A videovigilância e a compressão da privacidade

Lurdes Dias Alves*

Resumo: Videovigilância e privacidade são conceitos antagónicos mas que se apresentam como um dilema preocupante nesta sociedade do século XXI. Neste texto procuraremos analisar a necessidade de implementação de sistemas de videovigilância em locais públicos, tendo em conta a salvaguarda de direitos fundamentais e a devida adequação dessa instalação e implementação com o Regulamento Geral de Proteção de Dados. Estabelecendo-se o confronto de direitos legalmente protegidos – direito à privacidade *versus* direito à segurança, confronto que merece a devida reflexão. Será a privacidade (tal como a conhecemos) um conceito em vias de extinção ou ainda tem cabimento nesta sociedade cada vez mais pátula? Facilmente concluímos que, nesta sociedade cada vez mais aberta e adepta das novas tecnologias ao dispor, em que a vida privada, e até a vida familiar, é constantemente exposta sem a menor prudência, e até recato, deixou de ter cabimento a noção, e o sentido, da privacidade, tal como a conhecemos.

Palavras Chave: *Videovigilância; privacidade; direitos fundamentais; segurança.*

Abstract: Video surveillance and privacy are antagonistic concepts that present themselves as a worrying dilemma in this 21st century society. In this text we will analyse the need to implement video surveillance systems in public places, considering

---

* Licenciada em Direito pela Universidade Autónoma de Lisboa. Pós-graduada em Direito Comercial e Direito Societário pela Universidade Católica Portuguesa – Escola de Lisboa. Mestre em Direito (especialidade de Ciências Jurídicas) pela Universidade Autónoma de Lisboa. Doutoranda em Direito (especialidade de Ciências Jurídicas) na Universidade Autónoma de Lisboa, onde investiga o tema: "*A proteção de dados pessoais e o sigilo bancário – A derrogação da privacidade*". Investigadora integrada no RATIO LEGIS – Centro de Investigação e Desenvolvimento em Ciências Jurídicas da Universidade Autónoma de Lisboa. Cocoordenadora de Pós-Graduações em Proteção de Dados Pessoais, Privacidade e Cibersegurança na UE, na Autónoma Academy (Escola de Pós-graduações da Universidade Autónoma de Lisboa).

the safeguarding of fundamental rights and the adequate adaptation of this installation and implementation with the General Regulation of Data Protection. Establishing the confrontation of legally protected rights – the right to privacy versus the right to security, a confrontation that deserves due reflection. Is privacy (as we know it) an endangered concept, or does it still fit in this increasingly patulus society? We easily conclude that in this increasingly open society and adept at the new technologies available, where private life, and even family life, is constantly exposed without the slightest prudence, and even notion, and sense of privacy as we know it.

Keywords: *Video surveillance; privacy; fundamental rights; safety.*

Introdução

É indubitável que vivemos numa sociedade assente na tecnologia – e, por exemplo, basta pensar nas câmaras de videovigilância em grande parte do espaço público e privado; as instituições de crédito e sociedades financeiras sabem onde e como gastamos o nosso dinheiro (mais ainda, sabem como o ganhamos); as grandes superfícies sabem os produtos que consumimos, quais os nossos gostos e tendências, ao ponto de poderem definir um perfil pessoal dos nossos hábitos e rotinas; os «*radares*» e a «*via verde*» sabem por onde nos deslocamos e para onde viajamos; máquinas de «*raio X*» nos aeroportos visualizam os nossos pertences (e até o nosso corpo); a utilização de «*cookies*» permite determinar a nossa utilização e navegação na internet (a tão usualmente designada pegada digital); estas, entre muitas outras situações, mostram a variedade de casos em que, voluntária ou involuntariamente, a nossa privacidade fica mitigada ou até mesmo comprometida.

Nos últimos anos tem-se assistido a um crescimento exponencial do volume de dados gerados por sistemas de informação, em redes sociais, aparelhos móveis, entre outros, ligados em rede e que geram dados, interligados e a uma velocidade não antes imaginável.

O RGPD, apesar de encerrar em si muitos princípios, regras gerais, direitos e obrigações que já constavam da Diretiva N.º 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995 (Diretiva), a verdade é que vem introduzir alterações importantes ao regime anteriormente aplicável.

Uma das alterações introduzidas pelo RGPD é o fim do controlo prévio exercido pela Autoridade Nacional, no caso português, a CNPD. Assim, o tratamento de dados pessoais, onde naturalmente se inclui a videovigilância, deixa de ter a obrigatoriedade de autorização prévia.

Em Portugal e quanto à videovigilância, este facto assume especial relevância, dado que, a Lei de Segurança Privada (Lei 34/2013, de 16 de maio) estabelecia os requisitos a respeitar na instalação e exploração de um sistema de videovigilância. Contudo, sendo que a videovigilância não é um recurso exclusivo da segurança privada, tais requisitos não se impunham se a videovigilância fosse explorada fora do contexto da segurança privada. E é precisamente neste ponto que o controlo prévio exercido pela CNPD era fundamental, permitia que a Comissão estabelecesse as condições de exploração do sistema, especialmente quanto ao prazo máximo de gravação das imagens (geralmente 30 dias), a finalidade (usualmente, a proteção de pessoas e bens), os destinatários dos dados (em regra, apenas órgãos de polícia criminal e autoridades judiciárias, para utilização em processos crime) e o direito de informação (através da afixação em local visível da informação sobre a existência de videovigilância).

Excluindo o RGPD a obrigatoriedade do controlo prévio, nem definindo as regras a cumprir na utilização de videovigilância, existe a necessidade de Portugal, internamente e sem prejuízo da aplicabilidade do Regulamento, criar legislação que regule e fixe os limites da utilização da videovigilância.

