", https://www.aepd.es/documento/guia-videovigilancia.pdf p. 44.

[75] Da leitura do art. 6.º, n.º 1 do RGPD verifica-se que não existe hierarquia entre os diferentes fundamentos legítimos, como também interpreta GIL GONZÁLEZ que, no entanto, também nota que este não é um enunciado pacífico entre a doutrina, citando entre outras opiniões ADSUARA VALERA, B. "El consentimiento", cap. X in *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, Piñar Mañas, J.L. dir, Reus, Madrid, 2016, pp. 151-169 *(El interés legítimo en el tratamiento de datos personales*, *La Ley,* Madrid, 2022, pp. 55-56 nota 29). A este respeito, a INTXAURTIETA MADARIAGA observa que o consentimento, enquanto base legitimadora para o tratamento, não vai ser o mais aplicado nestes tratamentos e que tem vindo a perder peso na configuração do direito fundamental, deixando de ser um princípio de acordo com a Diretiva 95/46 para ser mais uma base legítima para o tratamento de acordo com o RGPD. No que respeita ao tratamento de imagens por câmaras de vídeo, na maioria dos casos, não tem sido o fundamento jurídico do tratamento, sendo o título habilitante outro, *op. cit*. p. 368. Por seu turno, RODRÍGUEZ AYUSO entende que, quando o consentimento é solicitado como pressuposto do (e não relacionado com o) serviço prestado, se o tratamento não puder ser baseado num "interesse legítimo", mesmo que o consentimento seja dado, será seguramente inválido, não tendo sido dado livremente, *op. cit*. p. 56, Sobre a relação entre os casos de tratamento lícito e o chamado "interesse legítimo", vide, para além da monografia citada nesta nota de Gil González, MARTOS, N., "Principios (Arts. 6-11)", in *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*, López Calvo, coord., Madrid, Wolters Kluwer, 2018, pp. 353-355.

[76] Como já foi referido, GIL MEMBRADO considera, a propósito da instalação de câmaras de vigilância nos espaços comuns das associações de condóminos, que uma vez aprovado esse acordo em assembleia de condóminos deixaria de ser necessário obter o consentimento do titular dos dados, em virtude do interesse público, como fundamento de legitimação do tratamento, *op. cit*.

[77] De forma duvidosa, considera-se que tais títulos habilitantes poderiam ser incluídos, "Videovigilancia", capítulo 19, *Memento practico Protección de Datos,* Piñar Mañas, J.L. (dir), obra colectiva, Madrid, F. Lefebvre, 2019, p. 495 ap. 6160. Por seu turno, PARDO MARQUINA considera que, nestes casos, poderia ser permitido o tratamento sem o consentimento prévio do titular dos dados, *op. cit*.

[78] Art. 4.11 do RGPD: "o consentimento da pessoa em causa é uma manifestação de vontade, livre, específica, informada e explícita,

Como também se exige que a manifestação de vontade seja "livre", a questão pressupõe uma decisão voluntária tomada por um indivíduo no pleno gozo das suas faculdades, tomada sem qualquer tipo de coação (GT 29)[79]. Como o consentimento pressupõe que o indivíduo *compreenda a informação que lhe é* apresentada, a escolha que faz e que dê uma indicação clara de concordância com a mesma, para cumprir este objetivo deverá ter um nível razoável de compreensão da informação que lhe é fornecida e das implicações da sua decisão[80].

Para o efeito, convém recordar a importância da *obrigação de informação* prévia à instalação de câmaras de vigilância, no âmbito do princípio da responsabilidade pró-ativa, do princípio da transparência e da necessidade probatória[81]. Para o efeito, é necessário que a informação seja prestada ao titular dos dados. Quanto à forma de *prestação* desta informação, que entendemos no duplo sentido deste termo[82], convém precisar que a pessoa em causa recebe a informação mas é o responsável pelo tratamento que a deve prestar por sua iniciativa, implicando necessariamente uma ação da sua parte. Cabe-lhe ainda encontrar uma forma que permita satisfazer as exigências de uma informação "concisa, facilmente acessível e compreensível, que utilize uma linguagem clara e simples e, além disso, se for caso disso, visualizada", por exemplo, através de ícones normalizados, considerandos (58) (60) e arts. 11, 12[83] e 13.º do RGPD[84]. Estes requisitos, embora redigidos de uma forma genérica para qualquer pessoa, serão de particular interesse para

pela qual a pessoa em causa aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento".

