Diretrizes 3/2019 sobre tratamento de dados pessoais através de dispositivos de vídeo

Versão 2.0

Adotado em 29 de janeiro de 2020

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Histórico de versões

Versão 2.1	26 de fevereiro de 2020	Alteração de erros materiais
Versão 2.0	29 de janeiro de 2020	Adoção das diretrizes após consulta pública
Versão 1.0	10 de julho de 2019	Adoção das diretrizes para consulta pública

Índice

O Comité Europeu para a Proteção de Dados

Tendo em conta o artigo 70.º, n.º 1, alínea e), do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (a seguir designado «RGPD»),

Tendo em conta o Acordo sobre o Espaço Económico Europeu (EEE) e, nomeadamente, o anexo XI e o Protocolo n.º 37, com a redação que lhe foi dada pela Decisão do Comité Misto do EEE n.º 154/2018, de 6 de julho de 2018[1],

Tendo em conta o artigo 12.º e o artigo 22.º do seu Regulamento Interno,

ADOTOU AS SEGUINTES DIRETRIZES

1 INTRODUÇÃO

1. O uso intensivo de dispositivos de vídeo tem repercussões no comportamento dos cidadãos. A utilização significativa deste tipo de equipamentos em muitas esferas da vida dos indivíduos exercerá uma maior pressão sobre o indivíduo para que evite a deteção de tudo o que possa ser percecionado como uma anomalia. Na verdade, estas tecnologias podem limitar as possibilidades de circulação anónima e de utilização anónima dos serviços e, regra geral, limitam a possibilidade de passar despercebido. As suas implicações em termos de proteção de dados são enormes.

2. Embora as pessoas possam não se incomodar com a utilização de videovigilância para determinadas finalidades de segurança, devem ser previstas garantias para evitar qualquer uso indevido para finalidades totalmente diferentes e – para o titular dos dados – inesperadas (por exemplo, finalidades de comercialização, controlo do desempenho dos trabalhadores, etc.). Além disso, são agora utilizadas muitas ferramentas que permitem explorar as imagens captadas e transformar as câmaras tradicionais em câmaras inteligentes. A quantidade de dados gerados pelo vídeo, combinada com estas ferramentas e técnicas, aumenta os riscos de utilização secundária (relacionada ou não com a finalidade originalmente atribuída ao sistema) ou mesmo de utilização indevida. Os princípios gerais do RGPD (artigo 5.º) devem ser sempre cuidadosamente considerados ao lidar com videovigilância.

3. Os sistemas de videovigilância mudam, de muitas formas, o modo como os profissionais dos setores privado e público interagem em locais privados ou públicos com o objetivo de aumentar a segurança, obter análises de audiência, apresentar publicidade personalizada, etc. A videovigilância adquiriu um elevado nível de desempenho através da crescente utilização da análise inteligente dos vídeos. Estas técnicas podem ser mais intrusivas (por exemplo, tecnologias biométricas complexas) ou menos intrusivas (por exemplo, algoritmos de contagem simples). É cada vez mais difícil manter o anonimato

[1] As referências a «Estados-Membros» no presente parecer devem ser entendidas como referências aos «Estados-Membros do EEE».

e preservar a privacidade individual. As questões de proteção de dados inerentes a cada situação e a análise jurídica podem diferir em função da tecnologia utilizada.

4. Para além das questões de privacidade, existem também riscos relacionados com possíveis avarias destes dispositivos e com o enviesamento que estes podem induzir. Os investigadores afirmam que o *software* utilizado para identificação, reconhecimento ou análise facial tem um desempenho diferente em função da idade, do género e da etnia da pessoa que está a ser identificada. O desempenho dos algoritmos varia em função da demografia, pelo que o enviesamento no reconhecimento facial ameaça reforçar os preconceitos da sociedade. Por este motivo, os responsáveis pelo tratamento dos dados também devem garantir que o tratamento de dados biométricos oriundos da videovigilância seja submetido a uma avaliação regular da sua pertinência e da adequação das garantias fornecidas.

