TRATAMENTO DE DADOS PESSOAIS NO ÂMBITO DA VIDEOVIGILÂNCIA FACE AO NOVO REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS (RGPD)

Jorge Miguel do Vale Martinez Batalha

Dissertação para obtenção do Grau de Mestre em

Segurança de Informação e Direito no Ciberespaço

Orientadores:

Prof. Doutor Carlos Manuel Costa Lourenço Caleiro

Prof. Doutor José Alexandre Guimarães Sousa Pinheiro

Júri:

Presidente: Prof. Doutor Paulo Alexandre Carreira Mateus

Vogal: Prof. Doutor Rui Guerra da Fonseca

Vogal: Prof. Doutor José Alexandre Guimarães Sousa Pinheiro

Lisboa, 2017

RESUMO

O presente texto é fruto de investigação desenvolvida no campo dos direitos fundamentais dos cidadãos, em particular, no que concerne à proteção de dados pessoais.

Hodiernamente, apesar da legislação nacional portuguesa acautelar cuidados especiais em matéria de proteção de dados pessoais, constata-se que, face à recente aprovação, pela União Europeia, do «Regulamento Geral sobre a Proteção de Dados», todos os Estados-Membros terão de cumprir regras mais apertadas. De tal forma que, em caso de incumprimento, as entidades públicas e privadas estarão sujeitas a sanções substancialmente mais pesadas do que as atualmente previstas, para além dos inerentes danos reputacionais.

Neste contexto, pretende-se dar resposta à seguinte pergunta: à luz do «Regulamento Geral sobre a Proteção de Dados» e no âmbito do tratamento de dados pessoais obtidos com recurso a sistemas de videovigilância, em espaços privados, quais as principais alterações aplicadas aos titulares dos dados, em particular no contexto laboral, que medidas devem os responsáveis destes tratamentos adotar e quais as necessidades de legislação complementar a que o Estado Português deve responder?

No final, com o foco principal na proteção de dados pessoais no contexto laboral e face à constatação depreendida pela investigação realizada, são apresentadas duas propostas que visam contribuir para colmatar as lacunas existentes quanto à regulação do tratamento de dados pessoais obtidos com recurso a sistemas de videovigilância em espaços privados.

PALAVRAS-CHAVE: RGPD, GDPR, Tratamento de dados, Videovigilância, CCTV, Proteção de dados pessoais.

ABSTRACT

The current text is the result of a research carried out in the field of citizens' fundamental rights, particularly, with respect to Personal Data Protection.

Nowadays, despite Portugal's national legislation ensuring special care in relation to Personal Data Protection, one notes that, the recent approval by the European Union, of the «General Data Protection Regulation», all Member States will have to comply with tighter rules. Thus, in the event of non-compliance, public and private entities will be subject to substantially heavier sanctions than currently envisaged, in addition to the inherent reputational damages.

In this context, the intention is to answer the following question: in the light of the «General Data Protection Regulation» when handling personal data obtained using video surveillance systems, in private spaces, what are the main changes imposed on data subjects, especially in the work context, what measures should those in charge of these processing take and what type of additional legislation requirements should the Portuguese State respond to?

At the end, with a special focus on the personal data protection in the work context, and considering the finding derived from the research work carried out, two proposals are suggested aimed at addressing the existing gaps in the regulation of the processing of personal data obtained using video surveillance systems in private spaces.

KEYWORDS: RGPD, GDPR, Data processing, Video surveillance, CCTV, Personal data protection.

ÍNDICE GERAL

ÍNDICE DE FIGURAS

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

ANPC – Autoridade Nacional de Proteção Civil

CNPD – Comissão Nacional de Proteção de Dados

CRP – Constituição da República Portuguesa

CT – Código do Trabalho

GDPR – *General Data Protection Regulation*

GNR – Guarda Nacional Republicana

LPDP – Lei de Proteção de Dados Pessoais

PSP – Polícia de Segurança Pública

RASP – Relatório Anual de Segurança Privada

RGPD – Regulamento Geral sobre a Proteção de Dados

TFUE – Tratado sobre o Funcionamento da União Europeia

UE – União Europeia

INTRODUÇÃO

O *Jornal Oficial da União Europeia* publicou em 2016 o novo *Regulamento Geral sobre a Proteção de Dados* (RGPD)[1], também conhecido internacionalmente como *General Data Protection Regulation* (GDPR). Trata-se de um documento vinculativo para todos os Estados-Membros, tendo como objetivo principal assegurar um nível equivalente de proteção das pessoas singulares e permitir a livre circulação de dados pessoais na União.

O designado *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, vigora desde 25 de maio de 2016 e é aplicável a partir de 25 de maio de 2018.

Na verdade, o Regulamento faz revogar a Diretiva 95/46/CE, com efeitos a partir de 25 de maio de 2018. Contudo, cabe aqui destacar o facto da referida Diretiva ser a base das diversas leis de proteção de dados dos Estados-Membros. Nestes, inclui-se naturalmente o Estado Português, o qual transpôs a Directiva para o regime jurídico nacional há cerca de dezanove anos, através da publicação da Lei 67/98, de 26 de Outubro, Esta é vulgarmente referida como *Lei da Proteção de Dados Pessoais* e atualmente regula, de forma geral, o tratamento de dados pessoais no ordenamento jurídico português.

É essencial entender que "*o tratamento dos dados pessoais deverá ser concebido para servir as pessoas*"[2]. Falamos de pessoas singulares que, na sua grande maioria, não se apercebeu da velocidade com que se tornou vulnerável em diversos aspetos. Um destes refere-se, sem dúvida, à proteção de dados pessoais.

Na parte inicial do texto do novo *Regulamento*, reconhece-se que "*a rápida evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados pessoais. A recolha e a partilha de dados pessoais registaram um aumento significativo. As novas tecnologias permitem às empresas privadas e às entidades públicas a utilização de dados pessoais numa escala sem precedentes no exercício das suas atividades. As pessoas singulares disponibilizam cada vez mais as suas informações pessoais de uma forma pública e global. As novas tecnologias transformaram a economia e a vida social e deverão contribuir para facilitar a livre circulação de dados pessoais na União e a sua transferência para países terceiros e organizações internacionais, assegurando simultaneamente um elevado nível de proteção dos dados pessoais*"[3].

---

[1] UNIÃO EUROPEIA, 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 (Regulamento Geral sobre a Proteção de Dados), in: http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX%3A32016R0679&from=EN, consultado em maio 2016, doravante referido como RGPD.

[2] RGPD, Considerando nº 4.

[3] RGPD, Considerando nº 6.

Neste contexto, o presente trabalho é focado na obtenção de resposta à seguinte pergunta: à luz do RGPD e no âmbito do tratamento de dados pessoais obtidos com recurso a sistemas de videovigilância, em espaços privados, quais as principais alterações aplicadas aos titulares dos dados, em particular no contexto laboral, que medidas devem os responsáveis destes tratamentos adotar e quais as necessidades de legislação complementar a que o Estado Português deve responder?

Face ao exposto, foi feita a revisão bibliográfica que se entendeu mais adequada. No âmbito nacional, deu-se relevância à Constituição da República Portuguesa, à Lei de Proteção de Dados Pessoais (Lei 67/98), ao Código do Trabalho, às Deliberações, Pareceres e Autorizações da Comissão Nacional de Proteção de Dados Pessoais e à legislação que regula a atividade de segurança privada. No contexto internacional, foi dado relevo à Diretiva 95/46/CE, à Carta dos Direitos Fundamentais da União Europeia, à Declaração Universal dos Direitos do Homem e ao Regulamento Geral sobre a Proteção de Dados.

O presente texto é composto por 12 capítulos que terminam, em jeito de conclusão face à investigação realizada, com a apresentação de dois contributos aplicáveis no contexto nacional português.

O primeiro destes corresponde a um projeto de código de conduta aplicável aos tratamentos de dados obtidos no âmbito da utilização de sistemas de videovigilância em contexto laboral. Por fim, é apresentado um conjunto de aspetos considerados relevantes, no âmbito da videovigilância, que se entendem ser solucionados através da produção de legislação nacional, face à inexistência de uma lei geral sobre a utilização de sistemas de videovigilância em Portugal.

1. DIREITO CONSTITUCIONAL

1.1. ENQUADRAMENTO

O Direito tem um papel fundamental no garante da justiça, segurança e liberdade. Paulo Otero entende estas três componentes como valores indispensáveis numa qualquer sociedade onde as pessoas sejam a base, o critério e o limite das instituições políticas em que estes seres vivos se inserem. Frisa ainda o autor que, "*se a Constituição escrita contrariar a justiça, não garantir a segurança ou negar a liberdade, suscita-se o problema da (in) validade das respectivas normas «constitucionais»*"[4].

Sendo o presente documento elaborado no âmbito do ensino superior, vale a pena aqui referir outras considerações de Paulo Otero. Ao abordar a temática do Direito Constitucional e ao definir a essência do ensino universitário, naturalmente associado à liberdade, escreve Otero: "(...) *assume-se, porém, que a liberdade de divergir de quem aprende nunca pode tolher a liberdade de quem ensina, tal como a liberdade de ensinar nunca pode deixar de respeitar a liberdade de aprender*"[5].

Com efeito, as normas constitucionais correspondem ao tronco de todos os diversos ramos do direito. Sem esquecer o facto de ter sido o caso português o pioneiro na "*constitucionalização expressa da relação informática/direitos fundamentais*"[6], propõe-se neste trabalho a reflexão sobre algumas das inúmeras questões de índole constitucional que a utilização de sistemas de videovigilância, em particular no contexto laboral, pode suscitar.

1.2. CONSTITUIÇÃO DA REPÚBLICA PORTUGUESA

Em 1976, a Assembleia Constituinte reuniu, aprovou e decretou a atual Constituição da República Portuguesa, doravante designada por CRP, em vigor desde Abril, desse ano, ou seja, dois anos após a revolução de 25 de abril de 1974.

Este documento a que o Estado português se encontra subordinado, mantêm-se em vigor apesar das sucessivas revisões, cuja sétima e última destas data de 12 de Agosto de 2005.

1.3. DIREITOS LIBERDADES E GARANTIAS

De acordo com Jorge Miranda, a Constituição de 1976 tem características especiais, atendendo ao passado recente de ditadura[7]. Este mesmo autor afirma ainda que, tendo em conta o regime autoritário

[4] Cf. OTERO, Paulo, *Instituições Políticas e Constitucionais – Volume I*, Coimbra: Livraria Almedina, 2009, p. 604.

[5] Cf. OTERO, Paulo, *Instituições Políticas e Constitucionais – Volume I*, Coimbra: Livraria Almedina, 2009, p. 16.

[6] Cf. PINHEIRO, Alexandre Sousa, *"Privacy" e Protecção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional*, Lisboa: AAFDL, 2015, p. 666.

[7] Cf. MIRANDA, Jorge, *Teoria do Estado e da Constituição*, Coimbra: Coimbra Editora, 2002, p. 210.

derrubado em 1974 e os riscos de implantação de nova ditadura em 1975, é uma Constituição muito preocupada com os direitos fundamentais dos cidadãos.

Efetivamente, o espaço reservado aos Direitos, Liberdades e Garantias, constam do Título II da Parte I da CRP, desde o art.º 24º ao art.º 57º.

1.4. UTILIZAÇÃO DA INFORMÁTICA

A «Comissão Nacional de Proteção de Dados», entidade administrativa independente, a qual irá ser sujeita a maior pormenor ao longo do presente trabalho, indica na sua página da internet o seguinte: "*desde 1976 que a Constituição da República Portuguesa consagrou, como direito fundamental, no seu artigo 35º, a proteção dos dados pessoais face à utilização da informática*"[8].

Efetivamente, conforme o n.º 1 do artigo 35º da CRP, "*todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei*"[9].

1.5. OUTROS DIREITOS PREVISTOS NA CRP

Naturalmente, na CRP estão ainda consagrados outros direitos pessoais. Entre estes, conforme o n.º 1 do artigo 26º, a "*todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação*"[10]. Mais à frente, caberá aqui ser dada particular atenção, entre outros aspetos, à questão da reserva da intimidade da vida privada.

[8] Cf. CNPD, *História da CNPD*, in: https://www.cnpd.pt/bin/cnpd/historia.htm, consultado em janeiro de 2016.

[9] Cf. PORTUGAL, *Constituição da República Portuguesa*, Coimbra: Livraria Almedina, 2011, p. 23.

[10] Cf. PORTUGAL, *Constituição da República Portuguesa*, Coimbra: Livraria Almedina, 2011, p. 18.

2. O OLHO TECNOLÓGICO

2.1. PANÓPTICO

O panóptico foi apresentado como um modelo arquitetónico, criado em 1785 por Jeremy Bentham. Consistia numa edificação circular, onde alguém vigia sem ser visto e destinava-se à vigilância penitenciária mas podia ser aplicado em escolas, hospitais, fábricas, ou até mesmo em bibliotecas. Este modelo é entendido pelos vários autores como inspirador das atuais câmaras de videovigilância[11].

Resumidamente, neste modelo aplicado a uma penitenciária, os prisioneiros sabiam que estavam a ser vistos. Mas pelo facto de não verem quem os controlava e apesar de estarem conscientes de alguma desatenção momentânea da pessoa com funções de controlo, como nunca saberiam se essa eventual desatenção ocorreria ou qual o momento em que ocorreria, desenvolviam um temor sobre esse elemento controlador e «omnipresente»[12].

Curiosamente, em Portugal ainda existe uma edificação inspirada neste modelo, localizada no Hospital Miguel Bombarda, em Lisboa. Na altura da sua construção, "*o pavilhão de alta segurança (1892-1896), conhecido por Panóptico, foi concebido para enfermaria-prisão destinada a doentes perigosos ou provenientes da penitenciária*"[13].

2.2. REALIDADE NACIONAL

Conforme indica Catarina Sarmento e Castro, "*existirá um tratamento de videovigilância, nomeadamente, nos casos em que a recolha de imagens se realize através de câmaras* Web*, ou quando se proceda à sua difusão com recurso à Internet, mas também quando esta recolha se realize em circuito fechado de vídeo (CCTV ou* Closed-Circuit Television)"[14]. Mais à frente iremos aprofundar a definição de «tratamento de dados» plasmada na legislação em vigor. Mas, de forma sucinta, poderá por agora ser entendido como qualquer operação ou conjunto de operações sobre dados pessoais.

Admitindo a hipótese de quanto maior for o número de câmaras menos ilícitos ocorrerão, regista-se de forma geral e em todo o país um crescente recurso a dispositivos de videovigilância, tanto ao nível público como privado. Como ensina Alexandre Sousa Pinheiro, "*o domínio total do espaço por câmaras*

---

[11] Cf. PINHEIRO, Alexandre Sousa, *"Privacy" e Protecção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional*, Lisboa: AAFDL, 2015, p. 185.

[12] Cf. PINHEIRO, Alexandre Sousa, *"Privacy" e Protecção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional*, Lisboa: AAFDL, 2015, p. 187.

[13] Cf. OPEN HOUSE LISBOA, *Panóptico do Hospital Miguel Bombarda*, in: http://2015.openhouselisboa.com/places/panoptico-do-hospital-miguel-bombarda-3/, consultado em dezembro 2015.

[14] Cf. CASTRO, Catarina Sarmento e, *Direito da Informática, Privacidade e Dados Pessoais*, Coimbra: Livraria Almedina, 2005, p. 125.

conduziria a um Éden de segurança"[15]. No entanto, apesar de o ser humano ser imperfeito por natureza e, consequentemente, gerador de crimes, não se poderá chegar ao exagero de julgar todos os cidadãos como suspeitos de serem suspeitos. Apesar disso, a sociedade portuguesa mantém-se silente em relação a esta matéria.

Parece, contudo, clara a posição da Comissão Nacional de Proteção de Dados quanto a esta matéria, ao referir que "*não será legítimo defender que todas as pessoas que frequentam os locais públicos sujeitos a videovigilância se apresentam como «potenciais suspeitos»*"[16].

Neste contexto, refere Pedro Moura Ferreira que, "*face à pressão dos cidadãos, pouco importa que a segurança proporcionada pela videovigilância seja largamente ilusória, desde que diminua o sentimento de insegurança e reforce a convicção da capacidade de intervenção do Estado*"[17]. Apesar dessa ilusória segurança, a videovigilância não opera, na realidade, como elemento dissuasor da prática de delitos. Quando muito, representa, na sua essência, um elemento de prova da realização dos mesmos[18].

O presente trabalho centra-se no âmbito privado, ou seja, videovigilância operada em espaços privados, sejam estes de acesso público ou não. Até porque é notório que "*não há em Portugal, até ao momento, uma discussão aprofundada sobre o aumento de dispositivos tecnológicos de vigilância*"[19]. Naturalmente, serão as imagens captadas para além da esfera das autoridades nacionais, ou seja, forças e serviços de segurança do Estado, aquelas que maior discussão aprofundada poderão suscitar. Basta pensar em quem opera, ou seja, quem vê as imagens em tempo real, seleciona alvos (pessoas ou objetos) e comanda o *zoom*[20] das câmaras de videovigilância. Por um lado, parte delas, as que registam imagens da via pública, serão operadas por elementos das forças e serviços de segurança pública do Estado, estando estes sujeitos a valores éticos e morais necessariamente elevados, para além da sua condição de funcionário público, com uma responsabilidade naturalmente acrescida, onde a sua missão não tem como objetivo principal o retorno financeiro inerente a uma atividade empresarial. Por outro lado, temos funcionários de empresas de segurança privada, com formação prevista em legislação aplicável, mas sujeitos a entidades patronais privadas, as quais tem como principal objetivo o retorno financeiro.

Cabe aqui salientar os sistemas de videovigilância que, não sendo operados por forças e serviços de segurança, nem por vigilantes de empresas de segurança privada (ou no regime de autoproteção), são

---

[15] Cf. PINHEIRO, Alexandre Sousa, *"Privacy" e Protecção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional*, Lisboa: AAFDL, 2015, p. 185.

[16] Cf. CNPD, *Deliberação nº 61/2004 - Princípios Sobre o Tratamento de Dados por Videovigilância*, in: https://www.cnpd.pt/bin/orientacoes/DEL61-2004-VIDEOVIGILANCIA.pdf, consultado em janeiro de 2016.

[17] Cf. FRÓIS, Catarina, *Vigilância e Poder*, Lisboa: Mundos Sociais, 2011, p. xv.

[18] Cf. CNPD, *Deliberação nº 61/2004 - Princípios Sobre o Tratamento de Dados por Videovigilância*, in: https://www.cnpd.pt/bin/orientacoes/DEL61-2004-VIDEOVIGILANCIA.pdf, consultado em janeiro de 2016.

[19] Cf. FRÓIS, Catarina, *Vigilância e Poder*, Lisboa: Mundos Sociais, 2011, p. 3.

[20] Efeito de afastamento ou aproximação que se obtém por meio da variação da distância focal da câmara.

operados, em contexto laboral, por entidades patronais ou trabalhadores dependentes destes. Efetivamente recai sobre o contexto laboral o particular destaque dado ao longo deste trabalho.

Com efeito, a segurança privada, sujeita a legislação específica, recorre a diversas medidas de segurança, entre as quais a videovigilância, visando atingir os fins legalmente estabelecidos, ou seja, proteção de pessoas e bens e prevenção da prática de crimes.

Na verdade, as regras estão plasmadas na Lei nº 34/2013 de 16 de maio, documento que estabelece o regime do exercício da atividade de segurança privada e procede à primeira alteração à Lei nº 49/2008, de 27 de agosto (Lei de Organização da Investigação Criminal). No entanto, parecem existir dúvidas quanto aos limites da instalação de sistemas de videovigilância, recolha de imagens e som, fins a que se destinam esses dados, para além de outros aspetos que eventualmente colidam com o estabelecido na Constituição da República Portuguesa. Admitindo previamente a hipótese da necessidade de correções, o legislador previu à data da publicação da lei, em 2013, a reavaliação, por parte do Governo, do regime jurídico que regula o exercício da atividade de segurança privada três anos após a sua entrada em vigor, conforme referido no artigo 66º da lei em apreço, ou seja, mais precisamente, no mês de junho de 2016[21]. Como até à presente data não se verificou nenhuma alteração, quiçá o presente trabalho possa contribuir para essa reflexão.

[21] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 34/2013 de 16 de maio*, 1ª série - nº 94, 16 de maio de 2013, p. 2940.

3. DADOS PESSOAIS

3.1. O QUE SÃO DADOS PESSOAIS

No âmbito da Lei de Proteção de Dados Pessoais e de acordo com a alínea a) do seu artigo 3º, entende-se por «dados pessoais» "*qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável a pessoa que possa ser identificada directa ou indirectamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social*"[22].

Desta definição, cabe aqui esclarecer o entendimento dado à palavra «identificável». Como refere Catarina Sarmento e Castro, "*o caso da recolha de imagens pelos sistemas vídeo (mas também fotografias) de controlo da passagem de veículos nas portagens ou do acesso de veículos a zonas de circulação condicionada, ou de controlo de velocidade, através dos quais se regista o número de matrícula de um veículo, permitindo, através desta, identificar o seu proprietário, ou o titular do contrato de via verde. Nestes casos, não se procede ao registo da imagem da pessoa em si, que não é identificada na imagem, mas torna-se possível a identificação de uma determinada pessoa, sendo, por conseguinte, identificável a pessoa em causa, ainda que com recurso a outras informações*"[23].

3.2. TRATAMENTO DE DADOS PESSOAIS

No âmbito da Lei de Proteção de Dados Pessoais e de acordo com a alínea b) do seu artigo 3º, o tratamento de dados pessoais é definido como "*qualquer operação ou conjunto de operações sobre dados pessoais, efectuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição*"[24].

De salientar que de acordo com o n.º 1 do artigo 27º da Lei de Proteção de Dados Pessoais, "*o responsável pelo tratamento ou, se for caso disso, o seu representante deve notificar a CNPD antes da realização de um tratamento ou conjunto de tratamentos, total ou parcialmente autorizados, destinados à prossecução de uma ou mais finalidades interligadas*"[25]. Como iremos ver mais à frente, têm sido estas notificações e consequentes decisões, em particular quanto ao tratamento de dados no âmbito

[22] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 67/98 de 26 de Outubro*, 1ª série - A, nº 247, 26 de outubro de 1998, p. 5536.

[23] Cf. CASTRO, Catarina Sarmento e, *Direito da Informática, Privacidade e Dados Pessoais*, Coimbra: Livraria Almedina, 2005 p. 124.

[24] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 67/98 de 26 de Outubro*, 1ª série - A, nº 247, 26 de outubro de 1998, p. 5536.

[25] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 67/98 de 26 de Outubro*, 1ª série - A, nº 247, 26 de outubro de 1998, p. 5543.

da videovigilância, as responsáveis por grande parte do trabalho da Comissão Nacional de Proteção de Dados.

3.3. DADOS SENSÍVEIS

3.3.1. O que são dados sensíveis

No âmbito da Lei de Proteção de Dados Pessoais e de acordo com o n.º 1 do seu artigo 7º entende-se serem dados sensíveis os "*dados pessoais referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica, bem como o tratamento de dados relativos à saúde e à vida sexual, incluindo os dados genéticos*"[26]. De salientar uma vez mais a questão da vida privada e, neste caso, a consideração deste aspeto como inserido no campo dos dados sensíveis.

3.3.2. Limitações ao tratamento de dados sensíveis

O mesmo artigo 7.º estabelece a proibição de tratamento de dados sensíveis. As exceções à proibição estão previstas nesse mesmo artigo, sendo, no entanto, dado destaque a eventual disposição legal, autorização da CNPD, ou quando exista consentimento expresso pelo titular dos dados, garantindo sempre a não discriminação e, uma vez mais, o respeito pelos direitos, liberdades e garantias do titular dos dados. Veja-se que, de modo geral, estão previstas medidas especiais de segurança a serem cumpridas pelos responsáveis pelo tratamento de dados, conforme referido no artigo 15º da Lei de Proteção de Dados Pessoais[27].

[26] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 67/98 de 26 de Outubro*, 1ª série - A, nº 247, 26 de outubro de 1998, p. 5537.

[27] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 67/98 de 26 de Outubro*, 1ª série - A, nº 247, 26 de outubro de 1998, p. 5540.

4. PROTEÇÃO DE DADOS PESSOAIS

4.1. LEGISLAÇÃO BASE

Desde o final do século passado, vigora em Portugal a Lei n.º 67/98, de 26 de outubro de 1998. Mais conhecida como a «Lei de Proteção de Dados Pessoais» (LPDP), este relevante documento legislativo foi produzido na sequência de orientações das instâncias europeias, visto que, conforme refere o seu artigo 1º, "*transpõe para a ordem jurídica interna a Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*"[28].

De salientar que a Comissão Nacional de Proteção de Dados refere que desde janeiro de 1994 foi criada, pelo Estado Português, uma entidade denominada «Comissão Nacional de Proteção de Dados Pessoais Informatizados» (CNPDPI), embora só em 1998 a lei "*vem alargar substancialmente o leque de atribuições e competências da Comissão, que passa desde então a designar-se CNPD – Comissão Nacional de Proteção de Dados*"[29].

Na realidade, a Comissão Nacional de Proteção de Dados, doravante designada CNPD, é uma autoridade nacional. Para além dessa condição, o n.º 1 do artigo 22º da Lei n.º 67/98, de 26 de outubro de 1998, doravante designada por Lei de Proteção de Dados Pessoais (LPDP), estabelece que a CNPD "*tem como atribuição controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de protecção de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei*"[30].