TEATINO GÓMEZ, D. et al., "Protección de datos en residencias de ancianos. Adaptación al RGPD en 2023", disponível em https://protecciondatos-lopd.com/empresas/residencias-ancianos-rgpd/#Se_pueden_publicar_fotografias_de_las_habitaciones_de_los_residentes_para_publicitar_la_Residencia.

79 Como refere DEL CASTILLO VÁZQUEZ, I-C., "Consentimiento (Comentario al art. 4.11 RGPD)", cap. 21, *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica De Protección De Datos Personales y Garantía De Los Derechos Fundamentales*, T. I, dir. Troncoso Reigada, A., pp. 683- 684.

80 GIL GONZÁLEZ, acrescentando que esta é a motivação para o facto de o RGPD dar especial atenção à forma como o consentimento das crianças é solicitado e dado, *El interés legítimo en el tratamiento de datos personales*, 2022, ed. La Ley - Wolters Kluwer, p. 77.

81 Sobre as medidas a adotar no âmbito empresarial para dar cumprimento ao princípio da responsabilidade proactiva ou princípio da *responsabilização,* PARDO MARQUINA, V., "Cámaras de videovigilancia: ¿mecanismo de seguridad o intromisión en el Derecho Fundamental a la protección de datos personales?", *Diario La Ley,* N. 9855, 21 de maio de 2021, *La Ley* 5138/2021.

82 Para uma explicação mais detalhada sobre a forma de fornecer, o conteúdo, o momento da informação e as consequências do seu incumprimento, ver ARIAS POU, M. "Transparencia e información que deberá facilitarse cuando los datos personales se obtengan del interesado. El derecho a la información desde el diseño (comentario al artículo 13 RGPD y al artículo 11.1 y 2 LOPDPGD", *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica De Protección De Datos Personales y Garantía De Los Derechos Fundamentales*, T. I, dir. TRONCOSO REIGADA, A. pp. 1366-1379.

83 Art. 12.º, n.º 1, do RGPD: "O responsável pelo tratamento deve tomar as medidas adequadas para *fornecer à pessoa em causa todas as informações* referidas nos artigos 13.º e 14.º, bem como todas as comunicações previstas nos artigos 15.º a 22.º e 34.º relativas ao tratamento, de forma *concisa, transparente, inteligível e facilmente acessível, numa linguagem clara e simples, em* especial as informações especificamente destinadas a uma criança. A informação é prestada por escrito ou por outros meios, incluindo, se for caso disso, por via eletrónica. A pedido da pessoa em causa, a informação pode ser prestada oralmente, desde que a sua identidade seja provada por outros meios".

84 A CNIL indicou na recomendação acima referida que as pessoas em causa (residentes e trabalhadores) devem ser *informadas* antes da instalação de sistemas de videovigilância. No entanto, considera que, no primeiro caso, no que se refere aos residentes, tal seria cumprido através da inclusão de uma cláusula no contrato de alojamento que indique que esse tratamento pode ser aplicado. E esclarece que essa cláusula deve também especificar que esse sistema só deve ser aplicado pelo estabelecimento de alojamento e não pela família. No que diz respeito aos trabalhadores, considera que esta obrigação pode ser cumprida através da inserção, por exemplo, no regulamento interno do estabelecimento, previamente apresentado ao Comité Económico e Social, de uma declaração que indique a possibilidade de instalar sistemas de videovigilância nos quartos dos residentes quando existam motivos razoáveis de suspeita de maus tratos. O empregador deve igualmente assegurar-se de que os trabalhadores foram informados individual e eficazmente (por correio eletrónico, correio postal, etc.).

todos os que sofrem de algum tipo de deficiência intelectual[85] .