Neste contexto, considera-se adequado analisar algumas questões inerentes à utilização da videovigilância, desde logo, enquanto meio de recolha de dados pessoais, a sua utilização à luz do RGPD, a eventual necessidade de avaliação prévia de impacto sobre a proteção de dados e as finalidades, da utilização, previstas em Portugal.

1. A Videovigilância enquanto meio de recolha de dados pessoais

É consensual a definição que a videovigilância se traduz na recolha de imagens por meio eletrónico e que constituem dados pessoais "*informação relativa a uma pessoa singular identificada ou identificável*" (n.º 1 do art. 4.º do RGPD). Logo, as imagens recolhidas por sistema de videovigilância constituem ou, pelo menos, são suscetíveis de constituir dados pessoais,

desde que recolham imagens de pessoas, de objetos ou de equipamentos que permitam, ainda que de forma indireta, a identificação concreta de pessoas.

A este propósito, sempre se dirá que, para que as imagens de videovigilância constituam dados pessoais, não é necessário que integrem imagens explícitas de pessoas, mas tão só imagens que permitam identificar ou localizar pessoas[1]. Sublinha-se que a imagem de pessoas, para além da salvaguarda no contexto da legislação de proteção de dados pessoais, encontra-se legalmente protegida, desde logo, na CRP que, no art. 26.º, n.º 1, ressalva que a todos é reconhecido, entre outros, o direito à imagem e à reserva da intimidade da vida privada. De igual modo, o CC, no art. 79.º, prevê o direito à imagem: "*o retrato de uma pessoa não pode ser exposto, reproduzido ou lançado no comércio sem o consentimento dela...*", bem como o CP que, no art. 199.º, criminaliza as gravações e fotografias ilícitas, prevendo a punição de quem "*fotografar ou filmar outra pessoa, mesmo em eventos em que tenha legitimamente participado*"[2]. Assim, a videovigilância, ao recolher imagens de pessoas, é suscetível de derrogar o direito à imagem e à reserva da vida privada[3].

De facto, existe um conflito de interesses entre o direito à privacidade e o interesse público, ou seja, a promoção e garantia de segurança *versus* o direito à privacidade e o direito à liberdade impõe um exercício

---

[1] Imagens que permitam identificar uma viatura, através da matrícula ou de outra caraterística inequívoca, que permita atribuir a propriedade ou utilização dessa viatura a determinada pessoa, constitui dado pessoal.

[2] Sendo estas as regras, existem, naturalmente, exceções, como a prevista no n.º 2 do art. 79.º do CC, que prevê que "*Não é necessário o consentimento da pessoa retratada quando assim o justifiquem a sua notoriedade, o cargo que desempenhe, exigências de polícia ou de justiça, finalidades científicas, didáticas ou culturais, ou quando a reprodução da imagem vier enquadrada na de lugares públicos, ou na de factos de interesse público ou que hajam decorrido publicamente.*".

[3] A este propósito, o TC, no Acórdão n.º 255/2002, 8 de Julho de 2002, p. 5239, debruçando-se sobre a Lei de Segurança Privada, à data em vigor (Decreto-Lei n.º 231/98 de 22 de julho) e declarando inconstitucional alguns dos seus preceitos, refere que "*Apesar de a lei impor a afixação, em local bem visível nos lugares objecto de vigilância com recurso àqueles meios, de avisos a informar do facto, prescrevendo assim uma espécie de consentimento implícito do cidadão que permanece naqueles locais, a verdade é que tal medida legal constitui também ela uma verdadeira restrição aos direitos à imagem e à reserva da intimidade da vida privada e familiar*", acrescentando, no entanto, que "*O interesse público inerente à actividade de segurança privada, expresso pelo próprio legislador, justificará as restrições em causa*".

permanente, para preservar o bem jurídico e manter o seu equilíbrio. Não foi certamente por mero acaso que, o legislador constitucional não dissociou a liberdade da segurança (art. 27.º CRP), criando normas que se pretendem indissociáveis, não sendo, ainda assim, direitos absolutos, tanto que "*a liberdade de cada um é relativizada pela liberdade de todos*"[4]. A videovigilância, pela proteção e salvaguarda dos direitos fundamentais que possa fazer perigar, tem sido objeto de vastas análises e não raras vezes de reservas quanto à sua utilização.

2. A videovigilância à luz do Regulamento Geral de Proteção de Dados

Começamos por salientar que embora o RGPD seja aplicável a todas as operações de dados em cujas atividades se aplique o direito da União Europeia, não se aplica ao tratamento de dados efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, bem como, também não se aplica quando efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas (art.º 2.º do RGPD).

O tratamento de dados de videovigilância, de modo sintético, pode absorver em si, por um lado, regras genéricas, por serem aplicáveis ao tratamento de todos os dados pessoais e, por outro lado, regras específicas, por serem aplicáveis em exclusivo à videovigilância.

Considerando como regras genéricas, os princípios da licitude, lealdade e transparência (art.º 5.º do RGPD), na origem do tratamento de dados pessoais tem de existir uma fonte de licitude – o consentimento do titular dos dados; execução de um contrato; cumprimento de uma obrigação legal; realização de um interesse legítimo; defesa de interesses vitais (*v.g.* saúde), exercício de funções de interesse público (art.º 6.º do RGPD).