No entanto, em Portugal, torna-se evidente o desconhecimento generalizado do conteúdo da LPDP, em particular quando esta é analisada no âmbito do contexto laboral. Tal como refere Amadeu Guerra, a LPDP "*não está suficientemente divulgada e a generalidade das entidades empregadoras desconhece, por isso, as regras que devem observar quando processam, automaticamente, dados pessoais dos seus empregados*"[31]. Se esta era a situação em 2004, data da publicação da obra citada, não é menos verdade que, presentemente, mais de uma década depois, as regras continuam a não ser cumpridas e, como adiante iremos demonstrar, é crescente o número de processos de contraordenação abertos, neste contexto, pela CNPD.

[28] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 67/98 de 26 de Outubro*, 1ª série - A, nº 247, 26 de outubro de 1998, p. 5536.

[29] Cf. CNPD, *História da CNPD*, in: https://www.cnpd.pt/bin/cnpd/historia.htm, consultado em janeiro de 2016.

[30] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 67/98 de 26 de Outubro*, 1ª série - A, nº 247, 26 de outubro de 1998, p. 5541.

[31] Cf. GUERRA, Amadeu, *A Privacidade no Local de Trabalho*, Coimbra: Livraria Almedina, 2004, p. 17.

4.2. GENERALIDADES

O artigo 2º da Lei de Proteção de Dados Pessoais define, como princípio geral, que "*o tratamento de dados pessoais deve processar-se de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias fundamentais*"[32]. De salientar que, tal como estabelece a CRP, a reserva da vida privada deve ser respeitada.

Desde logo, nesta lei, transposição para o ordenamento jurídico português da Diretiva n.º 95/46/CE[33], do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, pode inferir-se uma preocupação em cumprir a Constituição da República Portuguesa.

Para além disso, num parecer acerca da alteração do regime jurídico do exercício da atividade de segurança privada, a própria CNPD demonstra especial cuidado em chamar a atenção para às eventuais restrições a direitos fundamentais[34], recorrendo ao plasmado no n.º 2 do artigo 18º da CRP. Refere a Comissão, nesse documento, que a lei só pode restringir direitos, liberdades e garantias nos casos previstos na CRP, devendo, em caso de necessidade de restrição, limitar-se ao necessário para salvaguardar outros direitos ou interesses previstos na Constituição.

4.3. ÂMBITO DE APLICAÇÃO

Conforme refere o n.º 2 do artigo 4º da Lei de Proteção de Dados Pessoais, as pessoas singulares que efetuem tratamento de dados pessoais no exercício de atividades exclusivamente pessoais ou domésticas não estão sujeitas a esta legislação. No entanto, atendendo ao facto desta lei ser aplicada à videovigilância, para além de outros tipos de tratamento de dados pessoais, há que ter em especial atenção quanto à instalação de câmaras de videovigilância que, para além do espaço privado, captem imagens da via pública, mesmo que «apenas» parcialmente. De salientar que o tratamento de dados pessoais no exercício de atividades exclusivamente pessoais ou domésticas nunca poderá ser utilizado para vigiar funcionários, como, por exemplo, prestadores de serviços domésticos.

Apesar disso, num condomínio residencial, onde o recurso a dispositivos de videovigilância seja aprovado pelos condóminos, estará esta instalação necessariamente sujeita às regras impostas pela Lei de Proteção de Dados Pessoais. Ou seja, apenas o caso de uma pessoa singular, no exercício de atividades domésticas e exclusivamente do foro pessoal ou doméstico, não se encontra sujeita a esta legislação de proteção de dados pessoais. Por outras palavras, o âmbito da referida lei corresponde a

[32] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 67/98 de 26 de Outubro*, 1ª série - A, nº 247, 26 de outubro de 1998, p. 5536.

[33] Cf. UNIÃO EUROPEIA, *Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*, in: http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT, consultado em abril 2016.

[34] Cf. CNPD, *Parecer n.º 22/2003*, in: https://www.cnpd.pt/bin/decisoes/Par/40_22_2003.pdf, consultado em janeiro de 2016.

todos os outros casos em que exista recurso a dispositivos de videovigilância, para além de outros meios previstos no artigo 4º da Lei de Proteção de Dados Pessoais[35].

No presente trabalho, dá-se particular destaque ao recurso a sistemas de videovigilância no âmbito do regime jurídico do exercício da atividade de segurança privada. Note-se que, face à atual legislação, são diversas as empresas e entidades sujeitas à obrigatoriedade de adoção de medidas de segurança, com a finalidade de prevenir a prática de crimes[36]. Entre estas medidas incluem-se sistemas de videovigilância, supondo que em observância da Lei de Proteção de Dados Pessoais. Quer isto dizer que poderá ocorrer um conflito de intenções entre videovigilância e proteção de dados pessoais. Curiosamente, ambas as intenções visam a segurança, embora em perspetivas diferentes.

4.4. CONCEITO DE «EXERCÍCIO DE ATIVIDADES EXCLUSIVAMENTE PESSOAIS OU DOMÉSTICAS»

Face à hodierna diversidade de oferta tecnológica, residentes e/ou proprietários de moradias, ou de outras tipologias de propriedades privadas utilizadas como habitação, recorrem frequentemente a dispositivos de videovigilância com o intuito de proteger os seus familiares para além dos seus bens.

Persistem, todavia, dúvidas quanto aos limites dessa proteção. A este propósito, um recente acórdão do Tribunal de Justiça, em dezembro de 2014, refere que "*o artigo 3°, n.° 2, segundo travessão, da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, deve ser interpretado no sentido de que a exploração de um sistema de câmara que dá lugar a uma gravação vídeo de pessoas, guardada num dispositivo de gravação contínua, como um disco rígido, sistema esse instalado por uma pessoa singular na sua casa de família, para proteger os bens, a saúde e a vida dos proprietários dessa casa, e que vigia igualmente o espaço público, não constitui um tratamento de dados efetuado no exercício de atividades exclusivamente pessoais ou domésticas, na aceção desta disposição*"[37]. Fica clara a jurisprudência emanada por este órgão europeu. Ou seja, sempre que uma pessoa singular tenha uma ou mais câmaras de videovigilância na sua propriedade habitacional mas que, através dessas, vigie e/ou grave imagens igualmente do espaço público, esse sistema, por essa razão, não se enquadra no exercício de atividades exclusivamente pessoais ou domésticas.

A este propósito, vale a pena citar o exemplo referido por Catarina Sarmento e Castro, quando afirma, sobre o visionamento do espaço público onde se possa incluir a entrada da porta de um vizinho: "*basta*

[35] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 67/98 de 26 de Outubro*, 1ª série - A, nº 247, 26 de outubro de 1998, pp. 5536-5537.

[36] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 34/2013 de 16 de maio*, 1ª série - nº 94, 16 de maio de 2013, pp. 2923-2924.

[37] Cf. UNIÃO EUROPEIA, *Acórdão do Tribunal de Justiça (Quarta Secção) - 11 de dezembro de 2014*, in: http://curia.europa.eu/juris/document/document.jsf?text=&docid=160561&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=29158#Footnote*, consultado em dezembro 2015.

que se imagine que se trata de um espaço onde funcione um médico ou um advogado, para que se possa aferir da especial sensibilidade dessas imagens"[38]. Para além disso, frisa a mesma autora, "*para que os tratamentos de imagens fiquem sujeitos às disposições da proteção de dados não é necessário que exista gravação: a simples monitorização sem gravação também constitui um tratamento de dados pessoais*"[39].

No entanto, em Portugal, é notória a presença de exemplos destes em zonas residenciais, acreditando-se que por desconhecimento da ilegalidade dos proprietários/moradores ou pelo facto de não existir uma lei geral de videovigilância ou outros meios de controlo.

Precisamente pelo facto de a LPDP não abranger o tratamento de dados pessoais no exercício de atividades exclusivamente pessoais ou domésticas, esta lacuna foi referida na orientação dada pela CNPD quanto à necessidade de existência de legislação geral sobre videovigilância ou por outros meios eletrónicos de controlo[40].

Neste contexto, a necessidade de uma pessoa singular estar sempre a ver tudo o que se passa na sua própria casa, estando presente ou fora dela, merece uma especial reflexão. Antes de mais, não pode ser esquecido o risco de transmissão das imagens em tempo real, através da internet, sabendo que os meios de ataque intrusivo neste tipo de informação/plataforma são cada vez mais sofisticados. A este respeito, foi recentemente noticiada a plataforma criada com o intuito de mostrar o quão fácil é aceder aos sistemas de videovigilância, onde é colocada em causa a privacidade de milhares de pessoas em todo o mundo, incluindo diversas residências portuguesas e espaços de culto, até no interior de igrejas em vários localidades, entre as 254 câmaras a funcionar em território nacional[41]. Coloca-se uma vez mais a questão da privacidade dos cidadãos e, mais grave, do acesso público a dados sensíveis, como o caso da fé religiosa e outros que, como adiante veremos, se inserem neste campo considerado sensível.

Naturalmente, é aceitável a definição de um perímetro de segurança onde sejam instaladas câmaras de videovigilância, especialmente no caso de moradias com espaço privado envolvente, como seja um jardim, garagem ou piscina, supostamente por se encontrar mais vulnerável a eventuais intrusões não desejadas.

---

[38] Cf. CASTRO, Catarina Sarmento e, *Direito da Informática, Privacidade e Dados Pessoais*, Coimbra: Livraria Almedina, 2005, p. 127.

[39] Cf. CASTRO, Catarina Sarmento e, *Direito da Informática, Privacidade e Dados Pessoais*, Coimbra: Livraria Almedina, 2005, p. 125.

[40] Cf. CNPD, *Parecer n.º 22/2003*, in: https://www.cnpd.pt/bin/decisoes/Par/40_22_2003.pdf, consultado em janeiro de 2016.

[41] Cf. COELHO, Maria Inês, *Site Exibe na Web Imagens de Casas e Lojas em Portugal*, in: http://pplware.sapo.pt/informacao/site-exibe-imagens-em-directo-na-web-de-casa-e-lojas-em-portugal/, consultado em dezembro 2015.

Torna-se, porém, muito mais difícil entender o objetivo da instalação de câmaras de videovigilância no interior da residência, quando esse espaço é, naturalmente, o centro da vida privada e familiar. Há, no entanto, ao que parece, quem necessite de estar sempre a ver, sem ser visto, transmitindo a sensação de controlo total permanente. Nestes casos, mais preocupante se torna o registo de dados pessoais, pela indefinição de prazo de conservação de dados, pela possibilidade de registo de som, para além de imagens. Esses dados poderão servir até como argumento num eventual processo de divórcio litigioso, onde um conjunto de pormenores da vida privada e familiar poderão ser usados como indício ou eventualmente como prova, embora descontextualizados. Para além disso, em caso de divórcio, a pretensão da guarda de menores, sendo estes fruto de um matrimónio que chega ao seu término, pode recorrer a imagens registadas no interior da residência, que, num cúmulo de momentos naturais de tensão, quando não sucessivos, entre uma ou mais crianças e seus progenitores, poderão servir como argumento perante o juiz quanto à maior ou menor condição da guarda futura dos menores. Ou seja, como frequentemente se observa na sociedade, quando o litígio ocorre, «os fins justificam os meios».

Vale a pena aqui salientar o facto de o conceito de exercício de atividades exclusivamente pessoais ou domésticas terminar a partir do momento em que exista uma relação laboral no interior de uma residência. Na realidade, caso exista um ou mais trabalhadores que tenham a missão de cuidar de uma casa particular, no interior ou no espaço privado envolvente da residência, estando esse espaço a ser alvo da utilização de dispositivos de videovigilância, o conceito anteriormente referido deixa de fazer sentido. Ou seja, a partir da existência de uma relação laboral num espaço privado, a LPDP passa a ter de ser cumprida, não sendo permitido, a título de exemplo, como adiante verificaremos, a realização de controlo do desempenho profissional do trabalhador, como também não será admitida a recolha de som em todo o espaço a que os trabalhadores tenham acesso.

5. COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS

5.1. NATUREZA

De acordo com o artigo 21º da Lei de Proteção de Dados Pessoais, a CNPD é uma entidade administrativa independente, com poderes de autoridade, que funciona junto da Assembleia da República[42].

Para além de outros aspetos, refere o artigo acima indicado que a CNPD coopera com as autoridades de controlo de proteção de dados de outros Estados na difusão do direito e das regulamentações nacionais em matéria de proteção de dados pessoais, bem como na defesa e no exercício dos direitos de pessoas residentes no estrangeiro.

5.2. ATRIBUIÇÕES

Como já referido, a Lei N.º 67/98 estabelece no n.º 1 do artigo 22º, como primeira atribuição da CNPD, "*controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei*"[43]. O artigo em apreço, refere o dever da CNPD ser consultada sobre quaisquer disposições legais ou instrumentos jurídicos de âmbito europeu ou internacional relativamente ao tratamento de dados pessoais[44]. De salientar que a CNPD tem ainda poderes de investigação e inquérito, poderes de autoridade e de emissão de pareceres prévios, para além de legitimidade para intervir em processos judiciais em casos de violação das disposições da LPDP. A CNPD tem, de igual forma, o dever de denunciar ao Ministério Público as infrações de que tenha conhecimento, no exercício das suas funções e por causa delas.

5.3. COMPETÊNCIA

O artigo 23º da LPDP refere-se às competências da CNPD. Entre estas, constam a emissão de parecer de vária ordem, autorizar ou registar tratamento de dados pessoais, determinar o tempo de conservação de dados, entre outras medidas e autorizações que digam respeito ao tratamento de dados pessoais. No âmbito das suas competências, a CNPD pode ainda apresentar sugestões à Assembleia da República com vista à prossecução das suas atribuições e ao exercício dessas mesmas competências[45].

---

[42] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 67/98 de 26 de Outubro*, 1ª série - A, nº 247, 26 de outubro de 1998, p. 5541.

[43] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 67/98 de 26 de Outubro*, 1ª série - A, nº 247, 26 de outubro de 1998, p. 5541.

[44] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 67/98 de 26 de Outubro*, 1ª série - A, nº 247, 26 de outubro de 1998, pp. 5541-5542.

[45] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 67/98 de 26 de Outubro*, 1ª série - A, nº 247, 26 de outubro de 1998, p. 5552.

A título de exemplo, no âmbito da videovigilância e face às competências legislativas da Assembleia da República, numa anterior proposta de alteração ao regime jurídico do exercício da atividade de segurança privada, a CNPD pronunciou-se (num dos inúmeros pareceres que produziu até à data) no sentido de que "*a vigilância através de meios eletrónicos constitui uma restrição ou limitação a um «direito, liberdade ou garantia» - o direito à privacidade. E pode ainda atingir, mais especificamente, outros direitos da mesma natureza, tais como o direito à imagem e o de liberdade de movimentação*"[46]. Para além disso, referiu ser necessário criar legislação geral sobre vigilância por meios eletrónicos, estando a videovigilância entre esse tipo de meios, tanto para o sector público como privado. No entanto, continua a alargar-se o espaço temporal entre a sugestão de nova legislação (2003) e a sua concretização pelo legislador.

5.4. RELATÓRIOS RECENTES E A QUESTÃO DA VIDEOVIGILÂNCIA

Conforme a alínea p) do artigo 23º da LPDP, compete à CNPD "*promover a divulgação e esclarecimento dos direitos relativos à proteção de dados e dar publicidade periódica à sua atividade, nomeadamente através da publicação de um relatório anual*"[47]. Recorrendo a um dos mais recentes relatórios publicados até ao momento, referente a 2015[48], atente-se à figura seguinte, a qual ilustra a evolução do número total de decisões emitidas entre 2011 e 2015, como ainda o peso das decisões automatizadas nos resultados apresentados.

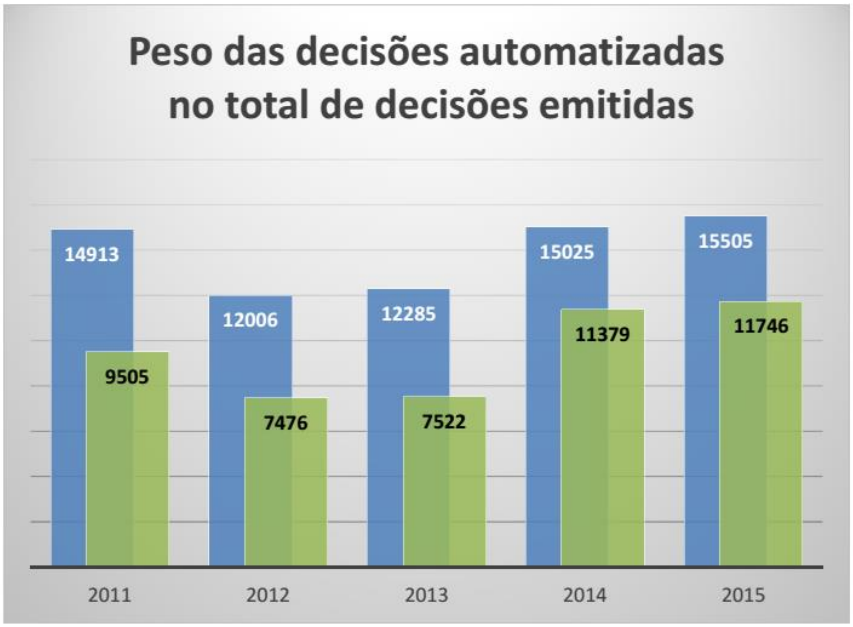

Figura 1: Evolução do total de decisões emitidas pela CNPD entre 2011 e 2015

[46] Cf. CNPD, *Parecer n.º 22/2003*, in: https://www.cnpd.pt/bin/decisoes/Par/40_22_2003.pdf, consultado em janeiro de 2016.

[47] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 67/98 de 26 de Outubro*, 1ª série - A, nº 247, 26 de outubro de 1998, p. 5542.

[48] Cf. CNPD, *Relatório de Atividades, 2015*, in: https://www.cnpd.pt/bin/relatorios/anos/Relatorio_2015.pdf, consultado em janeiro de 2017.

De acordo com o relatório acima indicado, "*os tratamentos de dados relativos aos sistemas de videovigilância continuam a aumentar, tendo sido emitidas no ano passado 10.883 decisões, o que certamente reflete a disponibilização pela CNPD de 24 formulários eletrónicos específicos de videovigilância, ajustados a diferentes setores de atividade*"[49]. Neste documento, em matéria de atividade decisória, é notório o peso da videovigilância no contexto nacional. Na verdade, em 2015, a percentagem ronda os 70%.

Relativamente aos processos de contraordenação abertos pela CNPD, regista-se um aumento superior a 50% no intervalo entre 2011 e 2015[50], conforme ilustra a figura seguinte.

Figura 2: Evolução do total de processos de contraordenação abertos pela CNPD entre 2011 e 2015

Destes processos de contraordenação, "*destaca-se o número de queixas que atingiu em 2015 um número recorde, dando origem a 746 processos. Também as participações realizadas pela GNR e pela PSP, essencialmente quanto às condições de funcionamento dos sistemas de videovigilância, motivaram a abertura de 603 processos*"[51]. Recorrendo à consulta do anterior relatório de atividades da CNPD (2013-2014)[52], quanto ao motivo das queixas apresentadas, "*é possível identificar algumas áreas em que as queixas são mais recorrentes, como sejam sobre sistemas de videovigilância de vizinhos ou de entidades empregadoras*"[53].

[49] Cf. CNPD, *Relatório de Atividades, 2015*, in: https://www.cnpd.pt/bin/relatorios/anos/Relatorio_2015.pdf, consultado em janeiro de 2017.

[50] Cf. CNPD, *Relatório de Atividades, 2015*, in: https://www.cnpd.pt/bin/relatorios/anos/Relatorio_2015.pdf, consultado em janeiro de 2017.

[51] Cf. CNPD, *Relatório de Atividades, 2015*, in: https://www.cnpd.pt/bin/relatorios/anos/Relatorio_2015.pdf, consultado em janeiro de 2017.

[52] Cf. CNPD, *Relatório de Atividades da Comissão Nacional de Proteção de Dados, 2013-2014*, in: https://www.cnpd.pt/bin/relatorios/anos/Relatorio_201314.pdf, consultado em janeiro de 2017.

[53] Cf. CNPD, *Relatório de Atividades da Comissão Nacional de Proteção de Dados, 2013-2014*, in: https://www.cnpd.pt/bin/relatorios/anos/Relatorio_201314.pdf, consultado em janeiro de 2017.

De acordo com os referidos documentos públicos, constata-se que em Portugal a videovigilância tem sido motivo de queixas recorrentes, de participações das forças de segurança, de processos de contraordenação e, consequentemente, de aplicação de coimas. De salientar que parte significativa das queixas apresentadas incidem sobre sistemas de videovigilância de entidades empregadoras. Neste âmbito, poder-se-á imaginar as queixas que não são apresentadas por desconhecimento dos direitos dos trabalhadores, por inconsciência dos riscos quanto aos seus dados pessoais ou mesmo por receio de perda dos seus postos de trabalho, face à relação desequilibrada que ocorre, de forma geral, entre empregador e empregado.

Tal como foi já feita aqui referência, salientava Amadeu Guerra[54], em 2004, que a legislação sobre proteção de dados parece estar pouco divulgada. Na presente data, face aos resultados produzidos em relatórios da CNPD, pode concluir-se que o desconhecimento da legislação em apreço mantêm-se, tornou-se ainda mais evidente, acabando as relações laborais por correr sérios riscos de deterioração.

5.5. GRUPO DE PROTEÇÃO DE DADOS DO ARTIGO 29.º

Comummente referido como «Grupo do artigo 29º», este grupo de trabalho foi instituído pelo artigo 29º da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995[55], doravante designada por Diretiva 95/46/CE. Trata-se de um órgão consultivo europeu independente em matéria de proteção de dados e privacidade, embora se tenha tornado num elemento relevante na definição de políticas e conceitos sobre proteção de dados. As suas atribuições são descritas no artigo 30º da Diretiva 95/46/CE[56] e no artigo 14º da Diretiva 97/66/CE[57]. Curiosamente, esta última Diretiva refere-se ao órgão em questão como o «Grupo de proteção das pessoas no que respeita ao tratamento de dados pessoais», realçando a inerente missão protetora das pessoas. Mais à frente, dar-se-á nota de pareceres e/ou recomendações emitidos por este grupo de trabalho.

[54] Cf. GUERRA, Amadeu, *A Privacidade no Local de Trabalho*, Coimbra: Livraria Almedina, 2004, p.17.

[55] Cf. UNIÃO EUROPEIA, *Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*, in: http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT, consultado em abril 2016.

[56] Cf. UNIÃO EUROPEIA, *Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*, in: http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT, consultado em abril 2016.

[57] Cf. UNIÃO EUROPEIA, *Diretiva 97/66/CE do Parlamento Europeu e do Conselho de 15 de Dezembro de 1997 relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das telecomunicações*, in: http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31997L0066&from=PT, consultado em dezembro 2015.

6. PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS NOUTROS DOCUMENTOS LEGISLATIVOS

6.1. CÓDIGO CIVIL

No ordenamento jurídico português, para além da CRP, o Código Civil também prevê o direito à reserva sobre a intimidade da vida privada. Conforme estabelecido no n.º 1 do artigo 80º, todos devem guardar reserva quanto à intimidade da vida privada de outrem[58].

6.2. CÓDIGO PENAL

No artigo 192º do Código Penal, estabelece-se que a devassa da vida privada, sem consentimento e com intenção, é punível com pena de prisão até 1 ano ou multa até 240 dias[59].

Caso a devassa recorra a meios informáticos, a punição está prevista no artigo 193º, podendo esta alcançar a duração de 2 anos de prisão[60].

6.3. DECLARAÇÃO UNIVERSAL DOS DIREITOS DO HOMEM

A Declaração Universal dos Direitos do Homem refere, no seu artigo 12º, que "*ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a protecção da lei*"[61]. Proclamada em 1948, esta Declaração Universal constitui um documento relevante a nível internacional, o qual, só viria a ser publicado em Diário da República em 9 de Março de 1978[62], justificando-se o atraso na adoção do documento à vigência de um regime autoritário em Portugal.

6.4. CONVENÇÃO EUROPEIA DOS DIREITOS DO HOMEM

No âmbito europeu, conforme determina o artigo 8º da Convenção Europeia dos Direitos do Homem[63], o respeito pela vida privada e familiar corresponde a um direito de qualquer pessoa.

---

58 Cf. PORTUGAL, *Código Civil*, in: https://dre.pt/web/guest/legislacao-consolidada/-/lc/107065833/201710311308/exportPdf/normal/1/cacheLevelPage?_LegislacaoConsolidada_WAR_drefrontofficeportlet_rp=indice, consultado em outubro de 2017.

59 Cf. PORTUGAL, *Códigos Penal e Processo Penal*, Porto: Porto Editora, 2015, p. 98.

60 Cf. PORTUGAL, *Códigos Penal e Processo Penal*, Porto: Porto Editora, 2015, p. 98.

61 Cf. PORTUGAL, *Constituição da República Portuguesa*, Coimbra: Livraria Almedina, 2011, p. 130.

62 Cf. PORTUGAL, *Constituição da República Portuguesa*, Coimbra: Livraria Almedina, 2011, p. 127.

63 Cf. CONSELHO DA EUROPA, *Convenção Europeia dos Direitos do Homem*, in: http://www.echr.coe.int/Documents/Convention_POR.pdf, consultado em maio 2016.

6.5. TRATADO SOBRE O FUNCIONAMENTO DA UNIÃO EUROPEIA (TFUE)

O artigo 16º, n.º 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelece que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.

6.6. CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA

Ainda no âmbito europeu, a proteção de dados pessoais está reforçada e prevista no artigo 8º da Carta dos Direitos Fundamentais da União Europeia. Assim, o n.º 1 refere que "*todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito*"[64].

Outras regras são descritas no n.º 2 do mesmo artigo, onde se estabelece que "*esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação*"[65].

Da citação anterior, cabe aqui destacar as questões da finalidade específica do tratamento dos dados, do consentimento do titular dos dados, do acesso aos dados e do direito de retificação desses dados.