A este respeito entende-se que, se for incluído no contrato *ad hoc* como cláusula contratual adicional, o consentimento não é considerado suficientemente dado (mas sim interpretado como uma falta de consentimento libre, sendo imposto) se o tratamento de dados não tiver passado o teste de proporcionalidade, o critério de intervenção mínima e o teste de adequação[86]. Ou seja, quando a instalação do sistema de videovigilância for desproporcionada em relação ao objetivo de segurança prosseguido. Esta é a interpretação do *Information Commissioner's Office* (ICO), da AEPD, da APDCAT e do CTPDA em relação ao consentimento para o tratamento de dados biométricos para o controlo e/ou registo da jornada de trabalho[87].

Para além do facto de ter de existir uma base legitimadora (*ex* art. 6.º, n.º 1, do RGPD), tal como referido pela CNIL francesa[88], os princípios da *necessidade e da proporcionalidade* devem ser respeitados no tratamento destes dados pessoais. Para este efeito e tendo em conta os elevados riscos que este tratamento pode gerar para os direitos e liberdades das pessoas em causa, a organização que implementa este sistema de videovigilância terá de efetuar uma avaliação de *impacto sobre a proteção de dados* (APD)[89] . As condições de implementação do sistema de videovigilância devem ser definidas de forma a minimizar os riscos para as pessoas em causa e a conformidade do tratamento com o RGPD deve ser demonstrada em caso de inspeção (artigos 35.º e 36.º do RGPD)[90] . Esta análise deve conter uma descrição pormenorizada do ficheiro implementado, abrangendo tanto os aspectos técnicos como os operacionais[91]. Por sua vez, a organização que implementa o sistema deve dar especial ênfase às razões pelas quais considerou que *outros meios menos intrusivos* seriam mais ineficazes[92], bem como

85 O mesmo é afirmado em *Estudio sobre el sistema de protección de datos personales con finalidad de prevención, detección e investigación policial de infracciones penales,* coord. FERNÁNDEZ GONZÁLEZ, C. M., Madrid, Ministerio del Interior, 2022, p. 104, https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/seguridad-ciudadana/Estudio_sobre_el_sistema_de_proteccion_de_datos..._126220091.pdf.

86 Assim, foi aplicada uma coima de 4000 euros num arrendamento para habitação pela instalação de uma câmara na cozinha do imóvel, para além da ordem de remoção do dispositivo em causa, arts. 83.5 a, 58.2 RGPD, por violação dos princípios básicos de tratamento, incluindo as condições de consentimento nos termos dos arts. 5, 6, 7 e 9 do RGPD, Processo n.º. EXP202207199 AEPD. Estes princípios aplicam-se mesmo à autorização da instalação de câmaras pelas Forças e Corpos de Segurança, AEPD, Guía sobre el uso de videocameras para seguridad y otras fines, https://www.aepd.es/documento/guia-videovigilancia.pdf, p. 29. 1.b) (execução de um contrato), GIL GONZÁLEZ, de forma semelhante ao raciocínio exposto, afirma que a mera incorporação de uma cláusula no contrato relativa ao tratamento de dados pessoais não legitima a atividade, sendo que as demais obrigações impostas pelo RGPD também devem ser cumpridas. Quando estas circunstâncias se verificam, a norma presume que os interesses de ambas as partes - titular dos dados e responsável pelo tratamento - estão equilibrados, pelo que o tratamento tem luz verde, *op. cit.*

87 Como explica ESPUGA TORNÉ, G., se houver consentimento com alternativa este foi dado livremente, ainda que tal não signifique que o tratamento seja proporcional. Assim, é possível ter a base legal mas não passar no teste da proporcionalidade que, no caso em apreço, será extremamente complexo devido à existência de medidas menos gravosas para os titulares dos dados e, consequentemente, o tratamento não poderá ser efectuado, "La ICO sí considera adecuado el consentimiento para tratar datos biétricos para control y/o registro de jornada", 27-11-2023, Linkedin.