Ainda, deve-se observar os princípios relativos ao tratamento de dados pessoais: o princípio da limitação das finalidades – a recolha e tratamento de dados pessoais deve ter uma finalidade determinada, explícita e legítima,

---

[4] Conforme afirma Dias, Manuel Domingos Antunes. *Liberdade, Cidadania e Segurança*. Coimbra: Almedina, 2001, p. 7.

não podendo posteriormente ser utilizados para outra finalidade que não aquela que previamente esteja identificada; princípio da minimização de dados – os dados a recolher e tratar deverão ser os mínimos e indispensáveis à finalidade a que se destinam, devendo respeitar critérios de proporcionalidade (adequação, necessidade e proporcionalidade em sentido estrito); princípio da exatidão – os dados devem ser exatos e atualizados, devendo ser adotadas medidas tendentes a que os eventuais dados inexatos sejam apagados ou retificados; princípio da limitação da conservação – devem ser definidos prazos limitativos para a conservação dos dados, devendo estes ser preservados apenas durante o prazo em que se mostrem necessários e adequados à finalidade para a qual foram recolhidos; princípio da integridade e confidencialidade – devem ser adotadas medidas de segurança que garantam a proteção contra o tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental; e o princípio da responsabilidade – o responsável pelo tratamento dos dados é responsável pelo cumprimento dos princípios atrás identificados e cabe a este, demonstrar e comprovar esse cumprimento (n.º 2 do art.º 5.º do RGPD).

Quanto a regras específicas a obedecer na exploração de um sistema de videovigilância, partindo do princípio de que estas regras não contrariam o já previsto especialmente na Lei de Segurança Privada, bem como nas autorizações emitidas pela CNPD, ainda que ao abrigo do RGPD, deverão considerar-se: as gravações de imagem obtidas pelos sistemas de videovigilância devem ser conservadas, em registo codificado, pelo prazo de 30 (trinta) dias contados desde a respetiva captação, findo o qual devem ser destruídas[5]; todas as pessoas que tenham acesso às gravações realizadas, em razão das suas funções, devem sobre as mesmas guardar sigilo[6]; nos locais objeto de vigilância com recurso a câmaras de vídeo é obrigatória

[5] Salvo expressa indicação legal em contrário, *v.g.*, o previsto na Lei 51/2006 de 29 de agosto, Lei n.º 54/2012 de 6 de setembro, em que os prazos são de 180 e 90 dias, respetivamente.

[6] Salvo expressa indicação legal em contrário (*v.g.*, o previsto na Lei 51/2006 de 29 de agosto) é proibida a cessão ou cópia das gravações obtidas, só podendo ser utilizadas nos termos da legislação processual penal, com eventual possibilidade da sua utilização para efeitos de apuramento de responsabilidade disciplinar, na medida em que o sejam no âmbito do processo penal.

a afixação, em local bem visível, do sinal identificado da existência de câmaras de vídeo[7]-[8].

3. Avaliação Prévia de Impacto sobre a Proteção de Dados

Embora com o RGPD tenha deixado de existir a figura do controlo prévio, anteriormente exercido pela CNPD, em certa medida, o controlo prévio passará a ser efetuado pelo EPD ou, do inglês, DPO (art.º 39.º do RGPD). Todavia, existe agora a figura da consulta prévia, segundo a qual o responsável pelo tratamento deve dirigir-se à autoridade de controlo antes de proceder a um tratamento de dados pessoais quando se tenha verificado, após uma prévia AIPD (art.º 35.º do RGPD), que se está perante um elevado risco para os direitos e liberdades das pessoas singulares.

Entre as singularidades e particularidades introduzidas pelo RGPD, encontramos a figura do EPD, que, não sendo uma figura nova no quadro da proteção de dados pessoais, individualizou-se assumindo-se como um dos elementos mais determinantes no seio das organizações, para a criação e/ou promoção de uma cultura de proteção de dados pessoais, e uma garantia permanente de *compliance* nesta área tão sensível.

A figura do EPD nas organizações não é nova. A Diretiva não obrigava as organizações a nomear um EPD, mas, ainda assim, a prática da nomeação de

---

[7] Cfr. anexo VIII da Portaria 273/2013, de 20 de agosto, acompanhado da seguinte informação: a) A existência e localização das câmaras de vídeo, *v.g.,* pode colocar-se no local objeto de vigilância uma informação com as seguintes menções «*neste espaço, existem 6 câmaras de videovigilância localizadas nos seguintes espaços: hall (2 câmaras), corredor norte (3 câmaras) e corredor sul (1 câmara)*»". b) A menção «*Para sua proteção, este local é objeto de videovigilância*»; c) A entidade de segurança privada autorizada a operar o sistema, pela menção do nome e alvará ou licença (no caso de a operação ser garantida por entidade de segurança privada); d) A identificação do responsável pelo tratamento dos dados recolhidos perante quem os direitos de acesso e retificação podem ser exercidos.

[8] Contudo, as câmaras, ou outros meios de captação de imagem, não podem incidir sobre: a) Vias públicas ou propriedades limítrofes, exceto no que seja estritamente necessário para cobrir os acessos ao imóvel; b) A zona de digitação de códigos de caixas multibanco ou outros terminais de pagamento ATM; c) O interior de áreas reservadas a clientes ou utentes onde deva ser respeitada a privacidade, designadamente instalações sanitárias, zonas de espera e provadores de vestuário; d) O acesso e o interior de áreas reservadas aos trabalhadores, designadamente vestiários e instalações sanitárias.

EPD desenvolveu-se em várias organizações dos Estados-Membros ao longo dos anos. Ainda antes da adoção do RGPD, o GT29[9] pugnava pela função do EPD como um pilar da responsabilidade, sendo que, a nomeação de um EPD poderia facilitar a conformidade com o RGPD e, além disso, propiciar uma vantagem competitiva às empresas que nomeassem um EPD[10].