Como não poderia deixar de ser e conforme previsto no n.º 3 do artigo em apreço[66], o cumprimento das regras anteriormente referidas fica sujeito a fiscalização por parte de uma autoridade independente.

---

[64] Cf. UNIÃO EUROPEIA, *Carta dos Direitos Fundamentais da União Europeia*, in: http://www.europarl.europa.eu/charter/pdf/text_pt.pdf, consultado em maio 2016.

[65] Cf. UNIÃO EUROPEIA, *Carta dos Direitos Fundamentais da União Europeia*, in: http://www.europarl.europa.eu/charter/pdf/text_pt.pdf, consultado em maio 2016.

[66] Cf. UNIÃO EUROPEIA, *Carta dos Direitos Fundamentais da União Europeia*, in: http://www.europarl.europa.eu/charter/pdf/text_pt.pdf, consultado em maio 2016.

7. VIDEOVIGILÂNCIA EM PORTUGAL

Em Portugal, como já foi dito, o recurso a dispositivos de videovigilância tem necessariamente de estar enquadrado com a Lei de Proteção de Dados Pessoais, exceto os casos em que esse recurso seja realizado no âmbito do exercício de atividades exclusivamente pessoais ou domésticas. Neste documento, o n.º 4 do artigo 4º é bastante claro ao considerar que "*a presente lei aplica-se à videovigilância e outras formas de captação, tratamento e difusão de sons e imagens que permitam identificar pessoas sempre que o responsável pelo tratamento esteja domiciliado ou sediado em Portugal ou utilize um fornecedor de acesso a redes informáticas e telemáticas estabelecido em território português*"[67].

Recordando o disposto no artigo 2º da LPDP, como princípio geral, "*o tratamento de dados pessoais deve processar-se de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias fundamentais*"[68].

Tendo a intenção de particularizar, não só mas também, a videovigilância operada no âmbito do exercício da atividade de segurança privada, tendo sido, até agora, apresentados alguns elementos base, entende-se chegado o momento adequado para refletir um pouco mais aprofundadamente sobre outros aspetos merecedores de especial atenção.

Assim, a videovigilância pode criar a sensação de um determinado espaço vigiado e por conseguinte seguro. Por outro lado, pode também fazer acreditar "*na possibilidade de impor um controlo sobre o espaço e os indivíduos que nele se encontram*"[69]. Pode ainda legitimamente imaginar-se que "*o sujeito passa a constituir um registo numa qualquer base de dados da qual não tem conhecimento, sem qualquer garantia de que desse registo não resultem consequências imprevisíveis*"[70].

Efetivamente, só muito recentemente o cidadão comum passou a dispor de informação clara, definida na lei, através de simbologia colocada antes da entrada e durante a presença num local de acesso público onde ocorra o registo de imagens. Veja-se que, no âmbito do exercício da atividade de segurança privada e de acordo com a legislação em vigor[71], nos locais objeto de vigilância com recurso a sistemas eletrónicos compostos por câmaras de vídeo para captação de imagem com o objetivo de proteger pessoas e bens, é obrigatória a colocação de um aviso/símbolo, conforme anexo VIII da

[67] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 67/98 de 26 de Outubro*, 1ª série - A, nº 247, 26 de outubro de 1998, p. 5537.

[68] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 67/98 de 26 de Outubro*, 1ª série - A, nº 247, 26 de outubro de 1998, p. 5536.

[69] Cf. FRÓIS, Catarina, *Vigilância e Poder*, Lisboa: Mundos Sociais, 2011, p. XIII.

[70] Cf. FRÓIS, Catarina, *Vigilância e Poder*, Lisboa: Mundos Sociais, 2011, p. XII.

[71] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 34/2013 de 16 de maio*, 1ª série - nº 94, 16 de maio de 2013, p. 2930.

Portaria n.º 273/2013[72], de forma bem visível e de modo mais conveniente ao seu fácil reconhecimento pelos utentes, tanto no perímetro exterior como no interior desses espaços[73].

Figura 3. Sinalização de meios de videovigilância eletrónica[74]

Finalmente, em 2013, foi legislada, em Portugal, uma uniformização da simbologia associada à videovigilância. Isto porque, até então, a simbologia era tão diversa quanto original. No interior de um qualquer estabelecimento comercial, tudo servia, desde um pedido para sorrir por estar a ser filmado, passando por uma simples folha de papel A4 com um *smile* junto a uma imagem de alguém a simular que está a filmar, até aos mais intimidatórios onde se afirmava servirem as imagens como prova de eventual infração criminal. No entanto, hodiernamente, continuam a proliferar estes métodos, sendo menos flagrante naqueles casos em que esses espaços privados de acesso público estão obrigados por lei a dispor de dispositivos de videovigilância com gravação de imagens.

Talvez por desconhecimento dos proprietários dos espaços privados de acesso público, mas certamente também por falta de fiscalização, esta simbologia não está tão disseminada em termos de espaços de acesso público onde se procede à gravação de imagens, como o caso dos inúmeros estabelecimentos comerciais de venda ao público, tais como restaurantes, cafés, pastelarias, cabeleireiros, oficinas, papelarias e outros diversos sectores de atividade.

Na realidade, a simples notificação à CNPD, relativa à instalação de videovigilância, é negligenciada por significativa parte dos responsáveis pelo tratamento de dados, especialmente nos estabelecimentos comerciais de venda ao público, os quais, não estando obrigados a dispor desse sistema, entendem certamente que, em caso de eventual fiscalização de alguma autoridade, bastará afirmar que as

[72] Cf. DIÁRIO DA REPÚBLICA, *Portaria nº 273/2013 de 20 de agosto*, 1ª série - nº 159, 20 de agosto de 2013, p. 4987.

[73] Cf. DIÁRIO DA REPÚBLICA, *Portaria nº 273/2013 de 20 de agosto*, 1ª série - nº 159, 20 de agosto de 2013, p. 4980.

[74] Cf. DIÁRIO DA REPÚBLICA, *Portaria nº 273/2013 de 20 de agosto*, 1ª série - nº 159, 20 de agosto de 2013, p. 4987.

câmaras estão desligadas e que, por essa razão, não deram à CNPD conhecimento da sua instalação. Esta parece ser a realidade que se poderá prolongar até que exista legislação que obrigue, de forma generalizada, os proprietários a cumprir com a legislação em vigor ou, em alternativa, a retirar as câmaras. O papel fiscalizador das forças de segurança, englobado no âmbito dos programas especiais que são anunciados publicamente, como é o caso do «policiamento de proximidade» ou ainda do «comércio seguro», pode, com toda a certeza, ter um efeito benéfico na evolução positiva deste cenário. Mas tudo depende das prioridades que são dadas por quem comanda.

Importa ainda ter em conta a opinião de autores que sustentam que "*a monitorização de certos espaços pode apenas conduzir a alterações no modus operandi criminal ou à deslocação da criminalidade para áreas adjacentes, sem resolver os problemas de fundo*"[75]. Na realidade, será uma ilusão aceitar a videovigilância como dissuasora da criminalidade. Ao invés, todos passam a ser suspeitos de serem suspeitos.

É certo que os sistemas de videovigilância podem produzir efeitos positivos em termos de segurança. Porém, como destacou o próprio Conselho da Europa, "*a eficácia dos seus efeitos não é uniforme. Algumas aplicações traduziram-se numa diminuição de actos ilícitos em espaços públicos. Outras mostraram-se ineficazes ou afastaram a criminalidade para zonas limítrofes ou limitaram-se a oferecer meios de prova em relação às pessoas observadas*"[76].

[75] Cf. FRÓIS, Catarina, *Vigilância e Poder*, Lisboa: Mundos Sociais, 2011, p. XIV.

[76] Cf. CNPD, *Deliberação nº 61/2004 - Princípios Sobre o Tratamento de Dados por Videovigilância*, in: https://www.cnpd.pt/bin/orientacoes/DEL61-2004-VIDEOVIGILANCIA.pdf, consultado em janeiro de 2016.

8. SEGURANÇA PRIVADA

8.1. LEGISLAÇÃO

Em Portugal, o exercício da atividade de segurança privada é sujeito a limites. Estes estão definidos na atual legislação, refletida na sua generalidade pela Lei n.º 34/2013, de 16 de Maio de 2013, doravante designada por Lei n.º 34/2013, para além dos diversos diplomas complementares, entre os quais a Portaria n.º 273/2013, de 20 de agosto de 2013 (alterada pela Portaria n.º 106/2015, de 13 de abril de 2015)[77]. Neste capítulo, serão estes alguns dos principais documentos sujeitos a análise.

A atividade de segurança privada é exercida na prossecução do interesse público, na complementaridade e subsidiariedade das forças e serviços de segurança do Estado, conforme refere o nº 2 do artigo 1º da Lei n.º 34/2013[78]. Porém, no n.º 3 do mesmo artigo, define-se que o exercício da atividade de segurança privada visa exclusivamente a proteção de pessoas e bens e a prevenção da prática de crimes[79]. De salientar que são estes – e apenas estes – os fins do exercício desta atividade.

Exercidas no âmbito da atividade de segurança privada, a exploração e a gestão de centrais de videovigilância fazem parte dos díspares serviços que prestam a terceiros (ou no regime de autoproteção). Contudo, estes serviços não podem deixar de respeitar o legalmente estabelecido, em especial no que concerne aos dados pessoais recolhidos. É certo que, na presente data, a legislação já não permite a recolha de sons de forma arbitrária. Com efeito, a Lei n.º 34/2013, relativamente aos sistemas de videovigilância, determina, no nº 8 do artigo 31º, ser "*proibida a gravação de som pelos sistemas referidos no presente artigo, salvo se previamente autorizada pela Comissão Nacional de Proteção de Dados, nos termos legalmente aplicáveis*"[80].

8.2. MEDIDAS DE SEGURANÇA OBRIGATÓRIAS

8.2.1. Dispositivos de videovigilância

De acordo com o artigo 7º da atual lei de segurança privada, os dispositivos de videovigilância enquadram-se no grupo de medidas de segurança obrigatórias a serem implementadas por algumas empresas ou entidades industriais[81].

[77] Cf. DIÁRIO DA REPÚBLICA, *Portaria nº 106/2015 de 13 de abril*, 1ª série - nº 71, 13 de abril de 2015, pp. 1811-1812.

[78] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 34/2013 de 16 de maio*, 1ª série - nº 94, 16 de maio de 2013, p. 2921.

[79] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 34/2013 de 16 de maio*, 1ª série - nº 94, 16 de maio de 2013, p. 2921.

[80] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 34/2013 de 16 de maio*, 1ª série - nº 94, 16 de maio de 2013, p. 2930.

[81] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 34/2013 de 16 de maio*, 1ª série - nº 94, 16 de maio de 2013, p. 2923.

8.2.2. Obrigatoriedade de instalação

De acordo com o artigo 8º da Lei n.º 34/2013[82], são diversas as empresas ou entidades industriais sujeitas à obrigatoriedade referida anteriormente, entre as quais se podem destacar:

- instituições de crédito e sociedades financeiras;
- conjuntos comerciais e grandes superfícies de comércio;
- estabelecimentos de exibição, compra e venda de metais preciosos;
- estabelecimentos de exibição, compra e venda de obras de arte;
- farmácias e postos de combustível.

Para além destas, dependendo da dimensão e lotação do espaço, estão eventualmente sujeitos à obrigatoriedade de dispor de dispositivos de videovigilância os seguintes locais:

- estabelecimento de restauração e bebidas com espaço de dança ou onde habitualmente se dance (lotação acima de 200 pessoas)[83];
- espetáculos desportivos de natureza profissional ou não profissional considerados de risco elevado[84].

Ou seja, nos casos em que a lotação destes estabelecimentos de restauração e bebidas com espaço de dança ou onde habitualmente se dance ultrapasse as 200 pessoas, em especial aqueles que funcionam durante o período noturno, constata-se a obrigatoriedade de procederem à instalação de dispositivos de videovigilância.

Como adiante veremos, estas empresas ou entidades industriais estão obrigadas à conservação dos dados registados no âmbito da videovigilância, durante um determinado prazo, geralmente 30 dias, após o qual os dados devem ser destruídos. No entanto, algumas delas dispõem de um prazo mais alargado e outras há em que se observa uma indefinição de limite máximo estabelecido para destruição desses dados.

8.3. RESPONSABILIDADE PELO TRATAMENTO DE DADOS

8.3.1. Legislação

No artigo 3º, alínea d) da LPDP, o responsável pelo tratamento de dados é definido como "*a pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais;*

[82] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 34/2013 de 16 de maio*, 1ª série - nº 94, 16 de maio de 2013, pp. 2923-2924.

[83] Cf. DIÁRIO DA REPÚBLICA, *Decreto-Lei nº 135/2014 de 8 de setembro*, 1ª série - nº 172, 8 de setembro de 2014, p. 4803.

[84] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 52/2013 de 25 de julho*, 1ª série - nº 142, 25 de julho de 2013, p. 4379.

sempre que as finalidades e os meios do tratamento sejam determinados por disposições legislativas ou regulamentares, o responsável pelo tratamento deve ser indicado na lei de organização e funcionamento ou no estatuto da entidade legal ou estatutariamente competente para tratar os dados pessoais em causa"[85].

Na verdade, quando não ocorre a identificação expressa de uma pessoa singular com a responsabilidade do tratamento de dados, em particular os relativos às imagens de videovigilância obtidas para além das que são registadas pelas autoridades públicas, torna-se difícil chegar ao autor de um ato ilícito, seja ele o eventual visionamento de imagens fora do previsto na LPDP, a cópia de ficheiros com imagens registadas ou outro ilícito que possa ser imaginado. Por essa razão, a reserva da vida privada e outros direitos fundamentais dos cidadãos podem estar postos em causa.

Comparativamente, veja-se o exemplo de um condutor de um veículo em excesso de velocidade. Quando um dispositivo de radar deteta esse incumprimento e caso não exista uma imediata intervenção das forças de segurança para identificar o condutor em causa, pode sempre ser indicado posteriormente um outro autor dessa transgressão ao Código da Estrada, pelo facto do verdadeiro transgressor ser superiormente penalizado do que um outro, eventualmente o cônjuge ou outro familiar possuidor de carta de condução. De igual modo, a desresponsabilização do ilícito no tratamento de dados parece facilmente poder ocorrer. No entanto, como adiante se verá, a União Europeia tomou recentemente medidas no sentido de um controlo mais acentuado neste domínio, da responsabilização dos responsáveis e de penalizações substancialmente mais pesadas para os infratores.

8.3.2. Garantia da proteção de dados

A responsabilidade pelo tratamento de dados parece ser um dos elementos-chave da preservação das imagens. Também por essa razão, o legislador teve a preocupação de obrigar a tornar público, de modo bem legível a qualquer cidadão, a identificação dos responsáveis pelo tratamento. Além da já referida obrigatoriedade de colocação de um aviso/símbolo, conforme anexo VIII da Portaria n.º 273/2013[86], desde 2013, passou a ser obrigatória a afixação conjunta de informação sobre o responsável pelo tratamento dos dados recolhidos, perante quem os direitos de acesso e retificação desses dados podem ser exercidos. Em conjunto com esta informação, o n.º 5 do artigo 31º da Lei n.º 34/2013[87] determina igualmente a obrigatoriedade de afixar em local bem visível informação relativa às seguintes matérias:

a) a existência e localização das câmaras de vídeo;
b) a menção «Para sua proteção, este local é objeto de videovigilância»;

[85] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 67/98 de 26 de Outubro*, 1ª série - A, nº 247, 26 de outubro de 1998, p. 5536.

[86] Cf. DIÁRIO DA REPÚBLICA, *Portaria nº 273/2013 de 20 de agosto*, 1ª série - nº 159, 20 de agosto de 2013, p. 4987.

[87] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 34/2013 de 16 de maio*, 1ª série - nº 94, 16 de maio de 2013, p. 2930.

c) a menção do nome e alvará ou licença da entidade de segurança privada autorizada a operar o sistema.

Uma ressalva deve ser feita nesta forma de dar conhecimento aos cidadãos para aqueles que, por deficiência, não conseguem ser informados. Veja-se o caso dos invisuais, em que a atual legislação não previu uma alternativa para que estes também possam ter informação antes e/ou depois de entrar num espaço com dispositivos de videovigilância. Talvez um simples sinal sonoro resolvesse esta questão e devolvesse o direito de informação a estes cidadãos com deficiência, da mesma forma que todos os outros já possuem.

8.3.3. Direito de acesso aos dados registados

O acesso aos dados registados, incluindo aqueles que se efetuem no âmbito da videovigilância, está previsto no artigo 11º da LPDP[88]. O titular desses dados, ou seja, a pessoa singular identificada ou identificável numa imagem, tal como acima mencionado[89], tem o direito, através de solicitação ao responsável pelo tratamento, de obter acesso aos seus dados, livremente e sem restrições, com periodicidade razoável e sem demoras ou custos excessivos. No entanto, o responsável pelo tratamento de dados deve tomar todas as medidas técnicas necessárias para mascarar/anonimizar as imagens de terceiros[90].

Para além deste legítimo direito do titular dos dados, as autoridades podem igualmente aceder a esses dados no âmbito de atividade policial, quando estão em causa finalidades relativas à «prevenção ou investigação criminal». Porém, pela diversidade de equipamentos técnicos existentes, com maior ou menor versatilidade, estes podem permitir a difusão ou acesso não autorizado. Uma vez mais se demonstra o risco que pode advir para os cidadãos da ocorrência de acessos não autorizados a dados pessoais.

A propósito desta questão, a CNPD refere que "*tanto o Grupo do artigo 29º como a autoridade italiana de proteção de dados também já sugeriram a adoção de uma solução «que consiste no uso de duas chaves de acesso – podendo uma delas estar na posse do responsável pelo tratamento e outra na da polícia – metodologia que será útil para garantir que as imagens são visualizadas apenas pelo pessoal da polícia e não por pessoal não autorizado»*"[91].

Com toda a certeza, tal como defende a CNPD, para que os responsáveis pelo tratamento de dados possam optar por equipamentos capazes de garantir o cumprimento das medidas de segurança a que

[88] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 67/98 de 26 de Outubro*, 1ª série - A, nº 247, 26 de outubro de 1998, p. 5539.

[89] Veja-se supra, subcapítulo 3.1.

[90] Cf. CNPD, *Deliberação nº 61/2004 - Princípios Sobre o Tratamento de Dados por Videovigilância*, in: https://www.cnpd.pt/bin/orientacoes/DEL61-2004-VIDEOVIGILANCIA.pdf, consultado em janeiro de 2016.

[91] Cf. CNPD, *Deliberação nº 61/2004 - Princípios Sobre o Tratamento de Dados por Videovigilância*, in: https://www.cnpd.pt/bin/orientacoes/DEL61-2004-VIDEOVIGILANCIA.pdf, consultado em janeiro de 2016.

se encontram obrigados, deverá existir um esforço dos produtores de sistemas de gravação de imagens na preocupação da «inviolabilidade».

8.4. PRAZOS DE CONSERVAÇÃO DE DADOS

Os prazos de conservação de dados parecem ser de elevada importância. De uma forma geral, verifica-se uma indefinição generalizada do limite de tempo de conservação de dados no contexto de videovigilância, salvo em casos muitos específicos, expressamente previstos na lei.

A título de exemplo, veja-se que, a Autoridade Nacional de Proteção Civil (ANPC), num *Guia de Apoio Técnico às Associações Humanitárias de Bombeiros*[92], referindo-se aos critérios a seguir para instalação de videovigilância nos quartéis das associações humanitárias de bombeiros, com a finalidade de proteção de pessoas e bens, afirma que "*a lei não estabelece prazo de conservação dos dados*"[93], acrescentando que "*o prazo máximo de 30 dias será um prazo ajustado para a garantia da prossecução das finalidades determinantes da recolha e/ou do tratamento*"[94]. No entanto, este prazo fica ao critério de cada uma das associações, contrariando recomendações da CNPD em não ultrapassar os 30 dias. Efetivamente, cada uma destas associações humanitárias tem os seus próprios órgãos de direção, parte deles em regime de voluntariado e, quiçá, com maior ou menor sensibilidade para as consequências do uso indevido desses dados pessoais. No entanto, não poderão estes elementos de direção escusar-se às responsabilidades e aos riscos de penalizações por incumprimento de regras, em matéria de proteção de dados pessoais.

Imaginem-se, como será facilmente entendível, as inúmeras situações de necessidade de auxílio urgente que justificam a deslocação de cidadãos comuns a um quartel de bombeiros. Nesses momentos de natural aflição, será, com toda a certeza, improvável que um cidadão se preocupe com a sua imagem e/ou vida privada, atendendo ao valor superior que o leva a pedir socorro. Não estando, de modo geral, expressamente definido na lei o limite de tempo para destruição das imagens registadas por câmaras de videovigilância, É caso para se questionar, até que ponto as imagens registadas desses momentos de aflição poderão ser sujeitas a futuras utilizações indevidas. Isto porque, face à rotatividade de quem dirige essas associações, é previsível de igual forma a rotatividade do indivíduo responsável pelo tratamento dos dados, ainda que, em grande parte dos casos, o responsável não seja uma pessoa singular mas sim a própria associação humanitária. Atendendo à dificuldade em definir exatamente o autor de eventual utilização indevida, coloca-se sempre a hipótese de desresponsabilização individual.

[92] Cf. ANPC [Autoridade Nacional de Protecção Civil], *Guia de Apoio Técnico às Associações Humanitárias de Bombeiros*, in: http://www.prociv.pt/Documents/CT_24_www.pdf, consultado em janeiro de 2016.

[93] Cf. ANPC [Autoridade Nacional de Protecção Civil], *Guia de Apoio Técnico às Associações Humanitárias de Bombeiros*, in: http://www.prociv.pt/Documents/CT_24_www.pdf, consultado em janeiro de 2016.

[94] Cf. ANPC [Autoridade Nacional de Protecção Civil], *Guia de Apoio Técnico às Associações Humanitárias de Bombeiros*, in: http://www.prociv.pt/Documents/CT_24_www.pdf, consultado em janeiro de 2016.

Em Portugal, sabendo que existem cerca de 300 municípios, cada um deles, geralmente, contando com um ou mais quartéis de bombeiros voluntários, facilmente se deduz existirem no país várias centenas de tais quartéis. De acordo com a informação disponível internet no *website* da CNPD, olhando apenas para o ano de 2015, verifica-se que foram autorizadas 16 instalações de videovigilância em quartéis de bombeiros voluntários[95]. Boa parte destas autorizações ultrapassam, cada uma delas, a dezena de câmaras de videovigilância, chegando mesmo às 16 câmaras instaladas num único quartel, como é o caso da Associação Humanitária dos Bombeiros Voluntários de Benavente[96].

A proteção de pessoas e bens deve ser, indubitavelmente, uma preocupação de quem dirige uma associação. Todavia, face à quantidade crescente de autorizações de instalação de dispositivos de videovigilância, parece ser necessário prestar maior cuidado quanto à proteção de dados pessoais dos cidadãos, em particular quando exista uma relação laboral.

Relativamente às empresas ou entidades industriais sujeitas à obrigatoriedade de instalação de dispositivos de videovigilância, no âmbito de serviços prestados por empresas de segurança privada, a lei estabelece prazos de conservação de dados registados por dispositivos de videovigilância. Apesar do disposto na Lei de Proteção de Dados Pessoais, nestes casos específicos, os prazos de conservação dos dados, de acordo com os respetivos diplomas legais indicados, são os seguintes:

- instituições de crédito e sociedades financeiras – Prazo não inferior a 30 dias (art.º 90º, n.º 3, da Portaria N.º 273/2013[97], alterada pela Portaria N.º 106/2015);
- conjuntos comerciais e grandes superfícies de comércio – Prazo não inferior a 30 dias (art.º 95º, n.º 3, da Portaria N.º 273/2013[98], alterada pela Portaria N.º 106/2015);
- estabelecimentos de exibição, compra e venda de metais preciosos – Exatamente 90 dias (art.º 97º, n.º 1 al. a) da Portaria N.º 273/2013[99], alterada pela Portaria N.º 106/2015); (art.º 67º, n.º 3 da Lei 98/2015)[100];
- estabelecimentos de exibição, compra e venda de obras de arte – Exatamente 30 dias (art.º 98º, n.º 1, al. a) da Portaria N.º 273/2013[101], alterada pela Portaria N.º 106/2015);

---

95 Cf. CNPD, *Decisões da Comissão*, in: https://www.cnpd.pt/bin/decisoes/decisoes.asp?primeira_escolha=2015&segunda_escolha=10, consultado em janeiro de 2016.

96 Cf. CNPD, *Processo n.º 14968/ 2015 – Autorização N.º 9932/ 2015*, in: https://www.cnpd.pt/bin/decisoes/aut/10_9932_2015.pdf, consultado em janeiro de 2016.

97 Cf. DIÁRIO DA REPÚBLICA, *Portaria nº 273/2013 de 20 de agosto*, 1ª série - nº 159, 20 de agosto de 2013, p. 4976.

98 Cf. DIÁRIO DA REPÚBLICA, *Portaria nº 273/2013 de 20 de agosto*, 1ª série - nº 159, 20 de agosto de 2013, p. 4977.

99 Cf. DIÁRIO DA REPÚBLICA, *Portaria nº 273/2013 de 20 de agosto*, 1ª série - nº 159, 20 de agosto de 2013, p. 4976.

100 Cf. DIÁRIO DA REPÚBLICA, *Lei n.º 98/2015 de 18 de agosto*, 1ª série - nº 160, 18 de agosto de 2015, p. 6100.

101 Cf. DIÁRIO DA REPÚBLICA, *Portaria nº 273/2013 de 20 de agosto*, 1ª série - nº 159, 20 de agosto de 2013, p. 4977.

- farmácias e postos de combustível – Exatamente 30 dias (art.º 100º, n.º 1, al. a) da Portaria N.º 273/2013[102], Alterada pela Portaria N.º 106/2015);
- estabelecimento de restauração e bebidas com espaço de dança ou habitualmente se dance – Exatamente 30 dias (art.º 5º n.º 2, Decreto-Lei N.º 135/2014)[103];
- espetáculos desportivos de natureza profissional ou não profissional considerados de risco elevado - Exatamente 90 dias (art.º 18, Lei N.º 39/2009, Alterada e Republicada pela Lei N.º 52/2013[104]).