88 CNIL: "Vidéosurveillance dans les chambres d'Ehpad", informação disponível em https://www.cnil.fr/sites/cnil/files/2023-02/projet_de_recommandation_videosurveillance_ephad.pdf.

89 Para mais informações sobre o EIPD, consultar o sítio Web da AEPD https://www.aepd.es/preguntas-frecuentes/2-rgpd/10-evaluacion-de-impacto.

90 Para o efeito, a AEPD publicou um guia para facilitar o cumprimento da chamada *accountability* ou "responsabilidade pró-ativa", cuja gestão se baseia numa abordagem baseada no risco, https://www.aepd.es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf.

91 No que diz respeito às obrigações de proteção de dados dos lares, é necessário manter um registo das actividades de tratamento. Deixa de ser necessário registar os processos na AEPD, mas passa a ser obrigatório conservar os processos num registo separado.

92 Considera que as organizações devem considerar a implementação de meios alternativos e menos intrusivos (como um botão de chamada de emergência sem fios) para garantir a segurança dos resi-

às salvaguardas a implementar para garantir que os empregados não são sujeitos a vigilância contínua enquanto trabalham no estabelecimento; às medidas para garantir a confidencialidade dos dados e às precauções tomadas para proteger a privacidade dos hóspedes[93]. No entanto, se se verificar que o nível de risco residual continua a ser elevado, o responsável pelo tratamento deve recorrer à autoridade de controlo francesa (n.º 5 do artigo 36.º do RGPD)[94].

Partindo do facto de estarmos perante casos de elevado risco para os direitos e liberdades das pessoas singulares, a AEPD estabelece eventuais medidas ou garantias relativamente a sujeitos considerados vulneráveis (idosos, menores, pessoas com deficiência, etc.), que devem ser adoptadas pelos responsáveis pelo tratamento e subcontratantes (art. 28.º, n.º 2, al. e) do RGPD[95]). Por sua vez, classifica uma lista de factores de risco identificados na regulamentação sobre o tratamento de dados pessoais, entre os quais inclui a categoria dos *titulares dos dados,* enumerando de forma não exaustiva "trabalhadores, menores, idosos, pessoas em situação vulnerável, vítimas, pessoas com deficiência, etc.". E, dentro deste grupo, considera os idosos com algum grau de incapacidade (e as pessoas com deficiência sem a circunstância da idade) com um elevado nível de risco. Quanto aos idosos, apenas devido à sua idade, é atribuído apenas um nível de risco médio, ao contrário das pessoas que sofrem de doenças mentais, cujo nível de risco é classificado como muito elevado[96].

Se, para além das razões normais de salvaguarda da segurança das pessoas, dos bens e das instalações e/ou das razões de saúde ou de assistência social que justificam a implementação de sistemas de videovigilância, existirem fortes suspeitas de maus tratos contra um residente, circunstância que levou a autoridade de controlo francesa a pronunciar-se, como acima se explicou, com base num conjunto de indícios corroborantes (hematomas, alterações de comportamento, etc.), uma organização deve poder instalar um sistema de videovigilância, indicando uma série de salvaguardas em consonância

dentes, tais como procedimentos de comunicação e monitorização de eventos preocupantes. Relativamente a este princípio de intervenção mínima a favor de outros meios menos intrusivos, ver TJUE, 11 de dezembro de 2019, *TK/Asociația de Proprietari bloc M5A-ScaraA*, Processo C-708/18, n.º 49, EUR-Lex Documento 62018CJ0708, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A62018CJ0708. Por outro lado, BALLESTEROS MOFFA refere que, embora se mova nas "areias movediças" dos conceitos jurídicos indeterminados, exige a inexistência de outra medida mais moderada para atingir a mesma finalidade de segurança; o que encontra aplicações legais específicas, como o regime de autorização quando utilizado pelas Forças e Corpos de Segurança, ou a captação excecional da via pública relativamente ao regime geral (art. 22.º, n.º 2, da LOPDGDD), *op. cit.*, p. 166.