Além de facilitar a conformidade através da implementação de instrumentos de responsabilização (*v.g.*, viabilizando avaliações de impacto sobre a proteção de dados e efetuando ou viabilizando auditorias), os EPD[11] são também intermediários com os *stakeholders* mais relevantes da organização, encimados pela CNPD.

A AIPD, sendo uma das inovações no tratamento de dados pessoais, é indiciadora de preocupação quanto à segurança dos dados e da importância

---

[9] Equipa instituída ao abrigo do artigo 29.º da Diretiva 95/46/CE, foi órgão consultivo europeu independente em matéria de proteção de dados e privacidade. As suas atribuições estiveram descritas no artigo 30.º da Diretiva 95/46/CE e no artigo 15.º da Diretiva 2002/58/CE.) Grupo este que deu lugar após 25 de maio de 2018 com a eficácia plena do RGPD, ao Comité Europeu para a Proteção de Dados.

[10] *Guidelines on Data Protection Officers from WP 29*. [Em linha]. Adotadas em 13 de dezembro de 2016. (Última redação revista e adotada em 5 de abril de 2017. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048. p.4. (acedido a 20/05/2018).

[11] A figura do EPD, apesar de não carecer de certificação profissional para o efeito, é designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados. A sua existência não é obrigatória para todos os tratamentos de dados, mas apenas para as situações previstas no art.º 37.º do RGPD, destacando-se aquelas em que o tratamento é efetuado por uma entidade pública, nomeadamente pelo Estado, regiões autónomas, autarquias locais, entidades administrativas independentes, institutos públicos, instituições de ensino superior públicas de natureza fundacional, empresas públicas sob forma jurídico pública e associações públicas. É, ainda, necessário designar um EPD quando as operações de tratamento exijam um controlo regular e sistemático dos titulares dos dados em grande escala, ou quando sejam tratados dados em grande escala de categorias especiais de dados ou de dados pessoais relacionados com condenações penais e infrações, estando estes definidos nos art.º 9.º e 10.º do RGPD, respetivamente. As funções do EPD devem ainda compreender todas as questões relacionadas com a proteção de dados, informando e aconselhando o responsável pelo tratamento ou o subcontratante, controlando o cumprimento das regras e requisitos, nomeadamente o previsto no RGPD, prestando aconselhamento e controlando a realização da avaliação prévia de impacto, bem como cooperando e sendo o ponto de contacto com a autoridade de controlo (art.º 39.º do RGPD).

a esta atribuída. O art.º 32.º do RGPD prevê que "o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, destacando, nomeadamente, as seguintes possíveis medidas: a pseudonimização e a cifragem dos dados pessoais; a capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento; a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico; um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento".

No tratamento de dados de videovigilância e considerando que estes são suportados informaticamente, deverá o sistema possuir as habituais medidas de segurança de qualquer sistema informático, que garantam a sua permanente disponibilidade, integridade e confidencialidade. Assim, o acesso a imagens deverá ser precedido de controlos físicos[12] e controlos lógicos[13].

A retirada do sistema de imagens gravadas deverá, para além de restrita a pessoas identificadas segundo critérios de necessidade, obrigar a justificação no próprio sistema. Tratando-se de sistema de videovigilância, cujas imagens apenas possam ser utilizadas para fins processuais penais, uma justificação prática e funcional será, por exemplo, registar no sistema o NUIPC para o qual as imagens serão disponibilizadas.

Ainda no que concerne à segurança dos dados, e não obstante as medidas de segurança que devem ser implementadas[14], sempre que ocorra um incidente de segurança que afete dados pessoais, ou se eventualmente os

---

[12] Controlo do acesso ao espaço físico onde as imagens podem ser visualizadas.

[13] Utilização de login e password individual e personalizado para acesso ao sistema, bem como registo desses mesmos acessos, que permitam conhecer quem acedeu, quando acedeu, ao que acedeu e especialmente que tratamento efetuou.

[14] O RGPD exige que o responsável pelo tratamento aplique todas as medidas técnicas de proteção e de organização para apurar imediatamente a ocorrência de uma violação e para informar rapidamente a autoridade de controlo e os titulares dos dados, deverá ainda, comprovar que a notificação foi enviada sem demora injustificada e importa ter em conta, em especial, a natureza e a gravidade da violação e as respetivas consequências e efeitos adversos para o titular dos dados.

dados forem violados[15] e acedidos por quem não o possa fazer ou utilizados para fim diverso da finalidade prevista, o responsável pelo seu tratamento notifica a autoridade de controlo (Art.º 33.º do RGPD) e, se essa violação for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, essa comunicação é efetuada, também, ao titular dos dados respetivos (Art.º 34.º do RGPD).

Neste contexto, a CNPD não difundiu, ou ainda não difundiu, uma lista de tipos de tratamento de dados cuja avaliação prévia de impacto não é obrigatória, tal como previsto no n.º 5 do art.º 35.º do RGPD. Ainda assim, e considerando que a alínea c) do n.º 3 do art.º 35.º do RGPD prevê a obrigatoriedade de realização desta avaliação em caso de "*controlo sistemático de zonas acessíveis ao público em grande escala*", é defensável que, por defeito, esta avaliação será obrigatória para a videovigilância, particularmente se esta for utilizada em zonas acessíveis ao público em grande escala (*v.g.* uma gare de transportes, um centro comercial ou um arruamento público).