5. A videovigilância não é por definição uma necessidade quando existem outros meios para alcançar o objetivo subjacente. Caso contrário, corremos o risco de mudar as normas culturais, levando à aceitação da falta de privacidade como o princípio geral.

6. Estas diretrizes visam dar orientações sobre como aplicar o RGPD em relação ao tratamento de dados pessoais através de dispositivos de vídeo. Os exemplos não são exaustivos, e a fundamentação geral pode ser aplicada a todas as potenciais áreas de utilização.

2 ÂMBITO DE APLICAÇÃO[2]

2.1 Dados pessoais

7. O controlo automatizado sistemático de um espaço específico por meios óticos ou audiovisuais, principalmente para fins de proteção de bens ou para proteger a vida e a saúde do indivíduo, tornou-se um fenómeno significativo nos nossos dias. Esta atividade resulta na recolha e conservação de informação pictórica ou audiovisual sobre todas as pessoas que entrem no espaço sob vigilância e que sejam identificáveis com base na sua aparência ou noutros elementos específicos. A identidade destas pessoas pode ser determinada com base nestes dados. Esta atividade permite também o tratamento posterior dos dados pessoais para obter informações sobre a presença e o comportamento das pessoas no espaço em questão. O risco potencial de utilização abusiva destes dados aumenta em função da dimensão do espaço sob vigilância e do número de pessoas que o frequentam. Este facto é refletido no Regulamento Geral sobre a Proteção de Dados, nomeadamente no artigo 35.º, n.º 3, alínea c), que exige a realização de uma avaliação de impacto da proteção de dados em caso de controlo sistemático de zonas acessíveis ao público em grande escala, bem como no artigo 37.º, n.º 1, alínea b), que exige que os subcontratantes designem um encarregado da proteção de dados sempre que as operações de tratamento, devido à sua natureza, exijam um controlo regular e sistemático dos titulares dos dados.

8. No entanto, o regulamento não se aplica ao tratamento de dados que não façam qualquer referência a uma pessoa, por exemplo, que não permitam identificar, direta ou indiretamente, um indivíduo.

> Exemplo: O RGPD não é aplicável a câmaras falsas (ou seja, qualquer câmara que não esteja a funcionar como tal e, portanto, não efetue o tratamento de dados pessoais). *Contudo, em alguns Estados-Membros, estas poderão estar sujeitas a outra legislação.*
>
> Exemplo: As gravações realizadas a altitudes elevadas só se enquadram no âmbito do RGPD se, nas circunstâncias em causa, os dados tratados puderem ser associados a uma pessoa específica.
>
> Exemplo: Há uma câmara de vídeo integrada num automóvel para prestar assistência de estacionamento. Se a câmara for construída ou adaptada de forma a não recolher quaisquer informações relativas a pessoas singulares (como matrículas ou informações que permitam identificar transeuntes), o RGPD não se aplica.

9.

2.2 Aplicação da Diretiva sobre a Proteção de Dados na Aplicação da Lei – Diretiva (UE) 2016/680

10. O tratamento de dados pessoais efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública, é abrangido pelo âmbito de aplicação da Diretiva (UE) 2016/680.

[2] O Comité Europeu para a Proteção de Dados (CEPD) observa que, sempre que o RGPD o permita, poderão aplicar-se requisitos específicos previstos na legislação nacional.

2.3 Isenção doméstica

11. Nos termos do artigo 2.º, n.º 2, alínea c), o tratamento de dados pessoais efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas, que podem incluir atividades em linha, está fora do âmbito de aplicação do RGPD[3].