93 A este respeito especifica que o responsável pelo tratamento, ao assegurar que o seu tratamento está em conformidade com o RGPD e a lei francesa sobre a proteção de dados, deve garantir que o período de conservação é limitado a alguns dias se as imagens não revelarem quaisquer maus-tratos ao residente ou, se revelarem, à duração do processo judicial.

94 Art. 36.5 do RGPD: "Em derrogação do n.º 1, a legislação dos Estados-Membros pode exigir que os responsáveis pelo tratamento consultem a autoridade de controlo e obtenham a sua autorização prévia em relação ao tratamento efectuado por um responsável pelo tratamento no exercício de funções de interesse público, em especial o tratamento relacionado com a proteção social e a saúde pública". Ver também sobre os requisitos de cumprimento da LOPDGDD, de forma resumida, " Proteção de dados em lares de idosos. Adaptação ao RGPD em 2023", disponível em https://protecciondatos-lopd.com/empresas/residencias-ancianos-rgpd/#Se_pueden_publicar_fotografias_de_las_habitaciones_de_los_residentes_para_publicitar_la_Residencia.

95 Art. 28.e) RGPD: "Quando os dados são tratados sobre grupos de pessoas em situação particularmente vulnerável e, em particular, sobre menores e pessoas com deficiência". Com exceção desta disposição, é censurável que os regulamentos de proteção de dados não prestem atenção expressa ao consentimento prestado por pessoas com deficiência ou que necessitem de medidas de apoio, enquanto existe regulamentação expressa para menores, como o art. 7 LOPDGDD ou a referência expressa a crianças como interessadas, no que diz respeito ao "interesse legítimo" do art. 6.1.f) RGPD, para além dos considerandos (38) e (75). Portanto, em relação à prestação do consentimento, devemos entender uma remissão para o regime geral.

96 AEPD, Guia: "Gestão de riscos e avaliação de impacto no tratamento de dados pessoais", junho de 2021, https://www.aepd.es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf , p. 78.

com este objetivo. Refere-se, em particular, à limitação da ativação ao longo do tempo; à restrição da captação de imagens em áreas privadas (casas de banho, chuveiros); à desativação do sistema de videovigilância quando se recebe a visita de familiares; bem como ao estabelecimento e aplicação de um quadro interno sobre as condições que justificam a instalação deste tipo de sistema. Além disso entende que, se o pedido partir do residente ou dos seus familiares, deve obter o consentimento do interessado (ou do seu representante, se o estado do residente não lhe permitir dar o seu consentimento); quando a iniciativa partir do estabelecimento, deve ser oferecida ao interessado a possibilidade de recusar a instalação deste tipo de dispositivo, desde que tenha o discernimento necessário. Caso contrário será o seu representante a autorizar a instalação, como acontece no direito francês[97] .

De qualquer modo, a Autoridade Francesa para a Proteção de Dados acaba por advertir no seu relatório intercalar que um sistema de videovigilância instalado com o objetivo de prevenir incidentes de segurança no *quarto de* uma pessoa alojada parece, em princípio, *desproporcionado,* na medida em que "constitui um ataque particularmente forte à dignidade das pessoas alojadas que são constantemente filmadas nos seus quartos e é suscetível de sujeitar os empregados a uma vigilância contínua, o que constituiria uma infração"[98]. Este facto foi igualmente considerado pela autoridade de supervisão sueca[99].