Na senda do que acima foi aqui defendido, a CNPD elaborou e publicitou o Projeto de Regulamento n.º 1/2018[16] relativo à lista de tratamento de dados pessoais sujeitos a AIPD, onde, além do tratamento de dados previstos no n.º 3 do artigo 35.º do RGPD, determina que estão sujeitos a prévia AIPD um elenco de tratamento de dados pessoais. No n.º 6 está prevista a obrigatoriedade de prévia AIPD no tratamento de dados pessoais recolhidos por sistemas de videovigilância.

Ainda que, em algumas situações não seja obrigatória a AIPD, esta pode ser realizada por iniciativa própria e é dispensável para os tratamentos que

---

[15] Em caso de *data breach* o responsável pelo tratamento fica obrigado a assegurar que terá, sempre, «conhecimento» de eventuais violações em tempo útil, para que possa tomar medidas adequadas. O que não se mostra de difícil apuramento e muito menos impossível, até porque, as circunstâncias de uma violação irão ditar as condições exatas em que se pode considerar que um responsável pelo tratamento tem «conhecimento» dessa violação. Casos há em que é relativamente evidente desde o início se tal ocorreu. Todavia, a maior preocupação não deve ser centrada na prova de momento do «conhecimento» da violação de dados, mas sim na ação imediata para investigar o incidente, o que originou a falha ou violação, a fim de determinar se os dados pessoais foram de facto violados e tomar medidas de reparação e notificação.

[16] Anúncio n.º 136/2018 de 12 de julho.

tiverem sido previamente controlados por uma autoridade de controlo[17]. A AIPD será, essencialmente, uma ferramenta de reflexão.

4. Videovigilância – as finalidades previstas em Portugal

Em Portugal, o recurso à implementação de sistemas de videovigilância em locais públicos não existe só enquanto possibilidade, mas mesmo enquanto recurso obrigatório, particularmente no quadro da segurança privada.

Há casos em que, a lei estabelece a obrigatoriedade de implementação de sistema de videovigilância. Impõe a Lei 34/2013, de 16 de maio, que estão obrigados a adotar um sistema de segurança onde, entre outros meios, se inclui videovigilância, desde logo as próprias empresas titulares de alvará para prestação de serviços de segurança privada e as empresas detentoras de licença para serviços de autoproteção, sistemas, a utilizar nas suas próprias instalações operacionais, conforme previsto no art.º 7.º desta Lei e complementarmente na Portaria 273/2013 de 20 de agosto.

Além das empresas de segurança privada, estão, ainda, obrigados a deter sistema de videovigilância as seguintes entidades e estabelecimentos: (i) As instituições de crédito e as sociedades financeiras (alínea b), n.º 1, art.º 8.º da Lei 34/2013 de 16 de maio e art.º 90.º da portaria 273/2013 de 20 de agosto); (ii) Os conjuntos comerciais com área bruta locável igual ou superior a 20.000m2 e as superfícies comerciais com área de venda nacional acumulada de 30.000m2 (alínea b), n.º 2, art.º 8.º da Lei 34/2013 de 16 de maio); (iii) Os estabelecimentos de exibição, compra e venda de metais preciosos e obras de arte, quando o valor seguro for superior a €15.000 (alínea a), n.º 3, art.º 8.º da Lei 34/2013 de 16 de maio e art.º 97.º e 98.º da Portaria 273/2013 de 20 de agosto); (iv) As farmácias e postos de combustível (n.º 4, art.º 8.º da Lei 34/2013 de 16 de maio e art.º 100.º da Portaria 273/2013 de 20 de agosto); (v) Os *Automated Teller Machine* (art.º 10.º da Lei 34/2013 de 16 de maio e art.º 103.º da Portaria 273/2013 de 20

[17] *i.e.*, realizados com base em autorizações emitidas nos termos da Lei n.º 67/98, de 26 de outubro e em condições que não tenham sido alteradas, conforme orientação do GT29 (em conformidade com o art.º 29.º da Diretiva 95/46/CE de 24 de outubro), adotada em 04 de abril de 2017.

de agosto); (vi) Os estabelecimentos de restauração e bebidas com pista de dança e lotação igual ou superior a 100 lugares (art.º 9.º da Lei 34/2013 de 20 de agosto e alínea a), n.º 1, art.º 4.º do D.L. 135/2014 de 08 de setembro); (vii) Os recintos desportivos, onde se realizem espetáculos desportivos de natureza profissional ou não profissional considerados de risco elevado, sejam nacionais ou internacionais (art.º 18.º da Lei n.º 39/2009, de 30 de julho, alterada pela Lei 52/2013 de 25 de julho); (viii) Os operadores de resíduos em cujas instalações se procede ao armazenamento, tratamento ou valorização de metais não preciosos (art.º 2.º da Lei n.º 54/2012 de 06 de setembro).

Uma outra questão, não menos importante, é a videovigilância em táxis, ainda que a sua utilização não seja obrigatória, está legal e expressamente prevista a possibilidade de os táxis disporem de sistema de videovigilância no interior das viaturas e com transmissão das imagens para uma central de receção e arquivo de imagens, devendo esta central estar integrada no conceito de segurança privada; isto é, a sua exploração e gestão apenas pode ser exercida por quem seja detentor de alvará ou licença para a prática da atividade de segurança privada. A instalação e utilização dos sistemas de videovigilância em táxis estão previstas na Lei n.º 33/2007, de 13 de agosto, que, igualmente, impõe que as imagens apenas possam ser utilizadas para promoção da segurança dos motoristas dos táxis e dos utentes, apenas podendo ser mantidas gravadas por estas centrais as imagens que identifiquem situações de risco ou perigo potencial ou iminente e pelo período indispensável à sua comunicação às Forças de Segurança, que nunca pode exceder cinco dias.