12. Esta disposição – a chamada isenção doméstica – no contexto da videovigilância deve ser interpretada de forma restrita. Assim, de acordo com o Tribunal de Justiça da União Europeia (TJUE), a chamada «isenção doméstica» deve «ser interpretada como tendo unicamente por objeto as atividades que se inserem no âmbito da vida privada ou familiar dos particulares, o que não é manifestamente o caso do tratamento de dados de caráter pessoal que consiste na sua publicação na Internet de maneira que esses dados são disponibilizados a um número indefinido de pessoas»[4]. Além disso, um sistema de videovigilância que envolve o registo e a conservação constantes de dados pessoais e se estende, «ainda que parcialmente, ao espaço público e, por esse motivo, se dirige para fora da esfera privada da pessoa que procede ao tratamento de dados por esse meio, não pode ser considerada uma atividade exclusivamente "pessoal ou doméstica", na aceção do artigo 3.º, n.º 2, segundo travessão, da Diretiva 95/46»[5].

13. Quanto aos dispositivos de vídeo operados dentro das instalações de um particular, podem ser abrangidos pela isenção doméstica. Tal dependerá de vários fatores, que têm de ser analisados no seu conjunto para se chegar a uma conclusão. Além dos elementos supramencionados identificados pelos acórdãos do TJUE, o utilizador da videovigilância em casa tem de verificar se possui algum tipo de relação pessoal com o titular dos dados, se a escala ou frequência da vigilância sugere algum tipo de atividade profissional da sua parte e se a vigilância tem algum possível impacto adverso nos titulares dos dados. A presença de qualquer um dos elementos acima mencionados não sugere necessariamente que o tratamento esteja fora do âmbito de aplicação da isenção doméstica, sendo necessária uma avaliação global para chegar a essa conclusão.

> Exemplo: Um turista está a gravar vídeos através do telemóvel e de uma câmara de vídeo para ficar com um registo das suas férias. Mostra as gravações a amigos e familiares, mas não as disponibiliza a um número indefinido de pessoas. Este caso seria abrangido pela isenção doméstica.
>
> Exemplo: Uma ciclista de *downhill* quer filmar a sua descida com uma *action cam*. Está numa zona remota e só planeia utilizar as gravações para entretenimento pessoal em casa. Esta situação seria abrangida pela isenção doméstica, embora envolva, em certa medida, o tratamento de dados pessoais.
>
> Exemplo: Um indivíduo monitoriza e grava imagens do seu próprio jardim. A propriedade é vedada e apenas o próprio responsável pelo tratamento e a sua família entram regularmente no jardim. Esta situação é abrangida pela isenção doméstica, contanto que a videovigilância não se estenda, ainda que parcialmente, a um espaço público ou a uma propriedade vizinha.

14.

[3] Ver também o considerando 18.

[4] Tribunal de Justiça, acórdão de 6 de novembro de 2003, *Bodil Lindqvist*, C-101/01, EU:C:2003:596, n.º 47.

[5] Tribunal de Justiça, acórdão de 11 de dezembro de 2014, *František Ryneš contra Úřad pro ochranu osobních údajů*, C-212/13, EU:C:2014:2428, n.º 33.

3 LICITUDE DO TRATAMENTO

15. Antes da utilização, as finalidades do tratamento têm de ser determinadas em pormenor (artigo 5.º, n.º 1, alínea b)). A videovigilância pode servir muitas finalidades, por exemplo apoiar a proteção de bens e de outros ativos, apoiar a proteção da vida e da integridade física dos indivíduos e recolher provas para ações cíveis[6]. Estas finalidades do controlo devem ser documentadas por escrito (artigo 5.º, n.º 2) e têm de ser especificadas para cada câmara de vigilância em utilização. As câmaras que são utilizadas para a mesma finalidade por um único responsável pelo tratamento podem ser documentadas em conjunto. Além disso, os titulares dos dados devem ser informados sobre a(s) finalidade(s) do tratamento em conformidade com o artigo 13.º (*ver secção 7, Obrigações em matéria de transparência e informação*). A videovigilância baseada na mera finalidade de «segurança» ou «salvaguarda da segurança» não é suficientemente específica (artigo 5.º, n.º 1, alínea b)). Além disso, é contrária ao princípio de que os dados pessoais devem ser objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados (ver artigo 5.º, n.º 1, alínea a)).