Em suma, no âmbito da obrigatoriedade legal de adoção de sistemas de videovigilância, os prazos estabelecidos por lei e para conservação de dados variam entre as modalidades de 30, 90 ou mais dias, sujeitos a deliberação da CNPD, dependendo do tipo de empresas, entidades industriais ou outras organizações.

[102] Cf. DIÁRIO DA REPÚBLICA, *Portaria nº 273/2013 de 20 de agosto*, 1ª série - nº 159, 20 de agosto de 2013, p. 4978.

[103] Cf. DIÁRIO DA REPÚBLICA, *Decreto-Lei nº 135/2014 de 8 de setembro*, 1ª série - nº 172, 8 de setembro de 2014, p. 4803.

[104] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 52/2013 de 25 de julho*, 1ª série - nº 142, 25 de julho de 2013, p. 4379.

9. ALGUNS RISCOS PARA OS CIDADÃOS

9.1. ACESSO INDEVIDO A DADOS PESSOAIS

Face ao exposto no presente texto e até ao momento, apesar das orientações de autoridades europeias e de alguma evolução ao longo dos últimos tempos, ficaram provadas, tanto a vulnerabilidade dos sistemas de gravação de imagens como a facilidade do acesso indevido às mesmas.

Na recente legislação de 2013, no âmbito do exercício da atividade de segurança privada, apesar de ter sido eliminada a possibilidade de gravação de som de forma indiscriminada, sendo hodiernamente necessária autorização fundamentada através de pedido prévio à CNPD, verifica-se, no entanto, a manutenção de equipamentos de deteção de intrusão instalados em múltiplos locais, os quais têm associada a esses equipamentos a possibilidade de registo de imagens e som. Estes equipamentos são instalados por empresas de segurança privada, em estabelecimentos comerciais de venda ao público ou outros, nomeadamente em instalações de empresas que deveriam ter maior preocupação com a proteção de propriedade intelectual, para além da preocupação com a privacidade de todos os colaboradores e visitantes das instalações.

A simples afirmação, por parte das empresas de segurança privada, de que «as imagens só serão visualizadas em caso de acionamento de um alarme» e que «a privacidade dos cidadãos está totalmente protegida e resguardada», pode deixar muitas dúvidas, até porque a «engenharia social» pode, de alguma forma, utilizar estas vulnerabilidades para atingir fins de dimensão assustadora. O mesmo se passa com as empresas/organizações onde estes sistemas estão instalados, teoricamente permitindo gravação de imagens e som apenas em caso de acionamento de alarme de intrusão. Note-se que, nos gabinetes de reuniões ou de direção, onde são tratados assuntos de índole confidencial, poderão, aí, ser escutados e/ou registados sons e imagens. Entra-se aqui no campo da segurança da informação nas organizações, missão a ser cumprida por especialistas em segurança de informação, os quais, por vezes, menosprezam estas pequenas/grandes vulnerabilidades ao realizarem a necessária avaliação e gestão de riscos.

9.2. FINS A QUE SE DESTINAM OS DADOS

Face à crescente evolução tecnológica, os sistemas de videovigilância têm beneficiado de capacidades extra, para além da função essencial de registo de imagens com o objetivo de proteção de pessoas e bens. Por exemplo, o caso da possibilidade de contagem de pessoas, através de tecnologia de reconhecimento facial, isto é, saber quantas pessoas foram registadas pela câmara n.º 1 ou n.º 2 de um determinado sistema de videovigilância.

Efetivamente, as autorizações para instalação de dispositivos de videovigilância que a CNPD atribui às diversas entidades que as solicitam, referem, por norma, o objetivo exclusivo de proteção de pessoas e bens. Mas, a título de exemplo, imagine-se o caso de um conjunto comercial, onde existem diversos

corredores, uns com maior número médio de passagem de pessoas do que outros. A questão é: até que ponto a contagem de pessoas, eventualmente para proteção de pessoas e bens, através de câmaras de videovigilância, não poderá ter outros interesses por parte de quem administra esse conjunto comercial, que, por norma, é também o responsável pelo tratamento dos dados e, consequentemente, tem fácil acesso aos mesmos? Talvez se encontre facilmente uma resposta.

Na realidade, esse tipo de informação pode revelar-se extremamente valiosa para a administração de um conjunto comercial. Na altura de negociar, com os lojistas, o valor a pagar mensalmente pelo metro quadrado do espaço de uma loja, tendo como argumento o número médio de pessoas que por ela passam, ou mesmo a faixa etária, recorrendo à análise associada à tecnologia de reconhecimento facial, poderá fazer subir ou descer o valor do arrendamento em função da frequência de passagem de pessoas, com determinado perfil, em frente a essa loja. Logo, esta finalidade da videovigilância não se enquadra com a proteção de pessoas e bens e, para além disso, os cidadãos podem ser feridos nos seus direitos fundamentais.

Como refere Catarina Sarmento e Castro, "*o não cumprimento das regras de proteção de dados pessoais, inclusive de regras de segurança, por qualquer das entidades que os recolhem e utilizam, ou por entidades terceiras, põe em perigo a nossa privacidade*"[105].

[105] Cf. CASTRO, Catarina Sarmento e, *Direito da Informática, Privacidade e Dados Pessoais*, Coimbra: Livraria Almedina, 2005, p. 21.

10. VIDEOVIGILÂNCIA EM CONTEXTO LABORAL

10.1. MEIOS DE VIGILÂNCIA A DISTÂNCIA

No ordenamento jurídico português, em matéria de legislação laboral, o Código do Trabalho (CT)[106] em vigor corresponde ao documento de referência quanto às normas do Direito do Trabalho.

Assim, o n.º 1 do artigo 20º do CT, relativo aos meios de vigilância à distância, refere que "*o empregador não pode utilizar meios de vigilância a distância no local de trabalho, mediante o emprego de equipamento tecnológico, com a finalidade de controlar o desempenho profissional do trabalhador*"[107]. De salientar que a violação ao disposto anteriormente referido constitui contraordenação muito grave, conforme estabelecido no n.º 4 do mesmo artigo.

Quanto à licitude, o n.º 2 do artigo 20º do CT estabelece que a utilização de equipamento referido no n.º 1 "*é lícita sempre que tenha por finalidade a proteção e segurança de pessoas e bens ou quando particulares exigências inerentes à natureza da atividade o justifiquem*"[108]. Retira-se deste excerto que, de modo geral, apenas a proteção de pessoas e bens confere licitude para a utilização de meios de vigilância a distância, como seja o caso da videovigilância.

Relativamente ao dever de informação, o n.º 3 do artigo 20º do CT determina que nos casos previstos no n.º 1 do mesmo artigo, "*o empregador informa o trabalhador sobre a existência e finalidade dos meios de vigilância utilizados, devendo nomeadamente afixar nos locais sujeitos os seguintes dizeres, consoante os casos: «Este local encontra-se sob vigilância de um circuito fechado de televisão» ou «Este local encontra-se sob vigilância de um circuito fechado de televisão, procedendo-se à gravação de imagem e som», seguido de símbolo identificativo*"[109].

A respeito do estabelecido no artigo 20º do CT, escreve Amadeu Guerra que merecem ser evidenciados alguns princípios, atendendo à sua clareza, simplicidade e coerência, a saber:

a) os sistemas de videovigilância não podem, em caso algum, ser utilizados para «controlar o desempenho profissional do trabalhador». Uma recolha sistemática de som e imagem e um controlo permanente com finalidade de verificação de desempenho da atividade e conduta do trabalhador configura-se agora, *ope legis*, como sendo excessivo e desproporcionado, violador dos direitos e da confiança mútua que o contrato pressupõe, a menos que – excecional e

[106] Cf. PORTUGAL, *Código do Trabalho*, in: http://cite.gov.pt/asstscite/downloads/legislacao/CT25092017.pdf, consultado em outubro 2017.

[107] Cf. PORTUGAL, *Código do Trabalho*, in: http://cite.gov.pt/asstscite/downloads/legislacao/CT25092017.pdf, consultado em outubro 2017.

[108] Cf. PORTUGAL, *Código do Trabalho*, in: http://cite.gov.pt/asstscite/downloads/legislacao/CT25092017.pdf, consultado em outubro 2017.

[109] Cf. PORTUGAL, *Código do Trabalho*, in: http://cite.gov.pt/asstscite/downloads/legislacao/CT25092017.pdf, consultado em outubro 2017.

pontualmente – o processo de produção (v.g. linha de montagem) esteja totalmente direcionado para um tipo de controlo (por supervisão à distância), com o objetivo exclusivo de permitir a interrupção do processo de produção quando se verifique alguma anomalia ou haja perigo para a segurança do trabalhador;

b) podem ser utilizadas estas tecnologias, no âmbito da empresa, com a finalidade de assegurar a proteção e segurança de pessoas e bens;
c) podem ainda ser instalados estes equipamentos quando, em razão da «natureza da atividade», tal tecnologia se apresente como necessária e justificada[110].

Sempre que determinada entidade pretenda recorrer à utilização de meios de vigilância à distância no local de trabalho, o n.º 1 do artigo 21º do CT esclarece que a mesma deverá sujeitar-se a autorização da Comissão Nacional de Proteção de Dados[111]. Importa ainda salientar que o pedido de autorização deve ser acompanhado de parecer da comissão de trabalhadores, conforme estabelecido no n.º 4 do referido artigo[112].

A autorização em causa "*só pode ser concedida se a utilização dos meios for necessária, adequada e proporcional aos objetivos a atingir*"[113], donde se inferem os princípios da necessidade, adequação e proporcionalidade.

De igual forma cabe aqui dar destaque a outros aspetos relativos a dados pessoais recolhidos através dos meios de vigilância à distância. Para que não existam dúvidas, o legislador estabeleceu que estes dados "*são conservados durante o período necessário para a prossecução das finalidades da utilização a que se destinam, devendo ser destruídos no momento da transferência do trabalhador para outro local de trabalho ou da cessação do contrato de trabalho*"[114]. Também aqui a violação do disposto no n.º 3 do artigo 21º do CT constitui contraordenação, embora neste caso seja considerada grave[115].

10.2. RESERVA DA INTIMIDADE DA VIDA PRIVADA EM CONTEXTO LABORAL

Como ensina José Abrantes, os trabalhadores têm "*o direito de esperar um certo grau de respeito pela sua vida privada no seu local de trabalho*"[116]. Na realidade e de forma geral, os trabalhadores não se

[110] Cf. GUERRA, Amadeu, *A Privacidade no Local de Trabalho*, Coimbra: Livraria Almedina, 2004, p. 363.

[111] Cf. PORTUGAL, *Código do Trabalho*, in: http://cite.gov.pt/asstscite/downloads/legislacao/CT25092017.pdf, consultado em outubro 2017.

[112] Cf. PORTUGAL, *Código do Trabalho*, in: http://cite.gov.pt/asstscite/downloads/legislacao/CT25092017.pdf, consultado em outubro 2017.

[113] Cf. PORTUGAL, *Código do Trabalho*, in: http://cite.gov.pt/asstscite/downloads/legislacao/CT25092017.pdf, consultado em outubro 2017.

[114] Cf. PORTUGAL, *Código do Trabalho*, in: http://cite.gov.pt/asstscite/downloads/legislacao/CT25092017.pdf, consultado em outubro 2017.

[115] Cf. PORTUGAL, *Código do Trabalho*, in: http://cite.gov.pt/asstscite/downloads/legislacao/CT25092017.pdf, consultado em outubro 2017.

[116] Cf. ABRANTES, José João, *Direitos Fundamentais da Pessoa Humana no Trabalho, em especial, a reserva da intimidade da vida privada (algumas questões)*, Coimbra: Livraria Almedina, 2014, p. 22.

encontram isolados quando a desempenhar as suas funções. Por consequência, desenvolvem parte significativa das suas relações com outras pessoas, sejam colegas de trabalho, clientes, fornecedores, ou outros.

O artigo 16.º do CT é muito claro quanto à reserva da intimidade da vida privada, tendo esta de ser respeitada tanto pelo empregador como pelo trabalhador[117]. Da leitura e análise dos artigos subsequentes do CT, pode concluir-se que a regra é de ouro: "*o direito à intimidade só pode ser limitado se interesses relevantes o justificarem, não podendo pôr-se em causa os princípios constitucionais da necessidade, adequação e proibição do excesso*"[118]. Aqui, a Constituição da República Portuguesa a funcionar, uma vez mais, como referência.

10.3. VIDEOVIGILÂNCIA E A DELIBERAÇÃO N.º 61/2004 DA CNPD

A Deliberação N.º 61/2004 da CNPD serve, ainda hoje, de referência para as respostas aos pedidos de autorização de tratamento de dados no âmbito da utilização de sistemas de videovigilância. Com base na pesquisa aos dados publicados na internet, na página oficial da CNPD, relativamente às entidades que solicitação e recebem autorização, sabe-se que, na grande maioria dos casos, a utilização destes sistemas é realizada em contexto laboral, importando analisar alguns aspetos que se consideram relevantes na atualidade, apesar de não poder deixar de se atender à diferença temporal que nos separa de 2004, altura da emissão da Deliberação.

Antes de mais, vale a pena reforçar, conforme refere a Deliberação em apreço, que os "*aspectos relativos à videovigilância constituem «matéria atinente a direitos, liberdades e garantias»*"[119]. Se recordarmos o ano de 2004 e o compararmos com a presente data, a capacidade tecnológica dos dias de hoje é substancialmente superior. Desde a qualidade das imagens obtidas, o acesso remoto aos dados, a velocidade de transmissão, o desenvolvimento de técnicas de reconhecimento facial, a possibilidade de visão noturna com as mesmas cores que o olho humano reconhece (sem o limite das imagens noturnas a «preto e branco»), a possibilidade de contagem de pessoas, entre outras evoluções técnicas, torna-se evidente o enorme salto qualitativo que ocorreu no campo da videovigilância. Na verdade, este salto permitiu uma capacidade de recolha de dados muito para além do que, à data da referida Deliberação, seriam as preocupações legítimas da CNPD.

Aliada à evolução tecnológica, assiste-se de igual forma à redução dos custos na implementação destes sistemas de segurança. De tal forma que, hodiernamente, proliferam os locais privados de

[117] Cf. PORTUGAL, *Código do Trabalho*, in: http://cite.gov.pt/asstscite/downloads/legislacao/CT25092017.pdf, consultado em outubro 2017.

[118] Cf. ABRANTES, José João, *Direitos Fundamentais da Pessoa Humana no Trabalho, em especial, a reserva da intimidade da vida privada (algumas questões)*, Coimbra: Livraria Almedina, 2014, p. 27.

[119] Cf. CNPD, *Deliberação nº 61/2004 - Princípios Sobre o Tratamento de Dados por Videovigilância*, in: https://www.cnpd.pt/bin/orientacoes/DEL61-2004-VIDEOVIGILANCIA.pdf, consultado em janeiro de 2016.

acesso público onde estes sistemas operam. Como consequência, os titulares dos dados correm maiores riscos de perder o controlo sobre os seus dados pessoais.

Saliente-se o facto de, à data da Deliberação da CNPD, ser evidente que, face à utilização de sistemas de videovigilância, "*não podem deixar de ser analisados os «efeitos potenciais sobre a liberdade e comportamento dos cidadãos», fazendo-se uma necessária reflexão «sobre o grau de violação da vida privada» que tenha especial incidência nas vertentes da «liberdade de circulação» e na análise de «comportamentos»*"[120]. Efetivamente, os fatores aqui mencionados são hoje ainda mais preocupantes, particularmente quando enquadrados na relação laboral.

Já então era destacada a "*necessidade de as entidades evitarem a «utilização desproporcionada» da videovigilância*"[121]. No entanto, conforme já demonstrado no subcapítulo 5.4., continua a observar-se um aumento anual de autorizações à CNPD.

Sabendo que, no âmbito do recurso à utilização de sistemas de videovigilância, "*o tratamento dos dados visa exclusivamente a protecção de pessoas e bens*"[122], admite-se, "*no mesmo contexto, a utilização destes sistemas para controlo de postos de trabalho que apresentem especiais riscos para os trabalhadores, quer pela sua especial perigosidade em relação ao manuseamento de certas substâncias perigosas, quer pela inacessibilidade ou especial solidão em que os trabalhadores exercem a sua actividade (vg. minas, centrais nucleares, laboratórios em que sejam manuseados produtos químicos perigosos)*"[123]. Assim, quando estão em causa a saúde e o risco de vida dos trabalhadores, o controlo de postos de trabalho pode ser enquadrado na finalidade de proteção de pessoas, neste caso, dos trabalhadores ao serviço de uma determinada entidade patronal; ou seja, nunca para controlo do desempenho laboral ou para outra finalidade de cariz ilícito.

Para além do referido, a Deliberação em apreço contém diversos elementos orientadores que, até à data, têm servido para elucidar os responsáveis pelos tratamentos de dados no âmbito do recurso a sistemas de videovigilância. No entanto, como adiante veremos, face à realidade presente, novas regras estão previstas, a nível internacional, quanto aos responsáveis pelo tratamento, assim como quanto às entidades subcontratadas que, no âmbito da atual legislação de segurança privada, entre outras atividades, instalam, monitorizam, realizam manutenção em equipamentos de videovigilância.

[120] Cf. CNPD, *Deliberação nº 61/2004 - Princípios Sobre o Tratamento de Dados por Videovigilância*, in: https://www.cnpd.pt/bin/orientacoes/DEL61-2004-VIDEOVIGILANCIA.pdf, consultado em janeiro de 2016.

[121] Cf. CNPD, *Deliberação nº 61/2004 - Princípios Sobre o Tratamento de Dados por Videovigilância*, in: https://www.cnpd.pt/bin/orientacoes/DEL61-2004-VIDEOVIGILANCIA.pdf, consultado em janeiro de 2016.

[122] Cf. CNPD, *Deliberação nº 61/2004 - Princípios Sobre o Tratamento de Dados por Videovigilância*, in: https://www.cnpd.pt/bin/orientacoes/DEL61-2004-VIDEOVIGILANCIA.pdf, consultado em janeiro de 2016.

[123] Cf. CNPD, *Deliberação nº 61/2004 - Princípios Sobre o Tratamento de Dados por Videovigilância*, in: https://www.cnpd.pt/bin/orientacoes/DEL61-2004-VIDEOVIGILANCIA.pdf, consultado em janeiro de 2016.

10.4. JURISPRUDÊNCIA NO ÂMBITO DA VIDEOVIGILÂNCIA EM CONTEXTO LABORAL

São públicas as decisões de tribunais superiores com especial interesse para a matéria de que aqui nos ocupamos. A título de exemplo, vale a pena olhar com particular atenção para o Acórdão do Tribunal da Relação do Porto, de 9/5/2011[124]. Das conclusões apresentadas, atente-se ao teor de algumas com as quais concordamos e que se entendem mais relevantes:

1) Nos termos do artigo 20°, n.° 1 do Código do Trabalho, o empregador não pode recorrer a meios de vigilância à distância no local de trabalho, de natureza tecnológica, com a finalidade de controlar o desempenho profissional do trabalhador.
2) O processo disciplinar instaurado à autora, com base exclusivamente nas imagens recolhidas, constitui um controlo abusivo do seu desempenho profissional. O que se pretende com um processo disciplinar senão a avaliação do desempenho profissional de um trabalhador?
3) A autora não autorizou o tratamento de dados pessoais (artigo 6° da Lei n.° 67/98 de 26/10 – Lei da Protecção de Dados), pelo que as imagens recolhidas não podem ser utilizadas no âmbito do processo disciplinar como meio de prova, constituindo a divulgação das referidas imagens uma abusiva intromissão na vida particular e a violação do seu direito à imagem.
4) A entidade empregadora dispõe de mecanismos legais que lhe permitem reagir contra actuações ilícitas dos seus trabalhadores, podendo não só exercer o poder disciplinar através do procedimento apropriado, efectuando as adequadas averiguações internas, como também participar criminalmente às entidades de investigação competentes, que poderão determinar as diligências instrutórias que se mostrarem convenientes.
5) Em qualquer caso, a instalação de câmaras de vídeo, incidindo directamente sobre os trabalhadores durante o seu desempenho profissional, não é uma medida adequada e necessária ao efeito pretendido pela entidade patronal, além de que gera um sacrifício dos direitos de personalidade que é inteiramente desproporcionado relativamente às vantagens de mero cariz económico que se visava obter.
6) As imagens recolhidas não podem, por isso, ser utilizadas como meio de prova em sede de procedimento disciplinar, pois, nestas circunstâncias, a sua divulgação constitui uma abusiva intromissão na vida privada e a violação do direito à imagem da autora (arts. 79° do Código Civil e 26° da Constituição da República Portuguesa), criminalmente punível (art.º 199°, n.° 1, alínea b) do Código Penal)[125].

---

[124] Cf. PORTUGAL, *Proc.º nº 379/10.6TTBCL-A.P1 Apelação*, in: http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/06145eddca240e4d80257893004b5074?OpenDocument, consultado em janeiro de 2017.

[125] Cf. PORTUGAL, *Proc.º nº 379/10.6TTBCL-A.P1 Apelação*, in: http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/06145eddca240e4d80257893004b5074?OpenDocument, consultado em janeiro de 2017.

Em suma, "*o empregador não pode, em processo laboral e como meio de prova, recorrer à utilização de imagens captadas por sistema de videovigilância para fundamentar o exercício da acção disciplinar, ainda que a infracção disciplinar possa, simultaneamente, constituir ilícito penal*"[126].

No entanto, decisões mais recentes divergem. Na verdade, as imagens captadas por sistema de videovigilância têm sido, por vezes, consideradas válidas para fundamentar o exercício da ação disciplinar.

De tudo o que precede, parece não subsistir qualquer dúvida quanto à necessidade de se estabelecerem regras claras quanto a estas matérias. Tal como refere a CNPD, falta publicar legislação geral de enquadramento sobre a utilização de sistemas de videovigilância[127].

[126] Cf. PORTUGAL, *Proc.º nº 379/10.6TTBCL-A.P1 Apelação*, in: http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/06145eddca240e4d80257893004b5074?OpenDocument, consultado em janeiro de 2017.

[127] Cf. CNPD, *Deliberação nº 61/2004 - Princípios Sobre o Tratamento de Dados por Videovigilância*, in: https://www.cnpd.pt/bin/orientacoes/DEL61-2004-VIDEOVIGILANCIA.pdf, consultado em janeiro de 2016.

11. O REGULAMENTO (EU) 2016/679, DE 27 DE ABRIL DE 2016

11.1. ENQUADRAMENTO

11.1.1. Generalidades

Recentemente, no âmbito na União Europeia (UE), os Estados-Membros tomaram conhecimento da publicação do novo «Regulamento Geral sobre a Proteção de Dados»[128], doravante designado por RGPD[129]. Conforme referido no artigo 99.º, a data de entrada em vigor deste documento foi estabelecida para o final de maio de 2016[130]. Apesar de este Regulamento ser obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros, na realidade o início da sua aplicação ocorrerá em 25 de maio de 2018[131]. Ou seja, foi estabelecido um intervalo de dois anos para que se procedam às alterações necessárias em cada Estado-Membro para o total cumprimento de novas regras.

No *Jornal Oficial da União Europeia*, a referência completa atribuída ao Regulamento em causa é: *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 (Regulamento Geral sobre a Proteção de Dados)*[132]. Interessa desde logo destacar uma das características principais deste documento, aliás evidente na própria designação: ou seja, a revogação da Diretiva 95/46/CE[133].

Cada Estado-Membro transpôs a Diretiva para o seu ordenamento jurídico da forma que entendeu, resultando em diferentes níveis de proteção de dados. Veja-se que "*os objetivos e os princípios da Diretiva 95/46/CE continuam a ser válidos, mas não evitaram a fragmentação da aplicação da proteção dos dados ao nível da União, nem a insegurança jurídica ou o sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrónica. As diferenças no nível de proteção dos direitos e das pessoas singulares, nomeadamente do direito à proteção dos dados pessoais no contexto do tratamento desses dados nos Estados-Membros, podem impedir a livre circulação de dados pessoais na União. Essas diferenças podem, por conseguinte, constituir um obstáculo ao exercício das atividades económicas a nível da União, distorcer a concorrência e impedir as autoridades de cumprirem as obrigações que lhes incumbem por força do direito da União. Essas diferenças entre os níveis de proteção devem-se à existência de disparidades na execução e aplicação da Diretiva*

[128] Cf. RGPD.

[129] É denominado na sua versão original como *General Data Protection Regulation* (GDPR).

[130] Cf. RGPD, Artigo 99º.

[131] Cf. RGPD, Artigo 99º.

[132] Cf. RGPD.

[133] Cf. RGPD, Artigo 94º.

95/46/CE"[134]. Face ao exposto, a necessidade de elevar o nível de proteção e torná-lo equivalente em todos os Estados-Membros resultou na concretização do RGPD.

Como anteriormente se afirmou, esta Diretiva 95/46/CE deu origem, no âmbito da ordem jurídica portuguesa, à Lei n.º 67/98[135], de 26 de Outubro.

No mesmo sentido, aponta a CNPD que o "*Regulamento Geral de Proteção de Dados (RGPD) passará a ser aplicado diretamente a partir de 25 de maio de 2018, e vem substituir a atual diretiva e lei de proteção de dados pessoais. O novo quadro legal traz algumas mudanças significativas que terão diferente impacto na vida das organizações, consoante a sua natureza, área de atividade, dimensão e tipo de tratamentos de dados pessoais que realizem*"[136].