Por fim refira-se, em conclusão, que nos casos de videovigilância acima descritos as sanções por violação dos princípios básicos do tratamento de dados pessoais (*ex* arts. 5.º, 6.º, 7.º, 9.º, 13.º, 35.º e 36.º, basicamente, RGPD), nos termos do art. 83.º do RGPD), de acordo com o art. 83.º do RGPD, variaram entre cerca de 5300 e 4000 euros para a instalação de uma câmara numa casa privada partilhada, respetivamente no corredor e na cozinha, passando por 6000 euros num apartamento turístico, no que respeita à AEPD, até cerca de 17800 euros (200 000 SEK) no caso sueco analisado. Seria ainda possível intentar acções de responsabilidade civil (ou acções contra a administração, se for caso disso), consoante a natureza do responsável pelo tratamento de dados ou do centro de cuidados (privado ou público), em caso de danos causados às pessoas em causa em resultado de violações do RGPD, *ex* art. 82.º do RGPD ou, de forma compatível, por violação dos direitos à honra, à privacidade pessoal e familiar e à autoimagem, nos termos da LO 1/1982, de 5 de maio[100].

A contextualização das sanções acima referidas, com as restantes infracções identificadas pela nossa autoridade de controlo, destaca no seu Relatório

[97] CNIL: "Vidéosurveillance dans les chambres d'Ehpad", informação disponível em https://www.cnil.fr/sites/cnil/files/2023-02/projet_de_recommandation_videosurveillance_ephad.pdf.

[98] Do mesmo modo, a AEPD afirma que, embora o objetivo seja a videovigilância, a utilização de câmaras nos quartos dos doentes para que os seus familiares possam ver o seu estado de saúde em "streaming" é considerada desproporcionada, "Guía sobre le uso de videocameras para seguridad y otras finalidades", https://www.aepd.es/documento/guia-videovigilancia.pdf, p. 44.

[99] A Autoridade Sueca para a Proteção de Dados concluiu que o Comité Social não tinha demonstrado que o interesse da vigilância se sobrepunha ao direito do residente à integridade pessoal e a uma esfera privada protegida. A Inspeção de Dados observou que a forma como a vigilância por câmara tinha sido efectuada implicava um controlo extensivo do residente, envolvendo uma interferência significativa na sua integridade pessoal. Concluiu que o tratamento de dados pessoais era desproporcionado em relação à sua finalidade e que não tinha cumprido os requisitos de exatidão estabelecidos no artigo 5.º, n.º 1, alínea a), da Diretiva e no RGPD.

[100] Sobre o procedimento sancionatório e a forma de atuação em eventuais casos de responsabilidade civil, remetemos para o extenso tratamento abordado por MORENO MARTÍNEZ, que também se debruça sobre a compatibilidade das acções civis em matéria de proteção de dados, e a que resulta da aplicabilidade da LO 1/1982, de 5 de maio, sobre a tutela civil do direito à honra, à intimidade pessoal e familiar e à própria imagem, *op. cit.*

2022 que, de todos os processos sancionatórios e coimas aplicadas, a área mais frequente dos primeiros foi a videovigilância (164 processos, contra 147 no ano anterior). No entanto, o maior volume de coimas foi para casos relacionados com serviços de Internet[101]. No entanto, em comparação com o número de queixas recebidas em 2021, a videovigilância registou um aumento de 26 % e os casos de serviços de Internet mantiveram-se praticamente inalterados[102].

[101] Este facto explica-se pela dimensão geralmente mais reduzida dos processos de videovigilância, quer em termos de gravidade, quer em termos do tipo de infrator (pessoas singulares) e da sua relação com a eficácia das coimas (em termos de proporcionalidade e dissuasor), face ao elevado impacto das infrações na área da Internet e à presença de grandes empresas nesta área. Assim, a maior coima aplicada no ano corresponde a um processo neste sector, em que a Google LLC foi multada em 10 milhões de euros por violação dos artigos 6.º e 17.º do RGPD e condenada a tomar as medidas necessárias para corrigir a infração e evitar a sua repetição no futuro, Relatório Anual 2022, pp. 92-93 e 150, disponível em https://www.aepd.es/documento/memoria-aepd-2022.pdf.

[102] Videovigilância: 1.735 queixas em 2021, em comparação com 2.196 em 2022. Serviços de Internet: 2 220 em 2021, e apenas mais um caso em 2022 (2 221), Relatório Anual 2022, pp. 92-93 e 150, disponível em https://www.aepd.es/documento/memoria-aepd-2022.pdf,p. 149.