Também está prevista a possibilidade de utilização de videovigilância para a deteção de incêndios florestais[18], a vigilância e deteção de incêndios pode ser assegurada, entre outros, "*por rede de videovigilância, que complementa e reforça em todo o território do continente, as funções de deteção fixa de ocorrências de incêndios*", salienta-se, ainda, que, a Rede Nacional de Postos de Vigia (para deteção de incêndios), constituída por postos de vigia públicos e privados e

[18] Encontra-se prevista em dois normativos legais – na Lei 1/2005 de 10 de janeiro, nos art.º 2.º e 15.º, para utilização pelas Forças e Serviços de Segurança; e no D.L. 124/2006 de 28 de junho, alterado pelo D.L. 15/2009, de 14 de janeiro, D.L. 17/2009 de 14 de janeiro, D.L. 114/2011 de 30 de novembro, D.L. 83/2014 de 23 de maio, Lei 76/2017 de 17 de agosto e D.L. 10/2018 de 14 de fevereiro.

"...pode ser complementada por sistema de videovigilância, meios de deteção móveis ou outros meios que venham a revelar –se tecnologicamente adequados..." (art.º 31.º e 32.º do Decreto-Lei n.º 10/2018, de 14 de fevereiro)[19].

A questão mais sensível e que pode comprometer a salvaguarda dos dados pessoais, é a da segurança de pessoas e bens e o seu enquadramento na segurança pública[20], porém encontram-se reguladas (n.º 1, do art.º 2.º da Lei 1/2005, de 10 de janeiro) a identificação e a limitação das finalidades deste tipo de videovigilância, como é o caso da: a) Proteção de edifícios e instalações públicas e respetivos acessos; b) Proteção de instalações com interesse para a defesa e a segurança; c) Proteção da segurança das pessoas e bens, públicos ou privados, e prevenção da prática de factos qualificados pela lei como crimes, em locais em que exista razoável risco da sua ocorrência; d) Prevenção e repressão de infrações estradais; e) Prevenção de atos terroristas; f) Proteção florestal e deteção de incêndios florestais.

Para além das finalidades elencadas, de forma muito sumária, importará reputar que: (i) O responsável pelo tratamento dos dados (imagens captadas), é indispensavelmente a força de segurança pública com jurisdição da área de captação ou o serviço de segurança requerente (n.º 2, art.º 2.º da Lei 1/2005, de 10 de janeiro); (ii) A instalação de câmaras fixas está sujeita a autorização do membro do Governo que tutela a força ou serviço de segurança requerente (n.º 1, art.º 3.º da Lei 1/2005, de 10 de janeiro); (iii) A decisão de autorização do Governo é precedida de parecer da CNPD (n.º 2, art.º 3.º da Lei 1/2005, de 10 de janeiro); (iv) Nos locais objeto de vigilância com recurso a câmaras fixas é obrigatória a afixação, bem visível, de informação sobre a existência e a localização das câmaras, a finalidade da

---

[19] Tecnologicamente, a utilização da videovigilância para deteção de incêndios florestais terá a sua génese em projeto desenvolvido pelo INOV, em meados da última década do século XX, com um projeto piloto para o parque nacional da Peneda Gerês. Dadas as dificuldades em vigiar áreas tão extensas, foi desenvolvido o sistema CICLOPE, que se baseia em imagens captadas, com infravermelhos para deteção noturna, integrando e articulando com outros dados recolhidos, nomeadamente dados meteorológicos e dados de qualidade do ar, permitindo uma deteção precoce e fiável de incêndios.

[20] Regulada pela Lei 1/2005, de 10 de janeiro, com as alterações introduzidas pelas Lei n.º 39-A/2005, de 29 de julho, Lei n.º 53-A/2006, de 29 de dezembro e Lei n.º 9/2012, de 23 de fevereiro, regula a utilização de câmaras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum.

captação de imagens e sons e a identificação do responsável pelo tratamento dos dados recolhidos, perante quem os direitos de acesso e retificação podem ser exercidos, utiliza-se, para o efeito, o modelo de dístico previsto na portaria 373/2012 de 16 de novembro.

A utilização do recurso de videovigilância para fins de segurança pública será, talvez, a finalidade que mais discussão e polémica tem gerado na sociedade portuguesa[21]. Vejamos a conclusão que chega Catarina Frois[22], que defende que os sistemas de videovigilância em locais públicos de utilização comum falharam redondamente na prevenção e dissuasão criminal, motivo pelo qual este é um tema particularmente sensível e objeto de necessária ponderação.

---

[21] Um dos locais mais conhecidos em Portugal na instalação de videovigilância para segurança pública foi o Bairro Alto, em Lisboa, em exploração desde maio de 2014. A requerimento do Diretor Nacional da Polícia de Segurança Pública, a CNPD deu parecer positivo à utilização deste recurso em determinados arruamentos públicos do Bairro Alto (Parecer n.º 68/2009 da CNPD). Neste parecer, fica bem patente a preocupação da CNPD na ponderação valores ou interesses – por um lado, o da segurança, por outro lado, o direito à imagem e à livre circulação – concluindo que, com a utilização da videovigilância, "*as pessoas não estão impossibilitadas de circular, porém, não o podem fazer de uma forma completamente livre, pois ficam registados todos os seus movimentos, designadamente com quem vão, como vão, entre outros aspetos da sua vida privada*." O parecer positivo da CNPD, ainda que parcial, impõe as seguintes limitações: 1. Período de funcionamento limitado ao período horário entre as 22H00 e as 07H00 (no requerimento, a PSP pretendia utilização permanente 24H/24H); 2. Proibição de recolha e gravação de som; 3. Apenas permite a utilização de câmaras fixas (no total de 27), não permitindo a utilização de câmaras ocultas; 4. Barramento automático de locais privados (portas, janelas, varandas, etc.), através de software denominada "máscara"); 5. Incapacidade técnica de busca inteligente para identificação de pessoas; 6. Colocação de sinalética de aviso da existência do sistema de videovigilância; 7. Obrigatoriedade de divulgação, através da comunicação social, da instalação do referido sistema; 8. Adoção de critérios de segurança lógica de acesso ao sistema; 9. Funcionamento durante um período máximo de 6 meses, prazo após o qual será efetuada reavaliação ao funcionamento do sistema. Mais de quatro anos depois deste parecer, após instalação, o sistema iniciou funcionamento em maio de 2014, mantendo-se em exploração após reavaliação dos fundamentos, particularmente pela CNPD. A entidade responsável pela exploração – Polícia de Segurança Pública – tem, igualmente, efetuado avaliações ao funcionamento e eficiência do sistema.