Atente-se que, no âmbito na União Europeia, um «regulamento» é um ato legislativo vinculativo, aplicável em todos os seus elementos em todos os Estados-Membros[137].

O documento em causa é bastante extenso. Foram vários anos de trabalho para chegar a um consenso e consequente publicação do texto final, onde, precedendo os 99 artigos que compõem o próprio Regulamento, são apresentados 173 considerandos. No entanto, "*no âmbito da sua aplicação, o Regulamento prevê uma larga margem de intervenção legislativa aos Estados-Membros*"[138]. Adiante analisaremos esta margem de intervenção legislativa, particularmente no que respeita ao tratamento de dados pessoais no contexto laboral.

Conforme indicado pela CNPD, "*é essencial conhecer as novas regras, analisar as novas obrigações, verificar o nível atual de cumprimento e adotar as medidas necessárias durante este período de transição para assegurar que tudo está pronto atempadamente*"[139].Também por esta razão, vale a pena aqui analisar alguns aspetos que se entendem mais relevantes para o cumprimento das novas regras.

11.1.2. Objetivos do regulamento

Logo no início do Regulamento é estabelecido que "*o presente regulamento tem como objetivo contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união económica,*

---

[134] Cf. RGPD, Considerando n.º 9.

[135] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 67/98 de 26 de Outubro*, 1ª série - A, nº 247, 26 de outubro de 1998, pp. 5544-5546.

[136] Cf. CNPD, *10 Medidas Para Preparar a Aplicação do Regulamento Europeu de Proteção de Dados*, in: https://www.cnpd.pt/bin/rgpd/10_Medidas_para_preparar_RGPD_CNPD.pdf, consultado em janeiro de 2017.

[137] Cf. UNIÃO EUROPEIA, *Regulamentos, Diretivas e Outros Atos Legislativos*, in: http://europa.eu/eu-law/decision-making/legal-acts/index_pt.htm, consultado em maio 2016.

[138] Cf. PORTUGAL, *Processo de Consulta Pública Para Aprovação de Legislação Nacional Relativa ao Regulamento Geral de Proteção de Dados (RGPD)*, in: http://www.portugal.gov.pt/pt/consultas-publicas/consultas-legistativas-curso/20170905-mpma-protecao-dados.aspx, consultado em setembro de 2017.

[139] Cf. CNPD, *10 Medidas Para Preparar a Aplicação do Regulamento Europeu de Proteção de Dados*, in: https://www.cnpd.pt/bin/rgpd/10_Medidas_para_preparar_RGPD_CNPD.pdf, consultado em janeiro de 2017.

para o progresso económico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares"[140].

Mais à frente pode ler-se que: "*o presente regulamento estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*"[141]. Fica claro o seu objetivo, ou seja, estabelecer as regras quanto ao tratamento de dados pessoais de pessoas singulares.

O n.º 2 do artigo 1º salienta a questão da defesa de direitos e liberdades fundamentais das pessoas singulares, nomeadamente o direito à proteção de dados pessoais[142]. A este propósito, cabe aqui mencionar que os direitos constitucionais de cada Estado-Membro nunca podem ser ultrapassados. Por outras palavras, a questão da liberdade e privacidade dos cidadãos não deve ser negligenciada em prol de outros interesses, tal como, aliás, a Constituição da República Portuguesa prevê.

De modo idêntico, no âmbito da União Europeia, são necessárias regras que defendam os cidadãos de forma justa e igualitária.

11.1.3. Âmbito da aplicação do regulamento

O artigo 2º do Regulamento em apreço, relativamente ao âmbito da sua aplicação material, determina, no n.º 1, que estas novas regras se aplicam "*ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados*"[143].

Relativamente ao âmbito de aplicação territorial, o artigo 3º estabelece o seguinte:

> "*1. O presente regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União.*
>
> *2. O presente regulamento aplica-se ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com:*
>
> *a) A oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento;*

[140] Cf. RGPD, Considerando n.º 2.

[141] Cf. RGPD, Artigo 1º.

[142] Cf. RGPD, Artigo 1º.

[143] Cf. RGPD, Artigo 2º.

b) O controlo do seu comportamento, desde que esse comportamento tenha lugar na União.

3. O presente regulamento aplica-se ao tratamento de dados pessoais por um responsável pelo tratamento estabelecido não na União, mas num lugar em que se aplique o direito de um Estado-Membro por força do direito internacional público"[144].

Antes de mais, há que esclarecer que, quando o legislador utiliza a palavra «subcontratante», deveria, na verdade, utilizar o termo «subcontratado», ou seja, a entidade subcontratada pelo responsável pelo tratamento de dados pessoais. Esta incorreção já se tinha verificado, com efeito, aquando da publicação da Diretiva 95/46/CE. Deduz-se que, tendo em conta o facto de este Regulamento constituir uma «atualização» da Diretiva, se tenha optado por manter a mesma designação no momento da tradução a partir do documento original em língua inglesa.

Feito o esclarecimento, e ainda no âmbito do texto acima citado, cabe salientar, entre outros aspetos o facto de, para além de existir uma previsão de cumprimento das novas regras por parte dos Estados-Membros, também os Estados que, não fazendo parte da União, tencionem proceder ao tratamento de dados pessoais de cidadãos europeus terão de ter em linha de conta a aplicação do Regulamento em causa. Ou seja, o âmbito deste documento é internacional.

11.2. PRINCIPAIS NOVIDADES APLICÁVEIS AO TRATAMENTO DE DADOS NO ÂMBITO DA VIDEOVIGILÂNCIA

11.2.1. Controlo regular e sistemático dos titulares dos dados em grande escala

No texto do RGPD encontram-se diversos termos ou expressões demasiado abrangentes e, consequentemente, a necessitar de clarificação. Exemplo disso é a expressão "*controlo regular e sistemático dos titulares dos dados em grande escala*"[145]. Veja-se que, de acordo com o n.º 1, alínea b) do artigo 37º do Regulamento, caso a atividade principal de um determinado responsável por tratamento de dados consista, pela sua natureza, âmbito e/ou finalidade ou exija o controlo de titulares de dados pessoais que a expressão anteriormente referida indica (controlo regular e sistemático dos titulares dos dados em grande escala), são impostas maiores obrigações[146]. É o caso da obrigatoriedade de designação de um encarregado de proteção e dados.

A este propósito, tal como entendeu esclarecer o Grupo de Trabalho do art.º 29º, nas linhas orientadoras já publicadas, o CCTV (*closed circuit television*), ou seja, a videovigilância, está incluída

[144] Cf. RGPD, Artigo 3º.

[145] Cf. RGPD, Artigo 37º.

[146] Cf. RGPD, Artigo 37º, alínea b), n.º 1.

neste grupo de atividades principais do responsável pelo tratamento ou do subcontratante[147]. Este organismo discrimina um conjunto de "*activities that may constitute a regular and systematic monitoring of data subjects: operating a telecommunications network; providing telecommunications services; email retargeting; data-driven marketing activities; profiling and scoring for purposes of risk assessment (e.g. for purposes of credit scoring, establishment of insurance premiums, fraud prevention, detection of money-laundering); location tracking, for example, by mobile apps; loyalty programs; behavioural advertising; monitoring of wellness, fitness and health data via wearable devices; closed circuit television; connected devices e.g. smart meters, smart cars, home automation, etc.*"[148].

O mesmo é dizer que a videovigilância, como parte da atividade principal de um determinado responsável por tratamento de dados, implica um controlo regular e sistemático dos titulares dos dados em grande escala.

No entanto, cabe aqui questionar o seguinte: imagine-se uma micro, pequena ou média empresa, onde seja instalado, pelo proprietário, um sistema de videovigilância sem ligação a nenhuma empresa de segurança privada. Face ao tratamento de dados em causa, não estaremos de igual forma perante um «controlo regular e sistemático dos titulares dos dados em grande escala»? Não estarão os trabalhadores sujeitos a esse controlo à distância por parte da entidade empregadora? As opiniões divergem. É nosso entendimento que, efetivamente, face à permanência sistemática e com regularidade no seu posto de trabalho, o trabalhador está sujeito, pelo empregador, a um «controlo regular e sistemático do titular dos dados em grande escala».

Face ao exposto, em casos idênticos ao acima apresentado, a designação de um encarregado de proteção de dados deverá ser equacionada como medida obrigatória pelas autoridades de controlo. Esta medida, para além de auxiliar os responsáveis pelo tratamento de dados, os quais, na sua grande maioria, não deverão possuir conhecimentos especializados em matéria de proteção de dados, evitaria maiores riscos de incumprimento do RGPD.

11.2.2. A responsabilidade do subcontratante

Até à data, a responsabilidade de atos ilícitos no âmbito da proteção de dados pessoais, perante as autoridades competentes, fica limitada ao responsável pelo tratamento de dados em causa.

Com o novo Regulamento, a responsabilidade passa a ser partilhada pelo responsável e pelo subcontratante. Segundo Alexandre Sousa Pinheiro e Carolina Moura, "*no considerando n.º 79, determina-se para o subcontratante um papel distinto do que se encontra hoje na Diretiva e na, ainda,*

[147] Cf. UNIÃO EUROPEIA, *Article 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'),* in: https://iapp.org/media/pdf/resource_center/WP29-2017-04-DPO-Guidance.pdf, consultado em agosto de 2017.

[148] Cf. UNIÃO EUROPEIA, *Article 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'),* in: https://iapp.org/media/pdf/resource_center/WP29-2017-04-DPO-Guidance.pdf, consultado em agosto de 2017.

legislação interna de proteção de dados: «A defesa dos direitos e liberdades dos titulares dos dados, bem como a responsabilidade dos responsáveis pelo seu tratamento e dos subcontratantes, incluindo no que diz respeito à supervisão e às medidas adotadas pelas autoridades de controlo, exigem uma clara repartição das responsabilidades nos termos do presente regulamento, nomeadamente quando o responsável pelo tratamento determina as finalidades e os meios do tratamento conjuntamente com outros responsáveis, ou quando uma operação de tratamento de dados é efetuada por conta de um responsável pelo tratamento». No citado contexto, o artigo 31º do regulamento geral prevê a cooperação com a autoridade de controlo quer do responsável pelo tratamento quer do subcontratante"[149].

Como consequência, toda a cadeia de subcontratantes, partindo do responsável pelo tratamento, terá de seguir o mesmo grau de proteção de dados que o responsável estabeleceu com o primeiro subcontratante.

11.2.3. Encarregado da proteção de dados

No Regulamento Geral sobre a Proteção de Dados, para além da obrigação de adoção de políticas e procedimentos de segurança de dados, é criada a figura do *Data Protection Officer* ou, na versão em língua portuguesa, «encarregado da proteção de dados». Este deve dispor de conhecimentos especializados neste domínio do direito e das práticas da proteção de dados e terá como principal função controlar o cumprimento das regras do novo Regulamento pela empresa ou organismo público.

A designação de «encarregado da proteção de dados» está definida no artigo 37º da seguinte forma:

1. O responsável pelo tratamento e o subcontratante designam um encarregado da proteção de dados sempre que:

    a) o tratamento for efetuado por uma autoridade ou um organismo público, excetuando os tribunais no exercício da sua função jurisdicional;

    b) as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou

    c) as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados nos

[149] Cf. CNPD, *Utilização de Tecnologia de Geolocalização e o Tratamento de Dados Pessoais no Regime Jurídico Português: A Propósito da Deliberação n.º 7680/2014 da Comissão Nacional de Protecção de Dados e Jurisprudência Posterior*, in: https://www.cnpd.pt/bin/revistaforum/forum2016_3/index.html, consultado em janeiro de 2017.

termos do artigo 9º e de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10º.

2. Um grupo empresarial pode também designar um único encarregado da proteção de dados desde que haja um encarregado da proteção de dados que seja facilmente acessível a partir de cada estabelecimento.

3. Quando o responsável pelo tratamento ou o subcontratante for uma autoridade ou um organismo público, pode ser designado um único encarregado da proteção de dados para várias dessas autoridades ou organismos, tendo em conta a respetiva estrutura organizacional e dimensão.

4. Em casos diferentes dos visados no n.º 1, o responsável pelo tratamento ou o subcontratante ou as associações e outros organismos que representem categorias de responsáveis pelo tratamento ou de subcontratantes podem, ou, se tal lhes for exigido pelo direito da União ou dos Estados-Membros, designar um encarregado da proteção de dados. O encarregado da proteção de dados pode agir em nome das associações e de outros organismos que representem os responsáveis pelo tratamento ou os subcontratantes.

5. O encarregado da proteção de dados 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, bem como na sua capacidade para desempenhar as funções referidas no artigo 39.º.

6. O encarregado da proteção de dados pode ser um elemento do pessoal da entidade responsável pelo tratamento ou do subcontratante, ou exercer as suas funções com base num contrato de prestação de serviços.

7. O responsável pelo tratamento ou o subcontratante publica os contactos do encarregado da proteção de dados e comunica-os à autoridade de controlo[150].

Como se constata, a função do «encarregado da proteção de dados» implica responsabilidades elevadas. Para as desempenhar, cabe aqui destacar a já mencionada necessidade de conhecimentos especializados no domínio do direito e das práticas de proteção de dados, mas também a identificação inequívoca perante a autoridade de controlo, que, nestas matérias e em Portugal, corresponde à Comissão Nacional de Proteção de Dados, vulgo CNPD.

O grupo de trabalho do artigo 29º também já se pronunciou acerca desta matéria, através da publicação de linhas orientadoras.

[150] Cf. RGPD, Artigo 37º.

11.2.4. Sanções aplicáveis

O Regulamento Geral sobre a Proteção de Dados prevê, para os casos de incumprimento, diversas sanções a serem aplicadas pela autoridade de controlo respetiva. Assim, entre outros, salienta-se o referido no n.º 6 do artigo 83º: "*o incumprimento de uma ordem emitida pela autoridade de controlo a que se refere o artigo 58.º, n.º 2, está sujeito, em conformidade com o n.º 2 do presente artigo, a coimas até 20 000 000 EUR ou, no caso de uma empresa, até 4 % do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante mais elevado*"[151].

No entanto, neste campo sancionatório, é evidente o cuidado que o Parlamento Europeu e o Conselho da União Europeia tiveram em dar alguma margem aos Estados-Membros, possibilitando o estabelecimento de regras de direito interno relativas a outras sanções aplicáveis no caso de violação do disposto no documento em causa. Apesar disso, conforme n.º 1 do artigo 84º, é frisado que as sanções previstas devem ser efetivas, proporcionais e dissuasivas[152].

Para além das sanções previstas no RGPD, em caso de existir um tratamento de dados que viole o Regulamento, poderá ser necessário indemnizar o titular dos dados pelos danos. Com efeito, "*o responsável pelo tratamento ou o subcontratante deverão reparar quaisquer danos de que alguém possa ser vítima em virtude de um tratamento que viole o presente regulamento* (…). *Os titulares dos dados deverão ser integral e efetivamente indemnizados pelos danos que tenham sofrido. Sempre que os responsáveis pelo tratamento ou os subcontratantes estiverem envolvidos no mesmo tratamento, cada um deles deverá ser responsabilizado pela totalidade dos danos causados*. (…) *Qualquer responsável pelo tratamento ou subcontratante que tenha pago uma indemnização integral, pode posteriormente intentar uma ação de regresso contra outros responsáveis pelo tratamento ou subcontratantes envolvidos no mesmo tratamento*"[153].

Em Portugal, parece existir falta de consciência dos cidadãos em geral para a questão da proteção de dados pessoais, constatando, os mais atentos, evidentes abusos por parte de diversas entidades, nomeadamente no campo da utilização de videovigilância em espaços comerciais, tanto nos de maior dimensão, vulgo grandes superfícies, como os de reduzida dimensão, onde as imagens registadas podem ser transmitidas, através da internet, para outros locais, eventualmente para fora do espaço europeu, colocando em risco os dados pessoais dos cidadãos.

Ainda quanto aos riscos, o RGPD estabelece que, "*sempre que dados pessoais atravessarem fronteiras fora do território da União, aumenta o risco de que as pessoas singulares não possam exercer os seus direitos à proteção de dados, nomeadamente para se protegerem da utilização ilegal ou da divulgação dessas informações. Paralelamente, as autoridades de controlo podem ser incapazes de dar*

[151] Cf. RGPD, Artigo 83º.

[152] Cf. RGPD, Artigo 84º.

[153] Cf. RGPD, Considerando n.º 146.

seguimento a reclamações ou conduzir investigações relacionadas com atividades exercidas fora das suas fronteiras"[154].

11.3. INTERESSES LEGÍTIMOS

Conforme refere o RGPD, "*os interesses legítimos dos responsáveis pelo tratamento, incluindo os dos responsáveis a quem os dados pessoais possam ser comunicados, ou de terceiros, podem constituir um fundamento jurídico para o tratamento, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais do titular, tomando em conta as expectativas razoáveis dos titulares dos dados baseadas na relação com o responsável. Poderá haver um interesse legítimo, por exemplo, quando existir uma relação relevante e apropriada entre o titular dos dados e o responsável pelo tratamento, em situações como aquela em que o titular dos dados é cliente ou está ao serviço do responsável pelo tratamento. De qualquer modo, a existência de um interesse legítimo requer uma avaliação cuidada, nomeadamente da questão de saber se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são recolhidos, que esses poderão vir a ser tratados com essa finalidade. Os interesses e os direitos fundamentais do titular dos dados podem, em particular, sobrepor-se ao interesse do responsável pelo tratamento, quando que os dados pessoais sejam tratados em circunstâncias em que os seus titulares já não esperam um tratamento adicional. Dado que incumbe ao legislador prever por lei o fundamento jurídico para autorizar as autoridades a procederem ao tratamento de dados pessoais, esse fundamento jurídico não deverá ser aplicável aos tratamentos efetuados pelas autoridades públicas na prossecução das suas atribuições. O tratamento de dados pessoais estritamente necessário aos objetivos de prevenção e controlo da fraude constitui igualmente um interesse legítimo do responsável pelo seu tratamento. Poderá considerar-se de interesse legítimo o tratamento de dados pessoais efetuado para efeitos de comercialização direta*"[155].

De acordo com o considerando n.º 40 do RGPD, para que um tratamento seja legítimo, caso a previsão da obrigatoriedade legal desse tratamento esteja estabelecida na legislação em vigor num Estado-Membro, é razão suficiente para a concretização do mesmo, sendo desnecessário, nestes casos, o consentimento do titular dos dados. Exemplo disso é o caso da implementação obrigatória de sistemas de videovigilância em diversos locais privados de acesso público, sejam ourivesarias, postos de abastecimento de combustível, etc., previsto em legislação nacional, como acima mencionado no subcapítulo 8.2.2.

11.4. CONTROLO DO DESEMPENHO PROFISSIONAL DO TRABALHADOR

De acordo com o estabelecido no RGPD, "*o tratamento de dados pessoais de titulares de dados que se encontrem na União por um responsável ou subcontratante que não esteja estabelecido na União deverá ser também abrangido pelo presente regulamento quando esteja relacionado com o controlo do*

[154] Cf. RGPD, Considerando n.º 116.

[155] Cf. RGPD, Considerando n.º 47.

comportamento dos referidos titulares de dados, na medida em que o seu comportamento tenha lugar na União. A fim de determinar se uma atividade de tratamento pode ser considerada «controlo do comportamento» de titulares de dados, deverá determinar-se se essas pessoas são seguidas na Internet e a potencial utilização subsequente de técnicas de tratamento de dados pessoais que consistem em definir o perfil de uma pessoa singular, especialmente para tomar decisões relativas a essa pessoa ou analisar ou prever as suas preferências, o seu comportamento e as suas atitudes"[156]. Donde se conclui que o controlo do desempenho profissional do trabalhador pode ser enquadrado no «controlo do comportamento».

A este respeito, atente-se ao caso da gravação de imagens num local distinto daquele onde as imagens são recolhidas. Veja-se que, através da instalação de um sistema de videovigilância no local de trabalho, o empregador tem a possibilidade de aceder a este meio de controlo à distância, utilizando a internet. Repare-se em situações nas quais o empregador não se encontra fisicamente na União Europeia ou quando um subcontratante disponibilize o serviço de acesso às imagens, gravadas ou em tempo real, não estando este subcontratante estabelecido na União.

Apesar dos esforços desenvolvidos pela CNPD em Portugal, é notório o imenso trabalho que se avizinha, em particular no campo das relações laborais. Quanto a isso, veja-se o referido no considerando n.º 122 do RGPD: "*as autoridades de controlo deverão ser competentes no território do respetivo Estado-Membro para exercer os poderes e desempenhar as funções que lhes são conferidas nos termos do presente regulamento. Deverá ser abrangido, em especial,* (…) *o tratamento que afete os titulares de dados no seu território, ou o tratamento de dados efetuado por um responsável ou subcontratante não estabelecido na União quando diga respeito a titulares de dados residentes no seu território. Deverá ficar abrangido o tratamento de reclamações apresentadas por um titular de dados, a realização de investigações sobre a aplicação do presente regulamento e a promoção da sensibilização do público para os riscos, regras, garantias e direitos associados ao tratamento de dados pessoais*"[157]. Assim, a realização de investigações sobre o RGPD compete à autoridade, ou autoridades de controlo[158], tal como a promoção da sensibilização das pessoas singulares para as matérias associadas ao tratamento de dados pessoais.

No entanto, apesar de algumas medidas propostas pela CNPD[159], é evidente a falta de sensibilização dos responsáveis de determinados tipos de tratamento, entre os quais os aspetos relacionados com videovigilância em espaços privados, os quais geram maior número de participações à CNPD por parte das forças de segurança que se deparam com diversas situações, em função da sua proximidade, de

[156] Cf. RGPD, Considerando n.º 24.

[157] Cf. RGPD, Considerando n.º 122.

[158] Cf. RGPD, Considerando n.º 117. Pode existir mais do que uma autoridade de controlo num Estado-Membro.

[159] Cf. CNPD, *10 Medidas Para Preparar a Aplicação do Regulamento Europeu de Proteção de Dados*, in: https://www.cnpd.pt/bin/rgpd/10_Medidas_para_preparar_RGPD_CNPD.pdf, consultado em janeiro de 2017.

incumprimento da atual LPDP. Nesses espaços existem, naturalmente, relações laborais que devem estar de acordo com o ordenamento jurídico português.

11.5. TRATAMENTO DE DADOS NO CONTEXTO LABORAL

O artigo 88º do Regulamento Geral sobre a Proteção de Dados refere-se especificamente ao tratamento de dados no contexto laboral. Desde logo, no n.º 1, expressa-se a liberdade dada aos Estados-Membros para o estabelecimento de normas mais específicas com vista à proteção dos trabalhadores em contexto laboral, desde o recrutamento até à cessação da relação de trabalho. No entanto, interessa ter em atenção todos os aspetos nomeados. Atente-se ao texto do referido artigo, onde é indicado que "*os Estados-Membros podem estabelecer, no seu ordenamento jurídico ou em convenções coletivas, normas mais específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral, nomeadamente para efeitos de recrutamento, execução do contrato de trabalho, incluindo o cumprimento das obrigações previstas no ordenamento jurídico ou em convenções coletivas, de gestão, planeamento e organização do trabalho, de igualdade e diversidade no local de trabalho, de saúde e segurança no trabalho, de proteção dos bens do empregador ou do cliente e para efeitos do exercício e gozo, individual ou coletivo, dos direitos e benefícios relacionados com o emprego, bem como para efeitos de cessação da relação de trabalho*"[160].

A garantia da defesa dos direitos e liberdades, relativamente ao tratamento de dados pessoais dos trabalhadores no contexto laboral, foi, sem dúvida, preocupação do legislador. Sabendo que o ordenamento jurídico da cada Estado-Membro poderá, neste campo, ser diferente de cada um dos outros, caberá a cada um destes estabelecer normas que garantam, entre outros aspetos, a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral. Veja-se o n.º 2 do referido artigo 88º, onde é expresso que "*as normas referidas incluem medidas adequadas e específicas para salvaguardar a dignidade, os interesses legítimos e os direitos fundamentais do titular dos dados, com especial relevo para a transparência do tratamento de dados, a transferência de dados pessoais num grupo empresarial ou num grupo de empresas envolvidas numa atividade económica conjunta e os sistemas de controlo no local de trabalho*"[161].

De salientar que, no n.º 3 do mesmo artigo, foi definido um prazo para cada Estado-Membro apresentar à Comissão as disposições de direito interno que adotarem, ou qualquer alteração subsequente das mesmas, em conformidade com estabelecido no n.º 1[162]. Com efeito, a data limite para esta medida ser

[160] Cf. RGPD, Artigo 88º.

[161] Cf. RGPD, Artigo 88º.

[162] Cf. RGPD, Artigo 88º.

tomada corresponde ao dia 25 de maio de 2018, ou seja, data a partir da qual o Regulamento Geral sobre a Proteção de Dados é aplicável[163].

Partindo da interpretação do n.º 1, cabe aqui destacar, antes de mais, um primeiro aspeto que se entende relevante: o legislador teve intenção expressa de garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral.

Um segundo aspeto a salientar é a eventual necessidade de estabelecer normas para proteção dos bens do empregador ou do cliente.

No entanto, conforme o n.º 2, as normas adotadas terão de incluir medidas adequadas e específicas para salvaguardar a dignidade, os interesses legítimos e os direitos fundamentais do titular dos dados[164]. Saliente-se o facto de ser dado especial relevo à transparência do tratamento de dados, bem como aos sistemas de controlo no local de trabalho.

Entende-se serem, neste momento, os aspetos anteriormente referidos a merecer particular reflexão, face ao tratamento de dados no âmbito da videovigilância em contexto laboral. Em suma, falamos de normas mais específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral. É o que iremos propor mais à frente.