16. Em princípio, todos os fundamentos jurídicos previstos no artigo 6.º, n.º 1, podem constituir uma base jurídica para o tratamento de dados de videovigilância. Por exemplo, o artigo 6.º, n.º 1, alínea c), aplica-se se a legislação nacional estipular a obrigação de realizar videovigilância[7]. Contudo, na prática, as disposições mais suscetíveis de serem utilizadas são:

- o artigo 6.º, n.º 1, alínea f) (interesses legítimos);
- o artigo 6.º, n.º 1, alínea e) (necessidade de exercer funções de interesse público ou de exercer a autoridade pública).

Em casos bastante excecionais, o artigo 6.º, n.º 1, alínea a) (consentimento) pode ser usado como base jurídica pelo responsável pelo tratamento.

3.1 Interesse legítimo – artigo 6.º, n.º 1, alínea f)

17. A avaliação jurídica do artigo 6.º, n.º 1, alínea f), deve assentar nos seguintes critérios, em conformidade com o considerando 47.

3.1.1 Existência de interesses legítimos

18. A videovigilância é lícita se for necessária para satisfazer os interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular (artigo 6.º, n.º 1, alínea f)). Os interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros podem ser de natureza jurídica[8], económica ou imaterial[9]. No entanto, o responsável pelo tratamento deve ter em conta que, se o titular dos dados se opuser à vigilância em conformidade com o artigo 21.º, o responsável pelo tratamento só pode efetuar a videovigilância desse titular dos dados se se tratar de interesses legítimos *imperiosos* que

[6] As regras relativas à obtenção de prova para ações cíveis variam entre os Estados-Membros.

[7] As presentes diretrizes não analisam nem descrevem em pormenor as legislações nacionais que possam divergir entre Estados-Membros.

[8] Tribunal de Justiça, acórdão de 4 de maio de 2017, *Rīgas satiksme*, C-13/16, EU:C:2017:336.

[9] Ver WP 217, Grupo de Trabalho do Artigo 29.º.

prevalecem sobre os interesses, os direitos e as liberdades do titular dos dados ou se o tratamento for necessário à declaração, ao exercício ou à defesa de um direito.

19. Numa situação real e perigosa, a finalidade de proteger bens contra assalto, furto ou vandalismo pode constituir um interesse legítimo para a videovigilância.

20. O interesse legítimo tem de ser real e atual (ou seja, não pode ser ficcional nem especulativo)[10]. É necessário que exista uma situação de perigo real – como danos ou incidentes graves no passado – antes de a vigilância poder ser iniciada. À luz do princípio da responsabilidade, seria aconselhável que os responsáveis pelo tratamento documentassem incidentes relevantes (data, método, perda financeira) e as acusações criminais correspondentes. Esses incidentes documentados podem constituir provas sólidas da existência de um interesse legítimo. A existência de um interesse legítimo e da necessidade de controlo devem ser reavaliadas periodicamente (por exemplo, uma vez por ano, dependendo das circunstâncias).

> Exemplo: O proprietário de uma loja quer abrir um novo estabelecimento e pretende instalar um sistema de videovigilância para prevenir o vandalismo. Consegue demonstrar, mediante a apresentação de estatísticas, que existe uma expectativa elevada de vandalismo na vizinhança próxima. É útil também, neste caso, a experiência das lojas vizinhas. Não é necessário que o responsável pelo tratamento em questão tenha sofrido danos, contanto que os danos na vizinhança sugiram um perigo ou uma situação semelhante e possam, desse modo, constituir uma indicação de interesse legítimo. No entanto, não basta apresentar estatísticas nacionais ou gerais de criminalidade sem analisar a zona em questão ou os perigos para o estabelecimento em causa.

21.