[22] Frois, Catarina. "Bases de dados pessoais e vigilância em Portugal: análise de um processo em transição", in *A sociedade vigilante: Ensaios sobre identificação, vigilância e privacidade*, Lisboa: ICS Imprensa de Ciências Sociais, 2008, p. 121 e ss.

No contexto da segurança rodoviária identificamos um duplo enquadramento para a utilização de videovigilância[23]. Conforme se perceberá, destacam-se duas principais finalidades e, por conseguinte, dois principais utilizadores da videovigilância: a finalidade de fiscalização, a desenvolver pelas Forças de Segurança; e a finalidade de gestão de tráfego e cobrança de taxas de portagens, a desenvolver pelo gestor da infraestrutura rodoviária nacional.

Na atividade de fiscalização rodoviária das Forças de Segurança (PSP e GNR) tem sido crescente o recurso à tecnologia, incluindo imagem, para deteção e prova de contraordenações, nomeadamente excesso de velocidade onde, à recolha da velocidade, associa-se a imagem da viatura em causa, de modo a fazer prova da viatura em infração. No apoio à atividade das Forças de Segurança, uma das mais recentes inovações é o "*Polícia automático*", que consiste na utilização de câmara de recolha de imagens que, direcionada à matrícula de viaturas e suportada em informação em memória, identifica matrículas de viaturas furtadas ou com outras situações legais pendentes (falta de seguro obrigatório, falta de inspeção periódica obrigatória, etc.).

Na atividade de gestão da infraestrutura rodoviária tem sido igualmente crescente o recurso a videovigilância. Em que poderemos distinguir duas subfinalidades: gestão de tráfego (incluindo ativação de recursos de apoio) e cobrança de portagens. Justifica-se esta distinção porque, em matéria de proteção de dados pessoais, fará toda a diferença.

Sendo que a videovigilância para a finalidade cobrança de portagens é imprescindível a captação de elementos identificativos da viatura (matrícula), pois, de outra forma e nas situações em que a viatura não é utilizadora de sistema de cobrança automática (via verde), seria impossível

---

[23] O previsto no artigo 13.º da Lei n.º 1/2005, de 10 de janeiro e regulamentado pelo Decreto-Lei n.º 207/2005, de 29 de Novembro, para utilização pelas Forças de Segurança, na sua atividade de deteção de infrações rodoviárias e a aplicação das correspondentes normas sancionatórias, bem como de ações de controlo de tráfego e ativação de mecanismo de prevenção e socorro e, ainda, de identificação de viaturas furtadas, com matrículas falsas ou outras situações legais pendentes (sistema polícia automático); e o previsto na Lei n.º 51/2006, de 29 de Agosto, para utilização pela empresa pública Infraestruturas de Portugal (sucedânea da Estradas de Portugal, de acordo com o D.L. 91/2015 de 29 de maio) e concessionários das Estradas, com a finalidade de monitorização do tráfego e consequente promoção de assistência rodoviária, bem como para apoio ao pagamento de taxas de portagens.

imputar o pagamento da portagem. Já para a gestão de tráfego, isto é, para percecionar se existem muitas ou poucas viaturas em circulação, se existe trânsito congestionado ou se existe alguma viatura parada ou mesmo a circular em contramão, não existe necessidade de recolha de elementos identificativos das viaturas. Nesta, como em qualquer outra circunstância, considerando o princípio da minimização dos dados, expresso no art.º 5.º do RGPD, estes deverão ser "*adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados*", motivo pelo qual, para esta finalidade, as imagens recolhidas não deverão permitir identificar pessoas nem dados de viaturas que possibilitem a posterior identificação do seu proprietário. Por conseguinte, e existindo interesse geral no acesso a estas imagens, para que qualquer cidadão possa perceber se determinado troço rodoviário está congestionado e melhor possa identificar o trajeto mais vantajoso, estas imagens poderão ser difundidas e cedidas a operadores de televisão e comunicações (n.º 3, art.º 16.º da Lei 51/2006 de 29 de Agosto).

Porém, a videovigilância, não estando sujeita a consentimento expresso das pessoas, cujos dados pessoais serão tratados, deve respeitar o direito de informação, isto é, em qualquer local onde seja utilizada, deverá ser exposta informação que, de forma clara e acessível, esclareça as pessoas acerca da sua existência, dos locais onde as câmaras estão e quem é o responsável pelo tratamento dos dados, respeitando modelo de sinal informativo.