11.6. CIRCULAÇÃO DE DADOS

Conforme se constata, "*a integração económica e social resultante do funcionamento do mercado interno provocou um aumento significativo dos fluxos transfronteiriços de dados pessoais. O intercâmbio de dados entre intervenientes públicos e privados, incluindo as pessoas singulares, as associações e as empresas, intensificou-se na União Europeia. As autoridades nacionais dos Estados-Membros são chamadas, por força do direito da União, a colaborar e a trocar dados pessoais entre si, a fim de poderem desempenhar as suas funções ou executar funções por conta de uma autoridade de outro Estado-Membro*"[165].

A circulação de dados pessoais de trabalhadores implica riscos, em especial quando a transferência desses dados ultrapassa as fronteiras de um determinado Estado ou, mais ainda, quando ultrapassa as fronteiras da UE. A esse propósito, o Grupo de trabalho do artigo 29º pronunciou-se recentemente, afirmando que "*the use of most applications in the cloud will result in the international transfer of employee data. It should be ensured that personal data transferred to a third country outside the EU takes place only where an adequate level of protection is ensured and that the data shared outsider the EU/EEA and subsequent access by other entities within the group remains limited to the minimum*

[163] Cf. RGPD, Artigo 88º.

[164] Cf. RGPD, Artigo 88º.

[165] Cf. RGPD, Considerando n.º 5.

necessary for the intended purposes"[166]. Em suma, a proteção dos dados tem de estar assegurada no destinatário, com acesso limitado ao necessário e os fins devidamente estabelecidos.

Ainda a este respeito, "*os responsáveis pelo tratamento que façam parte de um grupo empresarial ou de uma instituição associada a um organismo central poderão ter um interesse legítimo em transmitir dados pessoais no âmbito do grupo de empresas para fins administrativos internos, incluindo o tratamento de dados pessoais de clientes ou funcionários. Os princípios gerais que regem a transmissão de dados pessoais, no âmbito de um grupo empresarial, para uma empresa localizada num país terceiro mantêm-se inalterados*"[167].

11.7. FINS A QUE SE DESTINAM OS DADOS

O RGPD estabelece que "*as finalidades específicas do tratamento dos dados pessoais deverão ser explícitas e legítimas e ser determinadas aquando da recolha dos dados pessoais. Os dados pessoais deverão ser adequados, pertinentes e limitados ao necessário para os efeitos para os quais são tratados. Para isso, é necessário assegurar que o prazo de conservação dos dados seja limitado ao mínimo. Os dados pessoais apenas deverão ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios. A fim de assegurar que os dados pessoais sejam conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar os prazos para o apagamento ou a revisão periódica*"[168].

Ainda a este respeito, o RGPD refere que "*o tratamento de dados pessoais para outros fins que não aqueles para os quais os dados pessoais tenham sido inicialmente recolhidos apenas deverá ser autorizado se for compatível com as finalidades para as quais os dados pessoais tenham sido inicialmente recolhidos. Nesse caso, não é necessário um fundamento jurídico distinto do que permitiu a recolha dos dados pessoais.* (…) *A fim de apurar se a finalidade de uma nova operação de tratamento dos dados é ou não compatível com a finalidade para que os dados pessoais foram inicialmente recolhidos, o responsável pelo seu tratamento, após ter cumprido todos os requisitos para a licitude do tratamento inicial, deverá ter em atenção, entre outros aspetos, a existência de uma ligação entre a primeira finalidade e aquela a que se destina a nova operação de tratamento que se pretende efetuar, o contexto em que os dados pessoais foram recolhidos, em especial as expectativas razoáveis do titular dos dados quanto à sua posterior utilização, baseadas na sua relação com o responsável pelo tratamento; a natureza dos dados pessoais; as consequências que o posterior tratamento dos dados pode ter para o seu titular; e a existência de garantias adequadas tanto no tratamento inicial como nas outras operações de tratamento previstas.* (…) *Em todo o caso, deverá ser garantida a aplicação dos*

[166] Cf. UNIÃO EUROPEIA, *Opinion 2/2017 on data processing at work*, in: http://www.google.pt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjUm72n_prWAhXKyRoKHfBnBQQQFggmMAA&url=http%3A%2F%2Fec.europa.eu%2Fnewsroom%2Fdocument.cfm%3Fdoc_id%3D45631&usg=AFQjCNFL9EUmcaORV7p_Z6N12WltBgUlaA, consultado em agosto de 2017.

[167] Cf. RGPD, Considerando n.º 48.

[168] Cf. RGPD, Considerando n.º 39.

princípios enunciados pelo presente regulamento e, em particular, a obrigação de informar o titular dos dados sobre essas outras finalidades e sobre os seus direitos, incluindo o direito de se opor"[169].

Através do registo de imagens de videovigilância em contexto laboral – mas não só –, poderão estes dados ser utilizados para outros fins, incluindo, definição de perfis, por exemplo, quanto ao grau de produtividade de determinado trabalhador. No entanto, conforme referido no considerando n.º 60, "*os princípios do tratamento equitativo e transparente exigem que o titular dos dados seja informado da operação de tratamento de dados e das suas finalidades. O responsável pelo tratamento deverá fornecer ao titular as informações adicionais necessárias para assegurar um tratamento equitativo e transparente tendo em conta as circunstâncias e o contexto específicos em que os dados pessoais forem tratados. O titular dos dados deverá também ser informado da definição de perfis e das consequências que daí advêm*"[170].

11.8. ACESSO INDEVIDO A DADOS PESSOAIS

A obrigação de garantia de segurança dos dados pessoais também está prevista no RGPD, nos seguintes termos: "*os dados pessoais deverão ser tratados de uma forma que garanta a devida segurança e confidencialidade, incluindo para evitar o acesso a dados pessoais e equipamento utilizado para o seu tratamento, ou a utilização dos mesmos, por pessoas não autorizadas*"[171]. No âmbito da videovigilância, o acesso indevido aos dados entende-se como da maior relevância. Veja-se, a título de exemplo, o caso de obtenção de cópias de imagens registadas para utilização ilícita ou, noutro caso, a destruição das imagens gravadas, de forma a não possibilitar o recurso a essa informação como meio de prova de ato ilícito.

11.9. ADOÇÃO DE MEDIDAS PARA EFETIVA SEGURANÇA DAS IMAGENS

Tal como referido no RGPD, "*as pessoas singulares deverão poder controlar a utilização que é feita dos seus dados pessoais. Deverá ser reforçada a segurança jurídica e a segurança prática para as pessoas singulares, os operadores económicos e as autoridades públicas*"[172]. Na verdade, o reforço da segurança prática, referida na anterior citação, leva-nos a ponderar sobre as medidas a tomar pelos responsáveis de diversos tratamentos de dados, para que, especificamente no âmbito da videovigilância em contexto laboral, possam ser adotados procedimentos que evidenciem um reforço da segurança dos dados em causa.

Uma das preocupações dos responsáveis, e dos subcontratantes, pelo tratamento de dados, terá de ser a preservação da segurança a fim de evitar a violação do estabelecido no RGPD. Assim, no universo

[169] Cf. RGPD, Considerando n.º 50.

[170] Cf. RGPD, Considerando n.º 60.

[171] Cf. RGPD, Considerando n.º 39.

[172] Cf. RGPD, Considerando n.º 7.

de medidas sugeridas pelo legislador, é dada particular atenção ao recurso à criptografia. Como estipula o RGPD, "*a fim de preservar a segurança e evitar o tratamento em violação do presente regulamento, o responsável pelo tratamento, ou o subcontratante, deverá avaliar os riscos que o tratamento implica e aplicar medidas que os atenuem, como a cifragem*"[173].

Quanto a esta «ferramenta» de segurança da informação, a criptografia, pode ser sinteticamente entendida da seguinte forma:

"*Cryptography deals with two types of information:*

- *Unencrypted information – Information in understandable form. Unencrypted information is plaintext, or cleartext.*
- *Encrypted information – Information in scrambled form. Encrypted information is ciphertext.*

Encryption is the act of scrambling plaintext into ciphertext. Decryption is the act of unscrrambling ciphertext into plaintext.

Encryption uses a known mathematical process for performing its function. This process is known as an algorithm. An algorithm is a repeatable process that produces the same result when it receives the same imput. A cipher is an algorithm to encrypt or decrypt information. This repeatability is importante to make sure that information, once encrypted, can be decrypted"[174].

No âmbito do tratamento de dados através da videovigilância, esta medida revela-se de grande importância, atendendo aos riscos que envolve, não só pelo recurso a gravadores de vídeo como ainda pela transmissão de imagens pela internet. É preciso não esquecer que a tecnologia não tem parado de evoluir neste campo, possibilitando, entre outros aspetos, no contexto laboral, o controlo do trabalhador à distância.

11.10. OUTROS ASPETOS DE RELEVO NO RGPD

Ao longo do texto do RGPD, a referência a direitos fundamentais é uma constante. A título de exemplo, a seguinte afirmação é reflexo disso: "*a proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental*"[175].

De acordo com o RGPD, "*o direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade. O presente regulamento respeita todos os direitos*

[173] Cf. RGPD, Considerando n.º 83.

[174] Cf. KIM, David, SOLOMON, Michael G., *Fundamentals of Information Systems Security*, 2nd ed., Burlington: Jones & Bartlett Learning, 2013, p. 299.

[175] Cf. RGPD, Considerando n.º 1.

fundamentais e observa as liberdade e os princípios reconhecidos na Carta, consagrados nos Tratados, nomeadamente o respeito pela vida privada e familiar, pelo domicílio e pelas comunicações, a proteção dos dados pessoais, a liberdade de pensamento, de consciência e de religião, a liberdade de expressão e de informação, a liberdade de empresa, o direito à ação e a um tribunal imparcial, e a diversidade cultural, religiosa e linguística"[176]. Como se constata, o princípio da proporcionalidade é desde logo salientado. Apesar de tudo, a liberdade de empresa não deixa de ser referida, o que nos obriga a uma reflexão mais aprofundada sobre o tratamento de dados em contexto laboral.

Apesar da necessidade de "*assegurar em toda a União a aplicação coerente e homogénea das regras de defesa dos direitos e das liberdades fundamentais das pessoas singulares no que diz respeito ao tratamento de dados pessoais* (…), *o presente regulamento não exclui o direito dos Estados-Membros que define as circunstâncias de situações específicas de tratamento, incluindo a determinação mais precisa das condições em que é lícito o tratamento de dados pessoais*"[177].

Outro aspeto que interessa destacar prende-se com o âmbito da aplicação do RGPD quanto ao tecido empresarial. Veja-se que "*a fim de assegurar um nível coerente de proteção das pessoas singulares no conjunto da União e evitar que as divergências constituam um obstáculo à livre circulação de dados pessoais no mercado interno, é necessário um regulamento que garanta a segurança jurídica e a transparência aos operadores económicos, incluindo as micro, pequenas e médias empresas, que assegure às pessoas singulares de todos os Estados-Membros o mesmo nível de direitos suscetíveis de proteção judicial e imponha obrigações e responsabilidades iguais aos responsáveis pelo tratamento e aos seus subcontratantes, que assegure um controlo coerente do tratamento dos dados pessoais, sanções equivalentes em todos os Estados-Membros, bem como uma cooperação efetiva entre as autoridades de controlo dos diferentes Estados-Membros*"[178]. Em suma, as entidades públicas e privadas de todos os Estados-Membros devem, de forma equivalente, manter um controlo coerente do tratamento dos dados, cumprir as suas obrigações e assumir as suas responsabilidades.

Com efeito, o RGPD reforça a necessidade de cumprimento de vários princípios. Veja-se que "*o tratamento de dados pessoais deverá ser efetuado de forma lícita e equitativa. Deverá ser transparente para as pessoas singulares que os dados pessoais que lhes dizem respeito são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento e a medida em que os dados pessoais são ou virão a ser tratados. O princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples. Esse princípio diz respeito, em particular, às informações fornecidas aos titulares dos dados sobre a identidade do responsável pelo tratamento dos mesmos e os fins a que o tratamento se destina, bem como às informações que se destinam a assegurar que seja efetuado com equidade e transparência para com as pessoas singulares em causa, bem como a*

[176] Cf. RGPD, Considerando n.º 4.

[177] Cf. RGPD, Considerando n.º 10.

[178] Cf. RGPD, Considerando n.º 13.

salvaguardar o seu direito a obter a confirmação e a comunicação dos dados pessoais que lhes dizem respeito que estão a ser tratados. As pessoas singulares a quem os dados dizem respeito deverão ser alertadas para os riscos, regras, garantias e direitos associados ao tratamento dos dados pessoais e para os meios de que dispõem para exercer os seus direitos relativamente a esse tratamento"[179].

Quando se coloca a questão de um determinado dado poder ser considerado dado pessoal ou não, surgem por vezes algumas dúvidas. Nesse sentido, o RGPD oferece um maior esclarecimento quanto à questão de uma pessoa singular ser identificável ou não. Veja-se que "*para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica*"[180]. Ora, à presente data, no âmbito da utilização de sistemas de videovigilância, a tecnologia disponível permite identificar uma pessoa, com elevado grau de certeza, custos reduzidos e num curto espaço de tempo. Basta falar em reconhecimento facial em espaços privados de acesso público, tomando como exemplo as grandes superfícies comerciais.

Face à evolução tecnológica, outro aspeto que interessa aqui salientar reporta-se à possibilidade das modernas câmaras de videovigilância poderem ver o que o olho humano não vê. Ou seja, num local pouco iluminado, onde é suposto existir maior privacidade, um trabalhador pode supor encontrar-se menos visível pelo sistema de videovigilância. No entanto, na presente data, através do recurso a raios infravermelhos nas câmaras de videovigilância, é possível ver e registar imagens com níveis de qualidade elevados, transformando a pouca visibilidade em alta visibilidade e de forma policromática. Ou seja, até algum tempo atrás, durante a noite ou em locais de fraca iluminação, os sistemas de videovigilância só registavam imagens monocromáticas, vulgo «preto e branco». Atualmente, na mesma situação, a tecnologia permite a obtenção de imagens policromáticas, vulgo «a cores». Note-se que este aspeto não é geralmente considerado pela grande parte dos titulares dos dados, atendendo ao seu desconhecimento quanto às potencialidades que o desenvolvimento tecnológico tem refletido nos sistemas de videovigilância, facto este que implica o desconhecimento da consequente perda de privacidade.

Como de pode ler no RGPD, o "*regulamento não exige uma lei específica para cada tratamento de dados. Poderá ser suficiente uma lei para diversas operações de tratamento baseadas numa obrigação jurídica à qual esteja sujeito o responsável pelo tratamento, ou se o tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública. Deverá também caber ao direito da União ou dos Estados-Membros determinar qual a finalidade do tratamento dos dados.*

[179] Cf. RGPD, Considerando n.º 39.

[180] Cf. RGPD, Considerando n.º 26.

Além disso, a referida lei poderá especificar as condições gerais do presente regulamento que regem a legalidade do tratamento dos dados pessoais, estabelecer regras específicas para determinar os responsáveis pelo tratamento, o tipo de dados pessoais a tratar, os titulares dos dados em questão, as entidades a que os dados pessoais podem ser comunicados, os limites a que as finalidades do tratamento devem obedecer, os prazos de conservação e outras medidas destinadas a garantir a licitude e equidade do tratamento. Deverá igualmente caber ao direito da União ou dos Estados-Membros determinar se o responsável pelo tratamento que exerce funções de interesse público ou prerrogativas de autoridade pública deverá ser uma autoridade pública ou outra pessoa singular ou coletiva de direito público, ou, caso tal seja do interesse público, incluindo por motivos de saúde, como motivos de saúde pública e proteção social e de gestão dos serviços de saúde, de direito privado, por exemplo uma associação profissional"[181].

No campo dos direitos dos titulares dos dados, de acordo com o RGPD, "*deverão ser previstas regras para facilitar o exercício pelo titular dos dados dos direitos que lhe são conferidos ao abrigo do presente regulamento, incluindo procedimentos para solicitar e, sendo caso disso, obter a título gratuito, em especial, o acesso a dados pessoais, a sua retificação ou o seu apagamento e o exercício do direito de oposição. O responsável pelo tratamento deverá fornecer os meios necessários para que os pedidos possam ser apresentados por via eletrónica, em especial quando os dados sejam também tratados por essa via. O responsável pelo tratamento deverá ser obrigado a responder aos pedidos do titular dos dados sem demora injustificada e o mais tardar no prazo de um mês e expor as suas razões quando tiver intenção de recusar o pedido*"[182].

No entanto, não poderá deixar de se atender ao facto de "*quando um determinado conjunto de dados pessoais disser respeito a mais de um titular, o direito de receber os dados pessoais não deverá prejudicar os direitos e liberdades de outros titulares de dados nos termos do presente regulamento*"[183]. Por isso, no âmbito da videovigilância, o responsável pelo tratamento deverá munir-se de meios para proteger a identidade dos outros titulares de dados que surjam nas imagens.

Olhando agora para o campo dos direitos dos titulares dos dados, em particular quanto ao direito ao «esquecimento», mesmo em contexto laboral, veja-se que, conforme referido no RGPD, "*os titulares dos dados deverão ter direito a que os dados que lhes digam respeito sejam retificados e o «direito a serem esquecidos» quando a conservação desses dados violar o presente regulamento ou o direito da União ou dos Estados-Membros aplicável ao responsável pelo tratamento. Em especial, os titulares de dados deverão ter direito a que os seus dados pessoais sejam apagados e deixem de ser objeto de tratamento se deixarem de ser necessários para a finalidade para a qual foram recolhidos ou tratados, se os titulares dos dados retirarem o seu consentimento ou se opuserem ao tratamento de dados pessoais que lhes digam respeito ou se o tratamento dos seus dados pessoais não respeitar o disposto*

[181] Cf. RGPD, Considerando n.º 45.

[182] Cf. RGPD, Considerando n.º 59.

[183] Cf. RGPD, Considerando n.º 68.

no presente regulamento"[184]. A este respeito, pode ser tomado como exemplo o caso do término da relação laboral ou da mudança de local de trabalho de um trabalhador.

Mantendo o foco nos direitos das pessoas singulares, o RGPD estatui que "*o titular dos dados deverá ter o direito de não ficar sujeito a uma decisão, que poderá incluir uma medida, que avalie aspetos pessoais que lhe digam respeito, que se baseie exclusivamente no tratamento automatizado e que produza efeitos jurídicos que lhe digam respeito ou o afetem significativamente de modo similar, como a recusa automática de um pedido de crédito por via eletrónica ou práticas de recrutamento eletrónico sem qualquer intervenção humana. Esse tratamento inclui a definição de perfis mediante qualquer forma de tratamento automatizado de dados pessoais para avaliar aspetos pessoais relativos a uma pessoa singular, em especial a análise e previsão de aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados, quando produza efeitos jurídicos que lhe digam respeito ou a afetem significativamente de forma similar. (…) tal tratamento deverá ser acompanhado das garantias adequadas, que deverão incluir a informação específica ao titular dos dados e o direito de obter a intervenção humana, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e de contestar a decisão*"[185]. Refere ainda o RGPD que a "*definição de perfis está sujeita às regras do presente regulamento que regem o tratamento de dados pessoais, como o fundamento jurídico do tratamento ou os princípios da proteção de dados*"[186].

Quando estão em causa riscos para os titulares dos dados, "*deverá ser consagrada a responsabilidade do responsável por qualquer tratamento de dados pessoais realizado por este ou por sua conta. Em especial, o responsável pelo tratamento deverá ficar obrigado a executar as medidas que forem adequadas e eficazes e ser capaz de comprovar que as atividades de tratamento são efetuadas em conformidade com o presente regulamento, incluindo a eficácia das medidas. Essas medidas deverão ter em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como o risco que possa implicar para os direitos e liberdades das pessoas singulares*"[187]. Ou seja, também o responsável pelo tratamento de dados, no âmbito da videovigilância, em contexto laboral, tem a obrigação de executar medidas de acordo com o estabelecido no RGPD. Para além disso, tem de comprovar a sua eficácia.

No campo dos riscos associados ao tratamento de dados, estipula o RGPD que "*o risco para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial quando o tratamento possa dar origem à discriminação, à usurpação ou*

[184] Cf. RGPD, Considerando n.º 65.

[185] Cf. RGPD, Considerando n.º 71.

[186] Cf. RGPD, Considerando n.º 72.

[187] Cf. RGPD, Considerando n.º 74.

roubo da identidade, (…)*; quando os titulares dos dados possam ficar privados dos seus direitos e liberdades ou impedidos do exercício do controlo sobre os respetivos dados pessoais; quando forem tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical* (…)*; quando forem avaliados aspetos de natureza pessoal, em particular análises ou previsões de aspetos que digam respeito ao desempenho no trabalho*"[188].

Quanto à avaliação do grau de risco, de acordo com o RGPD, "*a probabilidade e a gravidade dos riscos para os direitos e liberdades do titular dos dados deverá ser determinada por referência à natureza, âmbito, contexto e finalidades do tratamento de dados. Os riscos deverão ser aferidos com base numa avaliação objetiva, que determine se as operações de tratamento de dados implicam risco ou risco elevado*"[189].

Neste contexto, o RGPD indica que "*as orientações sobre a execução de medidas adequadas e sobre a comprovação de conformidade pelos responsáveis pelo tratamento ou subcontratantes, em especial no que diz respeito à identificação dos riscos relacionados com o tratamento, à sua avaliação em termos de origem, natureza, probabilidade e gravidade, bem como à identificação das melhores práticas para a atenuação dos riscos, poderão ser obtidas nomeadamente recorrendo a códigos de conduta aprovados*"[190]; isto para além de outras soluções.

Consultando o *site* da CNPD e quanto ao recurso a códigos de conduta, verifica-se que não existe, em Portugal, ao contrário de outras autoridades de controlo de Estados-Membros, relativamente ao tratamento de dados no âmbito da videovigilância, particularmente em contexto laboral, nenhum código de conduta específico para videovigilância que possa orientar os responsáveis para a adoção das melhores práticas para atenuação dos riscos, e não só. Parece ser o momento ideal para a sua realização, podendo este código servir de referência para os responsáveis ou subcontratantes.

A este propósito e relativamente aos subcontratantes, determina o RGPD que "*o facto de o subcontratante cumprir um código de conduta aprovado ou um procedimento de certificação aprovado poderá ser utilizado como elemento para demonstrar o cumprimento das obrigações do responsável pelo tratamento*"[191]. Mais uma vez, a adesão a um código de conduta é apontada como uma solução para demonstrar o cumprimento do RGPD.

De acordo com o RGPD, um código de conduta poderá, nomeadamente, "*regular as obrigações dos responsáveis pelo tratamento e dos subcontratantes, tendo em conta o risco que poderá resultar do*

[188] Cf. RGPD, Considerando n.º 75.

[189] Cf. RGPD, Considerando n.º 76.

[190] Cf. RGPD, Considerando n.º 77.

[191] Cf. RGPD, Considerando n.º 81.

tratamento dos dados no que diz respeito aos direitos e às liberdades das pessoas singulares"[192]. Note-se o incentivo que o legislador transmite para a elaboração de códigos de conduta.

O papel fiscalizador das autoridades de controlo tem uma relevância significativa para que o cumprimento do RGPD seja efetivo. Como consta no RGPD, "*a fim de comprovar a observância do presente regulamento, o responsável pelo tratamento ou o subcontratante deverá conservar registos de atividades de tratamento sob a sua responsabilidade. Os responsáveis pelo tratamento e subcontratantes deverão ser obrigados a cooperar com a autoridade de controlo e a facultar-lhe esses registos, a pedido, para fiscalização dessas operações de tratamento*"[193].

Uma das preocupações dos responsáveis pelo tratamento de dados, e dos subcontratantes, consistirá na preservação da segurança dos dados com o objetivo de evitar a violação do estabelecido no RGPD. Assim, o recurso à criptografia afigura-se como uma das medidas sugeridas pelo legislador. Lê-se no RGPD que, "*a fim de preservar a segurança e evitar o tratamento em violação do presente regulamento, o responsável pelo tratamento, ou o subcontratante, deverá avaliar os riscos que o tratamento implica e aplicar medidas que os atenuem, como a cifragem*"[194].

No âmbito do tratamento de dados através da videovigilância, a cifragem dos dados revela-se de grande importância, atendendo aos riscos que estão em causa não só pelo recurso a gravadores de vídeo, como ainda pela possibilidade de transmissão de imagens pela internet. Relembremos que a tecnologia não tem cessado de evoluir neste campo, possibilitando, entre outros aspetos, no contexto laboral, o controlo do trabalhador à distância.

Ainda quanto aos riscos que envolvem o tratamento de dados pessoais, o RGPD disponibiliza alguns exemplos e consequências, "*tais como a destruição, perda e alteração acidentais ou ilícitas, e a divulgação ou o acesso não autorizados a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento, riscos esses que podem dar azo, em particular, a danos físicos, materiais ou imateriais*"[195].

No âmbito da videovigilância, numa primeira análise, os danos mais prováveis serão imateriais. Porém, pegando no exemplo de acesso não autorizado aos dados pessoais recolhidos, onde seja erradamente identificada uma pessoa singular a cometer um alegado ato ilícito, tanto os danos físicos como os materiais podem surgir. Seja por vingança, chantagem ou por outra qualquer razão, imagens de videovigilância em mãos erradas podem implicar, inclusivamente, a perda de vidas.

Estando em causa os direitos e liberdades das pessoas singulares, sempre que o risco de determinada operação de tratamento de dados seja suscetível de ser considerado elevado, o responsável pelo

[192] Cf. RGPD, Considerando n.º 98.

[193] Cf. RGPD, Considerando n.º 82.

[194] Cf. RGPD, Considerando n.º 83.