A finalidade da utilização das imagens de videovigilância deve estar previamente definida, não podendo ser utilizada para além dessa limitação e, só podem ser gravadas por período limitado, normalmente 30 (trinta) dias. Só excecionalmente as imagens podem ser utilizadas para fins que não os processuais penais, isto é, em processos-crime, não podendo ser utilizadas para controlo da atividade laboral de trabalhadores, nestas circunstâncias as câmaras não poderão incidir sobre o interior de áreas reservadas aos trabalhadores ou a clientes e utentes, designadamente vestiários, instalações sanitárias, zonas de espera e provadores de vestuário, dirigidas a zonas de digitação de códigos de caixas multibanco ou terminais de pagamento *Automated Teller Machine*.

Conclusão

A videovigilância é, atualmente, uma tecnologia indispensável no apoio às mais diversas atividades, sendo a sua utilização não só uma possibilidade, mas também uma obrigatoriedade nalgumas circunstâncias (agências bancárias, centros comerciais, ourivesarias, farmácias, postos de combustível, discotecas, recintos desportivos e operadores de resíduos).

Tratando-se de obrigatoriedade ou não, estes sistemas têm, no entanto, de respeitar determinados requisitos, de modo a minimizar o mais possível o impacto da utilização deste recurso nos direitos, liberdades e garantias do cidadão.

O RGPD, aplicável em todos os Estados membros da União Europeia desde o dia 25 de maio de 2018, introduziu várias alterações no tratamento de dados pessoais, entre os quais a videovigilância que, por tratar imagens de pessoas, as mesmas, constituem dados pessoais.

Contudo, a ameaça terrorista após os atentados de 11 de setembro de 2001 nos EUA é mais uma razão para a recolha e troca de dados, desta vez justificadas como medidas de segurança e de prevenção. Porém, esta intrusão, quer das empresas quer das autoridades públicas, ameaça «*desmoronar*» uma das mais importantes conquistas civilizacionais.

Com efeito, o elevado número de recolha, tratamento e troca de dados pessoais que atualmente ocorre, advém da maior disponibilização de informações privadas, cedidas, voluntária ou involuntariamente, pelas próprias pessoas (pelos próprios titulares dos dados pessoais), nomeadamente nas redes sociais.

O avanço tecnológico permitiu também um mais rápido e eficaz desenvolvimento científico. No entanto, apesar destas vantagens, nem sempre a nova ordem digital é acompanhada de medidas protetoras adequadas no plano jurídico, que evitem ou não permitam a proliferação de violações e limitações de direitos, sobretudo de direitos fundamentais e direitos humanos.

Atualmente, em todo o mundo, sobretudo nos países desenvolvidos, os cidadãos não só são perseguidos continuamente no dia-a-dia, como consentem, de livre vontade, na divulgação dos seus próprios dados, com a vigilância e o «*voyeurismo*» da sociedade. Não restem dúvidas: nas últimas décadas assistimos a uma revolução digital que tornou a sociedade numa sociedade de informação.

A tutela da vida privada exige, hoje, mais transparência e controlo no concernente ao tratamento de dados por empresas e autoridades públicas. Ainda assim, teremos de levar em linha de conta os comportamentos das pessoas, que cada vez mais estão menos cientes do seu direito à privacidade, permitindo a divulgação, e divulgando elas mesmo, informações pessoais, sem consciência das reais implicações dos seus atos, em redes totalmente abertas como a internet, nas quais não há controlo nem fiscalização.

O direito à privacidade, como corolário de direitos fundamentais intrínsecos na consciência das sociedades modernas, nem sempre está protegido: os meios tecnológicos disponíveis nos dias de hoje surgiram a uma velocidade que o direito não acompanhou. Assim, e centrando a atenção na União Europeia, tornou-se evidente a necessidade de proceder a uma profunda reforma do direito à proteção de dados pessoais.

Todavia, e um pouco contra a corrente, refira-se que uma hipotética uniformização de direitos fundamentais não deixa de ser preocupante, na medida em que a globalização impõe uma determinada visão do mundo e da vida, sem que os direitos fundamentais possam refletir as autonomias e peculiaridades dos povos, acabando por enfraquecer a diversidade cultural.

Consideramos que é imprescindível sensibilizar os indivíduos para a autoproteção da sua privacidade, os utilizadores das novas tecnologias devem estar cientes dos perigos que estas comportam e, nomeadamente, devem ter consciência de que a divulgação de informações em redes abertas como a *internet* escapa ao seu controlo. Dados uma vez disponibilizados estão para sempre disponíveis. Por isso mesmo, a privacidade, uma vez imiscuída, está imiscuída para sempre. Por tal, as novas tecnologias de informação impõem que o direito à privacidade seja repensado e reconfigurado como um direito ao anonimato.

Ao longo da elaboração deste texto, surge a convicção de que a compressão da privacidade não se verifica somente perante a hegemonia do interesse público (sobretudo por razões de segurança). Nos dias de hoje, tal compressão verifica-se, desde logo, pelos hábitos observados nos últimos anos de milhões de pessoas de partilhar detalhes e acontecimentos (por vezes íntimos) das próprias vidas, criando uma versão pública, *online,* da vida privada – *i.e.*, autocompressão da privacidade individual. A questão que se impõe formular é de saber se perante a revolução digital a que assistimos, será a privacidade (tal como a conhecemos) um conceito em vias de extinção ou ainda tem cabimento nesta sociedade cada vez mais pátula?.

De facto, nesta sociedade cada vez mais aberta, e adepta da era digital, onde se expõe com toda a abertura e transparência a vida privada, e até, a vida familiar, deixou de fazer sentido a privacidade, tal como a conhecemos. Na verdade, assistimos a mudanças de mentalidade e de comportamento social em que o valor da proteção da privacidade deixou de ser um «*bem supremo*», deixando até desvanecer a noção e o valor de que a privacidade é um direito inerentemente humano e um pré-requisito para a manutenção da condição humana com dignidade e respeito.