[195] Cf. RGPD, Considerando n.º 83.

tratamento deverá encarregar-se da realização de uma avaliação de impacto da proteção de dados. Esta terá como fim a "*determinação, nomeadamente, da origem, natureza, particularidade e gravidade desse risco. Os resultados dessa avaliação deverão ser tidos em conta na determinação das medidas que deverão ser tomadas a fim de comprovar que o tratamento de dados pessoais está em conformidade com o presente regulamento. Sempre que a avaliação de impacto sobre a proteção de dados indicar que o tratamento apresenta um elevado risco que o responsável pelo tratamento não poderá atenuar através de medidas adequadas, atendendo à tecnologia disponível e aos custos de aplicação, será necessário consultar a autoridade de controlo antes de se proceder ao tratamento de dados pessoais*"[196].

De acordo com a Diretiva 95/46/CE e tento em conta o estabelecido no regime jurídico português[197], como já acima foi salientado[198], é obrigatória a notificação do tratamento de dados pessoais à CNPD. No entanto, de acordo com o estabelecido no RGPD, "*além de esta obrigação originar encargos administrativos e financeiros, nem sempre contribuiu para a melhoria da proteção dos dados pessoais. Tais obrigações gerais e indiscriminadas de notificação deverão, por isso, ser suprimidas e substituídas por regras e procedimentos eficazes mais centrados nos tipos de operações de tratamento suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, devido à sua natureza, âmbito, contexto e finalidades*"[199].

Pela citação anterior, verifica-se uma notável alteração de paradigma. Assim, deixarão de existir notificações obrigatórias e passarão a ser necessárias regras e procedimentos eficazes. Ou seja, deixa de existir uma hétero-regulação, através da autoridade de controlo, vigorando a autorregulação a partir de 25 de maio de 2018, data a partir da qual o RGPD passa a ser aplicável[200].

As entidades públicas e privadas terão, efetivamente, de avaliar detalhadamente cada operação de tratamento de dados pessoais. Por conseguinte, no contexto laboral, as operações que envolvam sistemas de videovigilância passam a ter de ser encaradas de forma diferente do que têm sido. Com toda a certeza, em cada entidade, novas regras e procedimentos terão de ser definidos de modo a não ficarem sujeitas à condição de incumprimento com o RGPD.

No âmbito da realização de avaliações de impacto, caso seja solicitado, o subcontratante deverá prestar assistência ao responsável. Veja-se o referido no RGPD: "*o subcontratante deverá prestar assistência ao responsável pelo tratamento, se necessário e a pedido deste, para assegurar o cumprimento das*

[196] Cf. RGPD, Considerando n.º 84.

[197] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 67/98 de 26 de Outubro*, 1ª série - A, nº 247, 26 de outubro de 1998, p. 5543.

[198] Veja-se supra, subcapítulo 3.2.

[199] Cf. RGPD, Considerando n.º 89.

[200] Cf. RGPD, Artigo n.º 99.

obrigações decorrentes da realização de avaliações do impacto sobre a proteção de dados e da consulta prévia à autoridade de controlo"[201].

Efetivamente, grande parte das instalações de sistemas de videovigilância é realizada por entidades sujeitas ao designado «registo prévio», assim consideradas no âmbito do exercício da atividade de segurança privada[202]. Entende-se serem estas entidades consideradas subcontratantes, visto que procedem ao estudo e conceção, instalação, manutenção e/ou assistência técnica de material e equipamento de segurança, nomeadamente de sistemas de videovigilância. Ou seja, estas entidades ver-se-ão obrigadas a ter um conhecimento aprofundado em matéria de proteção de dados, de modo a responder às solicitações do responsável do tratamento.

No entanto, constata-se um significativo amadorismo por parte destes operadores. Como consta do *Relatório Anual de Segurança Privada* (RASP) de 2015, verifica-se "*um grande desconhecimento da necessidade de Registo Prévio por parte destes operadores, o qual eventualmente decorre do exercício complementar e não exclusivo desta atividade. De facto, apesar das inerentes dificuldades de fiscalização, decorrentes do seu exercício no espaço privado, têm sido denunciadas e apuradas múltiplas situações de operadores que exercem a atividade de forma irregular. Estas situações irregulares são motivo de maior preocupação quando se verifica que, paralelamente à instalação dos sistemas de segurança, estes operadores asseguram serviços exclusivos de entidades titulares de alvará C, aproveitando o desconhecimento dos particulares no que ao licenciamento da atividade de segurança privada diz respeito*"[203].

Veja-se o que implica o desconhecimento de quem contrata estes operadores. Sem dúvida, a preocupação assinalada na citação anterior irá ser ainda mais significativa com a aplicação do RGPD. De igual modo, neste género de situações, a existência de um DPO, seja internamente ou através de prestação de serviço externo, será uma mais-valia para o responsável pelo tratamento de dados.

Face ao exposto, considera-se ser o momento adequado para a elaboração de um projeto de código de conduta para aplicação em território português, focado no contexto laboral, a ser cumprido pelos responsáveis pelo tratamento de dados e respetivos subcontratantes, no âmbito do recurso a sistemas de videovigilância. Recordemos que a adesão a este veículo pode ser considerada, senão em todo mas em parte, como condição de conformidade com o RGPD.

---

[201] Cf. RGPD, Considerando n.º 95.

[202] Cf. DIÁRIO DA REPÚBLICA, *Lei nº 34/2013 de 16 de maio*, 1ª série - nº 94, 16 de maio de 2013, nº 3 do artigo 12º.

[203] Cf. PORTUGAL, *Relatório Anual de Segurança Privada 2015*, in: http://www.psp.pt/SP_CONSELHO_SEGURANCA/RASP_2015.pdf, consultado em outubro de 2016.

12. CÓDIGO DE CONDUTA PARA EFEITOS DE TRATAMENTO DE DADOS NO ÂMBITO DA VIDEOVIGILÂNCIA EM CONTEXTO LABORAL E EM CUMPRIMENTO COM O RGPD

12.1. ENQUADRAMENTO

A reflexão a que doravante nos dedicamos prende-se com o futuro das relações laborais em Portugal, face ao novo RGPD e, especificamente, nas instalações de entidades públicas e privadas onde a videovigilância esteja presente.

Tendo o objetivo de tornar mais acessível, de forma organizada, com linguagem clara, as principais regras estabelecidas pelo RGPD acerca do recurso a sistemas de videovigilância, entende-se ser o momento ideal para elaborar um projeto de código de conduta.

Com efeito, a elaboração de códigos de conduta já era sugerida na Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995[204]. Hodiernamente, o recurso a este elemento é mesmo incentivado em vários momentos do RGPD. Vejam-se as seguintes referências:

1) Relativamente à responsabilidade do responsável pelo tratamento, o RGPD refere que "*o cumprimento de códigos de conduta aprovados conforme referido no artigo 40.º ou de procedimentos de certificação aprovados conforme referido no artigo 42.º pode ser utilizada como elemento para demonstrar o cumprimento das obrigações do responsável pelo tratamento*"[205].
2) No que respeita ao subcontratante, o RGPD refere que "*o facto de o subcontratante cumprir um código de conduta aprovado conforme referido no artigo 40.º ou um procedimento de certificação aprovado conforme referido no artigo 42.º pode ser utilizado como elemento para demonstrar as garantias suficientes a que se referem os n.º 1 e 4 do presente artigo*"[206].
3) Quanto à segurança do tratamento, o RGPD afirma que "*o cumprimento de um código de conduta aprovado conforme referido no artigo 40.º ou de um procedimento de certificação aprovado conforme referido no artigo 42.º pode ser utilizado como elemento para demonstrar o cumprimento das obrigações estabelecidas no n.º 1 do presente artigo*"[207].
4) A respeito da avaliação de impacto sobre a proteção de dados, o RGPD declara que, "*ao avaliar o impacto das operações de tratamento efetuadas pelos responsáveis pelo tratamento ou pelos*

[204] Cf. UNIÃO EUROPEIA, *Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*, in: http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT, consultado em abril 2016.

[205] Cf. RGPD, Artigo n.º 24.

[206] Cf. RGPD, Artigo n.º 28.

[207] Cf. RGPD, Artigo n.º 32.

subcontratantes, em especial para efeitos de uma avaliação de impacto sobre a proteção de dados, é tido na devida conta o cumprimento dos códigos de conduta aprovados a que se refere o artigo 40.º por parte desses responsáveis ou subcontratantes"[208].

Das citações anteriores, conclui-se que o cumprimento de um código de conduta aprovado pode constituir um elemento relevante, tanto para os responsáveis pelo tratamento como para os subcontratantes, objetivando o cumprimento do RGPD.

Se não existissem outras razões, valeria aquela que muitas vezes preocupa os responsáveis dos tratamentos e os subcontratantes: a aplicação de sanções por infrações ao RGPD. Veja-se que, conforme estabelecido no RGPD, em caso de infração menor, o cumprimento de um código de conduta pelo responsável pelo tratamento ou pelo subcontratante será considerado de grande valor na medida em que pode servir de atenuante aquando da imposição de sanções pelas autoridades de controlo[209]. Ou seja, onde ocorra um tratamento de dados no âmbito da videovigilância e em contexto laboral, caso exista uma infração menor mas esteja a ser cumprido o código de conduta específico do tratamento em causa, será este cumprimento um fator válido para atenuar as sanções a impor pela autoridade de controlo.

São, com efeito, dados exemplos de regras no artigo 40º do RGPD. Assim, tendo presente as sugestões apontadas no RGPD para inclusão num código de conduta, propõem-se mais à frente as bases consideradas imprescindíveis e que não deverão faltar num projeto de código de conduta para o tratamento de dados em contexto laboral através da utilização de sistemas de videovigilância.

12.2. MEDIDAS PARA CUMPRIMENTO DO RGPD

A CNPD publicou, em Janeiro de 2017, um conjunto de dez medidas com o objetivo de auxiliar as entidades públicas e privadas na preparação da aplicação do RGPD[210]. Para aplicação no projeto de código de conduta de que nos ocupamos, vejam-se as dez medidas apresentadas, as quais têm por título e poderão ser resumidas da seguinte forma:

1. INFORMAÇÃO AOS TITULARES DOS DADOS

   O RGPD obriga a prestar mais informações ao titular dos dados do que atualmente, designadamente a base legal para o tratamento de dados, o prazo de conservação dos dados, informações mais detalhadas sobre as transferências internacionais e a possibilidade de apresentação de queixa junto da CNPD.

[208] Cf. RGPD, Artigo n.º 35.

[209] Cf. RGPD, Considerando.

[210] Cf. CNPD, *10 Medidas Para Preparar a Aplicação do Regulamento Europeu de Proteção de Dados*, in: https://www.cnpd.pt/bin/rgpd/10_Medidas_para_preparar_RGPD_CNPD.pdf, consultado em janeiro de 2017.

Para além disso, deve ser realizada a revisão de políticas de privacidade e de todos os textos que prestem informação aos titulares dos dados, ao mesmo tempo que deve ser verificado se é fornecida, em todas as situações, a informação exigida por lei.

2. EXERCÍCIO DOS DIREITOS DOS TITULARES DOS DADOS

Rever os procedimentos internos de garantia do exercício dos direitos dos titulares dos dados, em especial, quanto aos prazos máximos de resposta. Os direitos dos titulares foram alargados em relação à atual lei, passando a existir o direito à limitação do tratamento e o direito à portabilidade, bem como novos requisitos quanto ao direito à eliminação dos dados. São necessários procedimentos eficazes de comunicação com as entidades terceiras a quem se transmitiu os dados, de modo a assegurar o exercício efetivo dos direitos. Por se tratar de direitos fundamentais dos cidadãos, esta é uma área de intervenção essencial.

3. CONSENTIMENTO DOS TITULARES DOS DADOS

Verificar a forma e circunstâncias em que foi obtido o consentimento dos titulares, quando este serve de base legal para o tratamento de dados pessoais. É necessário apurar se o consentimento obtido pelo responsável pelo tratamento respeita todas as novas exigências.

4. DADOS SENSÍVEIS

Deve ser analisado o contexto e a escala destes tratamentos de dados para verificar se daí decorrem obrigações particulares, tais como a designação de um encarregado de proteção de dados.

5. DOCUMENTAÇÃO E REGISTO DE ATIVIDADES DE TRATAMENTO

Documentar de forma detalhada todas as atividades relacionadas com o tratamento de dados pessoais, tanto as que resultam diretamente da obrigação de manter um registo como as relativas a outros procedimentos internos, de modo a que a organização esteja apta a demonstrar o cumprimento de todas as obrigações decorrentes do RGPD. O Regulamento prevê que as entidades em regime de subcontratação, designadas de «subcontratantes», passem a ter quase as mesmas obrigações que os responsáveis pelos tratamentos, estando de igual modo obrigadas a provar que cumprem tudo o que lhes é exigido, a prossecução desta medida de forma atempada é vital, pois terão de começar do zero.

6. CONTRATOS DE SUBCONTRATAÇÃO

Rever os contratos de subcontratação de serviços realizados no âmbito de tratamentos de dados pessoais para verificar se contêm todos os elementos exigidos pelo Regulamento. O RGPD veio especificar o conteúdo dos contratos de subcontratação, impondo a introdução de

um vasto conjunto de informações. Quando houver lugar a sub-subcontratação, compete ao subcontratante verificar se detém as autorizações respetivas dos responsáveis pelo tratamento, exigidas expressamente pelo novo Regulamento.

7. ENCARREGADO DE PROTEÇÃO DE DADOS

Antes de mais, este elemento poderá desempenhar um papel fulcral neste período de transição para garantir que a organização cumpre todas as obrigações legais desde o início da aplicação do Regulamento. No RGPD foi ainda estabelecida a obrigação de designar um encarregado de proteção de dados, em determinadas circunstâncias, como seja o caso das entidades públicas. O responsável pelo tratamento e o subcontratante podem sempre, mesmo não se encontrando no momento em nenhuma das circunstâncias exigíveis, decidir ter um encarregado de proteção de dados. São evidentes as vantagens que tal pode significar para o nível de cumprimento das obrigações.

8. MEDIDAS TÉCNICAS E ORGANIZATIVAS E SEGURANÇA DO TRATAMENTO

Terão de ser revistas as políticas e práticas da organização à luz das novas obrigações do regulamento, como ainda, assegurar e poder comprovar que todos os tratamentos de dados efetuados estão em conformidade com o RGPD a partir do momento da sua aplicação.

9. PROTEÇÃO DE DADOS DESDE A CONCEÇÃO E AVALIAÇÃO DE IMPACTO

Há que tomar as medidas necessárias para confirmar um nível de segurança do tratamento adequado que previna a destruição, perda e alterações acidentais ou ilícitas ou, ainda, a divulgação ou acesso não autorizados de dados. Aplicar com eficácia os princípios da proteção de dados desde a conceção e por defeito. Devem ser tidas em devida conta as características do tratamento e os efeitos que este pode ter nos direitos dos cidadãos; se for suscetível de resultar num elevado risco, deve realizar uma avaliação de impacto sobre a proteção de dados, de modo a adotar as medidas adequadas para mitigar os riscos.

10. NOTIFICAÇÃO DE VIOLAÇÕES DE SEGURANÇA

Devem ser adotados procedimentos internos e ao nível da subcontratação, se for o caso, para lidar com casos de violações de dados pessoais, designadamente na deteção, identificação e investigação das circunstâncias, medidas mitigadoras, circuitos da informação entre responsável e subcontratante, envolvimento do encarregado de proteção de dados e notificação à CNPD, atendendo aos prazos prescritos no Regulamento. Notificar aquelas que sejam suscetíveis de resultar num risco para os direitos dos titulares. Todavia, todas as violações devem ser devidamente documentadas conforme preceituado no Regulamento. Nalguns casos, em que possa resultar um elevado risco para os titulares, é exigido que estes

sejam notificados, pelo que deve ser analisado desde logo o tipo de tratamentos de dados realizados e o potencial risco que pode ocorrer em caso de uma violação de segurança.

Este conjunto de medidas sugeridas pela CNPD enquadra-se com o referido no RGPD: "*as atividades de sensibilização das autoridades de controlo dirigidas ao público deverão incluir medidas específicas a favor dos responsáveis pelo tratamento e subcontratantes, incluindo as micro, pequenas e médias empresas, bem como as pessoas singulares, em particular num contexto educacional*"[211]. No entanto, possivelmente devido à manifesta falta de recursos humanos por parte da autoridade de controlo portuguesa para tão grande e nobre missão a nível nacional e internacional, não se conhecem até ao momento outras publicações, ou orientações, com medidas específicas que visem auxiliar os responsáveis pelo tratamento e subcontratantes a cumprir o estabelecido no RGPD.

Com base nestas medidas propostas pela CNPD, para além das suas deliberações, autorizações de tratamento de dados pessoais resultantes de videovigilância e jurisprudência, entre outras fontes consultadas e referidas neste texto, apresenta-se, seguidamente, uma proposta de projeto de código de conduta, pretendendo-se desta forma contribuir para a criação de um código de conduta para operações de tratamento de dados efetuadas no âmbito da utilização de sistemas de videovigilância em contexto laboral.

12.3. PROJETO DE CÓDIGO DE CONDUTA

PREÂMBULO

A evolução tecnológica implica novos e constantes desafios quanto ao tratamento de dados, em particular, no que concerne às relações laborais.

O Regulamento Geral sobre a Proteção de Dados (RGPD), aplicável em todos os Estados-Membros da União Europeia (UE), a partir de 25 de maio de 2018, constitui a principal referência do presente Código.

As entidades públicas e privadas que recorram ao tratamento de dados pessoais, no âmbito da utilização de sistemas de videovigilância em contexto laboral, vinculam-se, por sua livre vontade, ao presente Código.

Face ao ordenamento jurídico nacional, o presente Código refere-se às operações de tratamento de dados efetuadas no âmbito da utilização de sistemas de videovigilância em contexto laboral, sendo este aplicável a todo o território português.

[211] Cf. RGPD, Considerando n.º 132.

Artigo 1.º

Âmbito da aplicação

O presente Código aplica-se aos dados obtidos no âmbito da utilização de sistemas de videovigilância em contexto laboral, sendo estes considerados parte do conceito de vida privada.

Artigo 2.º

Enquadramento legal

O presente Código respeita o definido no 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 (Regulamento Geral sobre a Proteção de Dados).

O presente Código respeita de igual modo o definido no ordenamento jurídico português, em particular a Constituição da República Portuguesa e o que concerne ao estabelecido em matéria de legislação laboral.

Artigo 3.º

Princípio da transparência

Face ao regime de proteção de dados estabelecido no RGPD, o princípio da transparência tem de ser respeitado pelo responsável pelo tratamento de dados pessoais.

O responsável pelo tratamento de dados no âmbito da utilização de sistemas de videovigilância, nomeadamente em contexto laboral, obriga-se a garantir que o tratamento em causa seja realizado de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias do titular dos dados, ou seja, do trabalhador.

O facto deste Código se aplicar ao tratamento de dados no âmbito da utilização de sistemas de videovigilância em contexto laboral implica que o responsável pelo tratamento dos dados seja a entidade empregadora ou o organismo de emprego público, sendo estes a determinar as finalidades e os meios do tratamento.

Cabe ao responsável pelo tratamento tomar as medidas necessárias, inclusivamente por via contratual junto da entidade subcontratada, de modo a garantir que os dados obtidos através da utilização de sistemas de videovigilância em contexto laboral não sejam utilizados para nenhuma outra finalidade.

Artigo 4.º

Definição de regras

As entidades públicas e privadas que recorram à utilização de sistemas de videovigilância em contexto laboral obrigam-se a definir regras para que as finalidades do tratamento sejam previamente determinadas, explícitas e legítimas.

Quando exista comissão de trabalhadores, o responsável pelo tratamento obriga-se a consultar previamente o parecer sobre o recurso à utilização de sistemas de videovigilância em contexto laboral.

Artigo 5.º

Finalidades do tratamento

São apenas admitidos os tratamentos de dados relativos à videovigilância em contexto laboral com a finalidade de proteção de pessoas e bens. Excluem-se os casos, sujeitos a autorização prévia da autoridade de controlo, em que exista necessidade legítima de controlo de postos de trabalho que apresentem especiais riscos para os trabalhadores, quer pela sua especial perigosidade em relação ao manuseamento de certas substâncias perigosas, quer pela inacessibilidade ou especial solidão em que os trabalhadores exercem a sua atividade (vg. minas, centrais nucleares, laboratórios em que sejam manuseados produtos químicos perigosos).

O responsável pelo tratamento de dados obriga-se a dar conhecimento da finalidade do tratamento de dados com recursos a sistemas de videovigilância em contexto laboral, prazo de conservação dos dados, direitos dos titulares, forma de exercício dos direitos, incluindo a possibilidade e modo de apresentação de queixa junto da autoridade de controlo, bem como facultar outros esclarecimentos que lhe sejam solicitados por parte dos trabalhadores.

Artigo 6.º

Proibição de controlo do desempenho profissional

Os dados obtidos através da utilização de sistemas de videovigilância em contexto laboral não podem ser usados pelo responsável pelo tratamento ou por entidades subcontratadas para controlar o desempenho profissional do trabalhador, conforme disposto no n.º 1 do artigo 20º do Código do Trabalho (CT), pelo que essa não é uma finalidade legítima. Por essa razão, os dados pessoais, mesmo que recolhidos para outras finalidades legítimas, não podem ser utilizados direta ou indiretamente para a avaliação do desempenho do trabalhador.

Artigo 7.º

Acesso restrito aos dados

O responsável pelo tratamento de dados obriga-se a encontrar uma solução técnica – junto do subcontratante do serviço de videovigilância ou dentro da própria entidade empregadora, caso não exista entidade subcontratada – em que o registo dos dados de videovigilância fique selado, impedindo o acesso fácil, e o registo só será aberto em caso de eventual participação criminal, quando da ocorrência de ato ilícito no espaço legalmente abrangido pelo visionamento das câmaras.

Artigo 8.º

Acesso remoto

Nos casos previstos no ordenamento jurídico nacional em que exista a necessidade de acesso remoto às imagens de videovigilância em tempo real, recorrendo a diferentes tipos de dispositivos, como sejam os casos de *smartphones*, computadores ou *tablets*, o responsável pelo tratamento dos dados obriga-se a proteger a informação através de autenticação forte do utilizador para aceder ao sistema de videovigilância, com limitação do número de tentativas, recorrendo a métodos adequados de encriptação, os quais minimizem os riscos de acesso por terceiros não autorizados, em caso de perda ou furto dos dispositivos.

As entidades públicas e privadas obrigam-se a criar e cumprir políticas rigorosas de segurança da informação, tendo em conta que a saída de informação do espaço físico do responsável pelo tratamento em causa através do acesso remoto aos dados, com recurso à Internet, implica sempre um risco acrescido.

Artigo 9.º

Manutenção de registo de operações de tratamento

Caso seja necessário aceder aos dados obtidos através da utilização de sistemas de videovigilância em contexto laboral, eventualmente para satisfação do exercício do direito de acesso por parte dos titulares, as entidades públicas e privadas obrigam-se a criar e manter um registo, através de *logs*, que identifiquem quem, quando, respetiva data e hora (*timestamp*) e a que dados acedeu, sendo essas operações efetuadas atribuindo um número sequencial (id) a cada ocorrência e um campo de *hash* aplicado sobre os elementos anteriores (id, utilizador, data, hora e operação).

De forma a permitir a validade legal, os *logs* têm de estar assinados digitalmente. O responsável pelo tratamento de dados obriga-se a implementar uma política de análise de *logs*, com a realização de relatórios periódicos de análise, os quais terão de ser mantidos pelo responsável pelo tratamento de dados ou por entidades subcontratadas, para efeitos de fiscalização pela autoridade de controlo.

Para conservação dos *logs* anteriormente referidos, estabelece-se o prazo de 120 dias.

Artigo 10.º

Princípio da minimização dos dados

As entidades públicas e privadas que recorram à utilização de sistemas de videovigilância em contexto laboral obrigam-se a tomar medidas para que o tratamento de dados seja reduzido ao mínimo indispensável ao cumprimento da respetiva finalidade.

Artigo 11.º

Formação sobre proteção de dados pessoais

As entidades públicas e privadas obrigam-se a promover a formação inicial e revisão anual, com duração mínima de 4 (quatro) horas, no campo da proteção de dados pessoais, com avaliação que terá de ser obrigatoriamente positiva, aos trabalhadores que tenham ou possam vir a ter contacto com dados obtidos através da utilização de sistemas de videovigilância em contexto laboral.

As entidades subcontratadas, caso existam, cumprem na íntegra o disposto no parágrafo anterior.

Artigo 12.º

Prazo de conservação dos dados

O prazo máximo para a conservação de dados obtidos através da utilização de sistemas de videovigilância em contexto laboral é de 30 dias contados desde a respetiva captação, salvo as exceções previstas no ordenamento jurídico português.

O responsável pelo tratamento obriga-se a tomar medidas para assegurar que os dados são destruídos de imediato findo o prazo de conservação respetivo (dando indicações precisas nesse sentido à entidade subcontratada quando esta processa a informação), providenciando, devido ao curto período de armazenamento da informação, a introdução de um sistema de eliminação automática que garanta a observância do prazo máximo. A destruição dos dados tem de ser documentada através de *logs*.

Artigo 13.º

Entidade subcontratada

Caso exista necessidade de recorrer a uma entidade subcontratada, no momento da seleção, o responsável pelo tratamento pondera sobre a qualidade do subcontratado que fique encarregue de tratar os dados pessoais decorrentes da utilização de sistemas de videovigilância em contexto laboral, obrigando-se a estabelecer, contratualmente, a forma de não colocar em causa as garantias dos trabalhadores contempladas no CT.

O responsável pelo tratamento terá de dar instruções muito precisas à entidade subcontratada e encontrar soluções concretas que permitam proceder ao tratamento de dados de acordo com presente Código.

Nesse sentido, atendendo ainda à partilha de responsabilidades em caso de incumprimento do RGPD, a entidade subcontratada obriga-se, de forma contratual, ao cumprimento do presente Código.

Artigo 14.º

Permissão de acesso aos dados

Caso o processamento dos dados obtidos através da utilização de sistemas de videovigilância em contexto laboral seja realizado internamente, este não poderá ser efetuado pelo departamento de recursos humanos do responsável pelo tratamento, atendendo à possibilidade de comprometer a proibição de controlo do desempenho profissional do trabalhador através de meio de vigilância à distância (cf. disposto no n.º 1 do artigo 20º do CT).

A escolha e indicação expressa do(s) funcionário(s) autorizado(s) pelo responsável pelo tratamento que tenha(m) acesso aos dados obtidos através da utilização de sistemas de videovigilância em contexto laboral apenas e só no caso de necessidade de satisfação do direito de acesso aos dados de um titular deverá recair sobre o responsável pela área de segurança, não podendo este(s) dar conhecimento dos dados a que tenha(m) acesso.

O responsável pelo tratamento promove medidas organizacionais para o efeito e emite orientações claras sobre esta matéria ao pessoal envolvido.

Artigo 15.º

Violação de dados

Caso ocorra uma violação dos dados obtidos através da utilização de sistemas de videovigilância em contexto laboral, logo que o responsável pelo tratamento tenha conhecimento de uma violação desses dados pessoais deverá notificá-la à autoridade de controlo, sem demora injustificada e, sempre que possível, no prazo de 72 horas após ter tido conhecimento do ocorrido, a menos que seja capaz de demonstrar, em conformidade com o princípio da responsabilidade, que essa violação não é suscetível de implicar um risco para os direitos e liberdades das pessoas singulares. Se não for possível efetuar essa notificação no prazo de 72 horas, a notificação deverá ser acompanhada dos motivos do atraso, podendo as informações ser fornecidas por fases sem demora injustificada.

O responsável pelo tratamento de dados obtidos através da utilização de sistemas de videovigilância em contexto laboral obriga-se a manter registados os incidentes de violação de dados pessoais.

Artigo 16.º

Obrigações específicas do responsável

O responsável pelo tratamento de dados com recursos a sistemas de videovigilância em contexto laboral obriga-se a cumprir o seguinte:

A. Não proceder à recolha de som, salvo em situações previstas no ordenamento jurídico português;
B. Definir a localização das câmaras, os ângulos utilizados e as modalidades de registo de imagens;
C. Reduzir o campo visual em função da finalidade prosseguida;
D. Dispensar grandes planos ou detalhes não relevantes;
E. Não instalar câmaras de videovigilância desproporcionadamente, restringindo ao mínimo a sua quantidade;
F. Manter sempre atualizadas a data e hora das gravações;
G. Limitar as zonas abrangidas pelos sistemas de videovigilância, de acordo com as especificidades de cada entidade pública ou privada, aos seguintes locais:

1) Pontos de acesso a partir do exterior;
2) Cofres;
3) Sala de contagem de valores;
4) Hall e/ou acesso a elevadores;
5) Parque de estacionamento;
6) Zonas comuns (edifícios de habitação/condomínios);
7) Zona de ATM's;
8) Zonas internas de circulação;
9) Área de venda;
10) Balcão de atendimento ao público;
11) Caixas de pagamento;
12) Zona de exposição de produtos;
13) Armazém;
14) Oficinas;
15) Máquinas de *Vending*;
16) Zonas técnicas e/ou frigoríficas;
17) Área de fabrico;
18) Salas de jogos (casino/bingo);
19) Pistas de dança (estabelecimentos destinados a dança);
20) Bengaleiro;
21) Receção;
22) Área de conferência de fármacos (farmácias/parafarmácias e similares);
23) Laboratório (farmácias/parafarmácias e similares);
24) Atendimento noturno ao público (farmácias);
25) Acesso a quartos das especialidades infantis (estabelecimentos de saúde);
26) Pontos de acesso a divisões interiores (estabelecimentos de saúde);
27) Farmácias (estabelecimentos de saúde);
28) Zonas internas de circulação em lares e outros estabelecimentos de apoio social (exceto corredores de acesso aos quartos);

29) Ilhas de abastecimento (gasolineiras);
30) Área comercial da loja (gasolineiras);
31) Área de lavagem automóvel (gasolineiras);
32) Montras (exibição, compra e venda de artigos com metais preciosos);
33) Área do espetáculo desportivo (recintos desportivos);
34) Zonas comerciais (recintos desportivos);
35) Anel ou perímetro de segurança (recintos desportivos);
36) *Takeaway* exterior (restauração);
37) Zona de fornos (restauração);
38) Zona de balança/báscula (sucateiras);
39) Parque de resíduos (sucateiras);

H. No momento da instalação das câmaras e com revisão periódica trimestral, documentar e manter registo, nomeadamente através de *printscreen*, de modo a confirmar que as imagens obtidas respeitam os seguintes itens:

1) Não incidem regularmente sobre os trabalhadores durante a atividade laboral;
2) Não incluem recolha de som;
3) Limitam-se à propriedade do responsável;
4) Não abrangem imagens da via pública ou de propriedades limítrofes;
5) Não captam a digitação dos códigos em terminais de pagamento ATM;
6) Não são recolhidas imagens no interior de local de culto (igrejas);
7) Não abrangem imagens de acesso ou interior de instalações sanitárias;
8) Não abrangem imagens de acesso e interiores de vestiários ou outras áreas destinadas aos trabalhadores;
9) Não abrangem imagens do interior de elevadores;
10) Não abrangem imagens de piscinas e imediações;
11) Não abrangem imagens de *lobbies* (hotéis e outros estabelecimentos de hotelaria);
12) Não abrangem imagens de jardins (hotéis e outros estabelecimentos de hotelaria);
13) Não abrangem imagens de acessos e interior dos quartos e interior de bares e restaurantes (hotéis e outros estabelecimentos de hotelaria);
14) Não abrangem imagens de local destinado ao entretenimento de crianças (p.e. *play centers*).

Os elementos anteriormente referidos são obrigatoriamente transmitidos aos trabalhadores e aos contratados.

Artigo 17.º

Exercício de direitos dos titulares

Caso seja solicitado o exercício do direito de acesso aos dados pessoais por parte de um titular dos dados recolhidos no âmbito do tratamento de dados com recursos a sistemas de videovigilância em contexto laboral, antes de corresponder ao solicitado, o responsável do tratamento em causa obriga-se a tomar as medidas técnicas necessárias para ocultar/anonimizar as imagens de terceiros.

Artigo 18.º

Interconexões

O responsável pelo tratamento de dados obtidos através da utilização de sistemas de videovigilância em contexto laboral obriga-se a tomar medidas para assegurar que não existe recurso a interconexões com outros tratamentos de dados, em particular da responsabilidade do mesmo empregador, como sejam as bases de dados de recursos humanos.

Artigo 19.º

Auditorias

O responsável pelo tratamento de dados obtidos através da utilização de sistemas de videovigilância em contexto laboral obriga-se a garantir um acesso restrito, tanto físico como lógico, aos servidores do sistema, os quais devem manter um registo de acesso à informação, bem como registos da transmissão de dados, para controlo das operações e para a realização de auditorias internas e externas.

Para efeitos de auditoria, os requisitos expostos no parágrafo anterior serão sempre avaliados com vista à verificação da condição efetiva de proteção de dados da entidade em causa.

Artigo 20.º

Avaliação de impacto sobre a proteção de dados

As entidades públicas e privadas que pretendam recorrer à utilização de sistemas de videovigilância em contexto laboral obrigam-se, previamente, a realizar uma avaliação de impacto da utilização das tecnologias na privacidade dos trabalhadores, em conformidade com o disposto no artigo 35º do RGPD e, posteriormente, recorrer aos meios mais adequados e menos intrusivos para alcançar os legítimos objetivos.

Artigo 21.º

Comunicação das imagens

As imagens só podem ser transmitidas nos termos da lei processual penal. Detetada a eventual infração penal, o responsável pelo tratamento de dados obtidos através da utilização de sistemas de

videovigilância em contexto laboral deverá, juntamente com a participação, enviar à autoridade judiciária ou ao órgão de polícia criminal competentes as imagens recolhidas.

Noutras situações em que as autoridades solicitem acesso às imagens, tal só poderá ocorrer, no âmbito de processo judicial devidamente identificado, em cumprimento de despacho fundamentado da autoridade judiciária competente.

Fora destas condições não pode o responsável comunicar as imagens.

Artigo 22.º

Sinalização obrigatória

Para todos os responsáveis pelo tratamento de dados obtidos através da utilização de sistemas de videovigilância em contexto laboral, é obrigatória a afixação, em locais bem visíveis, de avisos informativos da existência de videovigilância, com os requisitos e especificações técnicas da sinalização e as suas dimensões nos mesmos termos do disposto no artigo 115º da Portaria n.º 273/2013, de 20 de agosto, e em conformidade com o respetivo anexo VIII, recorrendo à seguinte simbologia:

Os avisos são colocados no perímetro exterior do local ou zona objeto de vigilância com recurso a equipamentos eletrónicos de videovigilância por câmaras de vídeo, não ultrapassando estes avisos a altura de 2 (dois) metros em relação ao solo e da forma mais conveniente ao seu pronto reconhecimento pelos trabalhadores.

No interior do local ou zona objeto de vigilância, devem ser repetidos os avisos de informação, não ultrapassando estes avisos a altura de 2 (dois) metros em relação ao solo.

O responsável pelo tratamento de dados obtidos através da utilização de sistemas de videovigilância em contexto laboral tem a obrigação de afixar, em conjunto com a simbologia e nos termos definidos anteriormente, as seguintes informações:

a) a existência e localização das câmaras de vídeo;
b) a menção «Para sua proteção, este local é objeto de videovigilância»;

c) aaso exista, a entidade de segurança privada autorizada a operar o sistema, pela menção do nome e alvará ou licença;
d) o responsável pelo tratamento dos dados recolhidos perante quem os direitos de acesso e retificação podem ser exercidos.

12.4. NECESSIDADE DE LEGISLAÇÃO GERAL DE VIDEOVIGILÂNCIA

Apesar das regras previstas no RGPD, continua a denotar-se a necessidade de legislação específica no âmbito da videovigilância. Como já foi dito, falta publicar legislação geral de enquadramento sobre a utilização de sistemas de videovigilância.

A CNPD, como entidade de controlo, deixará, a partir de 25 de maio de 2018, de exercer um papel de controlo prévio, de forma geral, sobre os tratamentos de dados, face à data estabelecida para início de aplicabilidade do RGPD. No entanto, as autorizações de tratamento de dados continuam a ser válidas, desde que se adaptem às novas regras estabelecidas, conforme provado ao longo deste texto.

Relativamente ao tratamento de dados no âmbito da utilização de sistemas de videovigilância, caso houvesse dúvidas quanto à necessidade de legislação geral, com a aplicação do RGPD as dúvidas terminam. Ou seja, o legislador nacional português deverá produzir legislação no âmbito da videovigilância, a qual deverá, entre outros aspetos, definir o seguinte:

1. Âmbito da aplicação da legislação;
2. Finalidades admissíveis para o tratamento de dados obtidos através da utilização de sistemas de videovigilância;
3. Obrigação de avaliação de impacto sobre a proteção de dados pessoais;
4. Prazos de conservação de dados;
5. Princípios a respeitar pelos responsáveis e entidades subcontratadas;
6. Obrigatoriedade de frequência de ações periódicas anuais de formação em proteção de dados pessoais, com duração mínima de 4 (quatro) horas, para os responsáveis pelo tratamento;
7. Obrigatoriedade de frequência de ações periódicas anuais de formação em proteção de dados pessoais, com duração mínima de 4 (quatro) horas, para entidades subcontratadas que tenham intervenção no tratamento, nomeadamente, empresas de segurança privada e entidades sujeitas a registo prévio (instaladores de sistemas de segurança);
8. Forma de exercício dos vários direitos dos titulares dos dados;
9. Obrigatoriedade de sinalização igual à definida em legislação de segurança privada e no âmbito da informação da existência de sistemas de videovigilância;
10. Sanções dissuasoras, prevendo o agravamento das mesmas em caso de reincidência;
11. Obrigação de indeminização aos titulares dos dados em caso de violação de segurança;
12. Definição de limites quanto aos locais abrangidos pelas câmaras;
13. Definição de limites das zonas abrangidas pelos sistemas de videovigilância, de acordo com as especificidades de cada entidade pública ou privada;

14. Definição de zonas proibidas para abrangência das câmaras;
15. No momento da instalação das câmaras e com revisão periódica trimestral, documentar e manter registo, através de *printscreen* obtidos nos extremos dos campos abrangidos, a confirmar que as imagens obtidas não violam a legislação em vigor;
16. Definição de limites quanto às capacidades técnicas das câmaras, como seja a possibilidade de gravação de som;
17. Especificar as medidas de segurança obrigatórias a serem tomadas pelo responsável e por entidades subcontratadas;
18. Definir limites para o controlo remoto dos sistemas de videovigilância, em particular, quando em contexto laboral;
19. Definição de plataforma de apresentação de queixas por tratamentos ilícitos que garanta o anonimato do queixoso;
20. Obrigação de nomeação de um encarregado de proteção de dados, com as qualificações estabelecidas no «Regulamento Geral sobre a Proteção de Dados» ou, em alternativa, o recurso à contratação de serviços externos, com definição de número mínimo de horas a serem contratadas anualmente;
21. Manutenção de registo de operações de tratamento através de *logs*;
22. Proibição de interconexão de dados;
23. Definição de regras de cedência de imagens no âmbito de processo judicial.

CONCLUSÕES

A utilização ilícita de dados pessoais por terceiros pode implicar efeitos inimagináveis, com prejuízo para os titulares dos dados. Por essa razão, uma das conclusões a que se pode chegar, desde já, é a seguinte: os cidadãos necessitam de ser despertos para os seus direitos em matéria de proteção de dados pessoais. Aliás, ao longo deste trabalho foram apresentados alguns exemplos concretos dessa realidade.

Tal como o povo diz: quem não deve, não teme. Mas, como vimos, relativamente à videovigilância, mesmo os que nada devem, têm razões para temer.

Em Portugal, é notória a necessidade urgente de estabelecer um compromisso entre segurança e liberdade. Apesar dessa necessidade, a videovigilância terá sempre efeitos, embora benéficos, bastante limitados. No entanto, ficou provada a limitação de direitos fundamentais dos cidadãos quando sujeitos ao tratamento de dados através de sistemas de videovigilância. E aí já se perde parte da liberdade, sem garantia de segurança como retorno.

Com o foco nos direitos dos titulares de dados pessoais, o destaque que aqui foi dado quanto à utilização destes sistemas de videovigilância em contexto laboral resulta, por um lado, da legislação nacional portuguesa, em particular no que concerne à relação laboral, da Constituição da República Portuguesa, da jurisdição de tribunais superiores quanto à matéria em apreço e das orientações produzidas pela Comissão Nacional de Proteção de Dados. Por outro lado, foram tidos em conta os diversos documentos legislativos de nível europeu atinentes a direitos dos titulares de dados pessoais, dando-se substancial ênfase ao «Regulamento Geral sobre a Proteção de Dados».

Este documento legislativo, de cumprimento obrigatório por todos os Estados-Membros da União Europeia, já entrou em vigor e é aplicável a partir de 25 de maio de 2018. Por essa razão, o seu estudo, a ponderação dos vários aspetos que o envolvem, a interpretação obrigatória e a repercussão nos mais variados setores de atividade, resultaram em dois potenciais contributos que poderão ser reconhecidos por parte do Estado Português com vista à promoção da sensibilização dos cidadãos para os riscos, regras, garantias e direitos associados ao tratamento de dados pessoais.

O primeiro destes contributos consiste num projeto de código de conduta. Constatou-se a sua inexistência e a sua necessidade. Ou seja, provou-se que, no RGPD, é repetidamente sugerida a criação deste tipo de instrumento de modo a que os responsáveis pelo tratamento de dados e as entidades subcontratadas tenham a possibilidade de aderirem ao mesmo, demonstrando dessa forma a sua vontade em cumprir as novas regras estabelecidas.

Já o segundo contributo consiste na apresentação de um conjunto de itens considerados relevantes, os quais deverão ser incluídos em legislação nacional, face à inexistência de uma lei geral sobre a utilização de sistemas de videovigilância em Portugal.

Por fim, não pode deixar de ser dada nota quanto à falta de obrigação de formação específica, no âmbito do exercício da segurança privada, em matéria de proteção de dados pessoais, sabendo que são os vigilantes, funcionários das entidades subcontratadas pelo responsável pelo tratamento de dados, no âmbito da utilização de sistemas de videovigilância, a desempenhar um papel profissional de maior proximidade física e acesso às imagens recolhidas.

Em paralelo ao referido grupo, encontram-se as entidades sujeitas a registo prévio, no âmbito da legislação aplicável à atividade de segurança privada, as quais procedem ao estudo **e** conceção, instalação, manutenção ou assistência técnica de material e equipamento de segurança, como seja o caso dos sistemas de videovigilância. Naturalmente, em função das suas atividades, têm fácil acesso a dados pessoais registados nas imagens recolhidas, pelo que deverão ter formação adequada e obrigatória em matéria de proteção de dados pessoais.

Referências Bibliográficas

ABRANTES, José João, *Direitos Fundamentais da Pessoa Humana no Trabalho, em especial, a reserva da intimidade da vida privada (algumas questões)*, Coimbra: Livraria Almedina, 2014.

ANPC [Autoridade Nacional de Protecção Civil], *Guia de Apoio Técnico às Associações Humanitárias de Bombeiros*, in: http://www.prociv.pt/Documents/CT_24_www.pdf, consultado em janeiro de 2016.

CASTRO, Catarina Sarmento e, *Direito da Informática, Privacidade e Dados Pessoais*, Coimbra: Livraria Almedina, 2005.

CNPD [Comissão Nacional de Proteção de Dados], *10 Medidas Para Preparar a Aplicação do Regulamento Europeu de Proteção de Dados*, in: https://www.cnpd.pt/bin/rgpd/10_Medidas_para_preparar_RGPD_CNPD.pdf, consultado em janeiro de 2017.

CNPD, *Decisões da Comissão*, in: https://www.cnpd.pt/bin/decisoes/decisoes.asp?primeira_escolha=2015&segunda_escolha=10, consultado em janeiro de 2016.

CNPD, *Deliberação nº 61/2004 - Princípios Sobre o Tratamento de Dados por Videovigilância*, in: https://www.cnpd.pt/bin/orientacoes/DEL61-2004-VIDEOVIGILANCIA.pdf, consultado em janeiro de 2016.

CNPD, *História da CNPD*, in: https://www.cnpd.pt/bin/cnpd/historia.htm, consultado em janeiro de 2016.

CNPD, *Parecer n.º 22/2003*, in: https://www.cnpd.pt/bin/decisoes/Par/40_22_2003.pdf, consultado em janeiro de 2016.

CNPD, *Processo n.º 14968/ 2015 – Autorização N.º 9932/ 2015*, in: https://www.cnpd.pt/bin/decisoes/aut/10_9932_2015.pdf, consultado em janeiro de 2016.

CNPD, *Relatório de Atividades da Comissão Nacional de Proteção de Dados, 2013-2014*, in: https://www.cnpd.pt/bin/relatorios/anos/Relatorio_201314.pdf, consultado em janeiro de 2017.

CNPD, *Relatório de Atividades, 2015*, in: https://www.cnpd.pt/bin/relatorios/anos/Relatorio_2015.pdf, consultado em janeiro de 2017.

CNPD, *Utilização de Tecnologia de Geolocalização e o Tratamento de Dados Pessoais no Regime Jurídico Português: A Propósito da Deliberação n.º 7680/2014 da Comissão Nacional de Protecção de Dados e Jurisprudência Posterior*, in: https://www.cnpd.pt/bin/revistaforum/forum2016_3/index.html, consultado em janeiro de 2017.

COELHO, Maria Inês, *Site Exibe na Web Imagens de Casas e Lojas em Portugal*, in: http://pplware.sapo.pt/informacao/site-exibe-imagens-em-directo-na-web-de-casa-e-lojas-em-portugal/, consultado em dezembro 2015.

CONSELHO DA EUROPA, *Convenção Europeia dos Direitos do Homem*, in: http://www.echr.coe.int/Documents/Convention_POR.pdf, consultado em maio 2016.

DIÁRIO DA REPÚBLICA, *Decreto-Lei nº 135/2014 de 8 de setembro*, 1ª série - nº 172, 8 de setembro de 2014, pp. 4802-4805.

DIÁRIO DA REPÚBLICA, *Lei n.º 98/2015 de 18 de agosto*, 1ª série - nº 160, 18 de agosto de 2015, pp. 6081-6108.

DIÁRIO DA REPÚBLICA, *Lei nº 34/2013 de 16 de maio*, 1ª série - nº 94, 16 de maio de 2013, pp. 2921-2942.

DIÁRIO DA REPÚBLICA, *Lei nº 52/2013 de 25 de julho*, 1ª série - nº 142, 25 de julho de 2013, pp. 4365-4387.

DIÁRIO DA REPÚBLICA*, Lei nº 67/98 de 26 de Outubro*, 1ª série - A, nº 247, 26 de outubro de 1998, pp. 5536-5546.

DIÁRIO DA REPÚBLICA, *Portaria nº 106/2015 de 13 de abril*, 1ª série - nº 71, 13 de abril de 2015, pp. 1811-1812.

DIÁRIO DA REPÚBLICA, *Portaria nº 273/2013 de 20 de agosto*, 1ª série - nº 159, 20 de agosto de 2013, pp. 4956-4988.

FRÓIS, Catarina, *Vigilância e Poder*, Lisboa: Mundos Sociais, 2011.

GUERRA, Amadeu, *A Privacidade no Local de Trabalho*, Coimbra: Livraria Almedina, 2004.

KIM, David, SOLOMON, Michael G., *Fundamentals of Information Systems Security*, 2nd ed., Burlington: Jones & Bartlett Learning, 2013.

MIRANDA, Jorge, *Teoria do Estado e da Constituição*, Coimbra: Coimbra Editora, 2002.

OPEN HOUSE LISBOA, *Panóptico do Hospital Miguel Bombarda*, in: http://2015.openhouselisboa.com/places/panoptico-do-hospital-miguel-bombarda-3/, consultado em dezembro 2015.

OTERO, Paulo, *Instituições Políticas e Constitucionais – Volume I*, Coimbra: Livraria Almedina, 2009.

PINHEIRO, Alexandre Sousa, *"Privacy" e Protecção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional*, Lisboa: AAFDL, 2015.

PORTUGAL, *Código Civil*, in: https://dre.pt/web/guest/legislacao-consolidada/-/lc/107065833/201710311308/exportPdf/normal/1/cacheLevelPage?_LegislacaoConsolidada_WAR_drefrontofficeportlet_rp=indice, consultado em outubro de 2017.

PORTUGAL, *Código do Trabalho*, in: http://cite.gov.pt/asstscite/downloads/legislacao/CT25092017.pdf, consultado em outubro 2017.

PORTUGAL, *Códigos Penal e Processo Penal*, Porto: Porto Editora, 2015.

PORTUGAL, *Constituição da República Portuguesa*, Coimbra: Livraria Almedina, 2011.

PORTUGAL, *Proc.º nº 379/10.6TTBCL-A.P1 Apelação*, in: http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/06145eddca240e4d80257893004b5074?OpenDocument, consultado em janeiro de 2017.

PORTUGAL, *Processo de Consulta Pública Para Aprovação de Legislação Nacional Relativa ao Regulamento Geral de Proteção de Dados (RGPD)*, in: http://www.portugal.gov.pt/pt/consultas-publicas/consultas-legistativas-curso/20170905-mpma-protecao-dados.aspx, consultado em setembro de 2017.

PORTUGAL, *Relatório Anual de Segurança Privada 2015*, in: http://www.psp.pt/SP_CONSELHO_SEGURANCA/RASP_2015.pdf, consultado em outubro de 2016.

UNIÃO EUROPEIA, *Acórdão do Tribunal de Justiça (Quarta Secção) - 11 de dezembro de 2014*, in: http://curia.europa.eu/juris/document/document.jsf?text=&docid=160561&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=29158#Footnote*, consultado em dezembro 2015.

UNIÃO EUROPEIA, *Article 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'),* in: https://iapp.org/media/pdf/resource_center/WP29-2017-04-DPO-Guidance.pdf, consultado em agosto de 2017.

UNIÃO EUROPEIA, *Carta dos Direitos Fundamentais da União Europeia*, in: http://www.europarl.europa.eu/charter/pdf/text_pt.pdf, consultado em maio 2016.

UNIÃO EUROPEIA, *Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*, in: http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT, consultado em abril 2016.

UNIÃO EUROPEIA, *Diretiva 97/66/CE do Parlamento Europeu e do Conselho de 15 de Dezembro de 1997 relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das telecomunicações*, in: http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31997L0066&from=PT, consultado em dezembro 2015.

UNIÃO EUROPEIA, *Opinion 2/2017 on data processing at work*, in: http://www.google.pt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjUm72n_prWAhXKyRoKHfBnBQQQFggmMAA&url=http%3A%2F%2Fec.europa.eu%2

Fnewsroom%2Fdocument.cfm%3Fdoc_id%3D45631&usg=AFQjCNFL9EUmcaORV7p_Z6N12WltBgUlaA, consultado em agosto de 2017.

UNIÃO EUROPEIA, *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 (Regulamento Geral sobre a Proteção de Dados)*, in: http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX%3A32016R0679&from=EN, consultado em maio 2016.

UNIÃO EUROPEIA, *Regulamentos, Diretivas e Outros Atos Legislativos*, in: http://europa.eu/eu-law/decision-making/legal-acts/index_pt.htm, consultado em maio 2016.