22. As situações de perigo iminente podem constituir um interesse legítimo, nomeadamente no caso de bancos ou lojas que vendem artigos valiosos (por exemplo, joalharias) ou de zonas conhecidas por serem cenários habituais de crimes contra a propriedade (por exemplo, bombas de gasolina).

23. O RGPD também estabelece claramente que as autoridades públicas não podem invocar o interesse legítimo para justificar o tratamento dos dados na prossecução das suas atribuições (artigo 6.º, n.º 1, segundo parágrafo).

3.1.2 Necessidade do tratamento

24. Os dados pessoais devem ser adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»); ver artigo 5.º, n.º 1, alínea c). Antes de instalar um sistema de videovigilância, o responsável pelo tratamento deve sempre examinar criticamente se esta medida é, em primeiro lugar, adequada para atingir o objetivo desejado e, em segundo lugar, adequada e necessária às respetivas finalidades. As medidas de videovigilância só devem ser escolhidas se a finalidade do tratamento não puder ser razoavelmente cumprida por outros meios que sejam menos intrusivos para os direitos e liberdades fundamentais do titular dos dados.

25. Por exemplo, um responsável pelo tratamento que pretenda evitar crimes contra a propriedade pode, em vez de instalar um sistema de videovigilância, adotar medidas de segurança alternativas, como vedar a propriedade, introduzir patrulhas regulares por pessoal de segurança, utilizar porteiros, melhorar a iluminação, instalar fechaduras de segurança e janelas e portas invioláveis ou aplicar

[10] Ver WP 217, Grupo de Trabalho do Artigo 29.º, p. 24 e seguintes. Ver também processo C-708/18 do TJUE, n.º 44.

revestimento ou película *antigrafitti* nas paredes. Estas medidas podem ser tão eficazes como os sistemas de videovigilância contra assaltos, furto e vandalismo. O responsável pelo tratamento tem de avaliar caso a caso se estas medidas podem constituir uma solução razoável.

26. Antes de operar um sistema de câmaras, o responsável pelo tratamento é obrigado a avaliar onde e quando as medidas de videovigilância são estritamente necessárias. Normalmente, um sistema de vigilância que funcione de noite e fora do horário normal de trabalho satisfaz as necessidades do responsável pelo tratamento relativamente à prevenção de eventuais perigos para a sua propriedade.

27. Regra geral, a necessidade de utilizar videovigilância para proteger as instalações dos responsáveis pelo tratamento termina nos limites da propriedade.[11] No entanto, há casos em que a vigilância da propriedade não é suficiente para assegurar uma proteção eficaz. Em determinados casos, pode ser necessário alargar a videovigilância às imediações das instalações. Nesta situação, o responsável pelo tratamento deve ponderar a utilização de meios físicos e técnicos, por exemplo a ocultação ou a pixelização das zonas não relevantes.

> Exemplo: Uma livraria quer proteger as suas instalações contra vandalismo. Regra geral, as câmaras só devem filmar as próprias instalações, uma vez que a finalidade em questão não exige a vigilância das instalações vizinhas nem dos espaços públicos circundantes.

28.

29. Relativamente à forma como os elementos de prova são preservados, também se colocam questões relacionadas com a necessidade de tratamento. Em alguns casos, pode ser necessário utilizar soluções de caixa negra em que as gravações são automaticamente apagadas após um determinado prazo de conservação e só são consultadas caso ocorra um incidente. Noutras situações, pode não ser necessário gravar o material de vídeo, justificando-se em vez disso recorrer ao controlo em tempo real. A decisão entre as soluções de caixa negra e o controlo em tempo real também se deve basear na finalidade em questão. Se, por exemplo, a finalidade da videovigilância for a preservação de provas, os métodos em tempo real geralmente não são adequados. Por vezes, o controlo em tempo real também pode ser mais intrusivo do que a conservação e a eliminação automática do material após um período de tempo limitado (por exemplo, se alguém estiver constantemente a visualizar o monitor, o método pode ser mais intrusivo do que se não houver nenhum monitor e o material for diretamente armazenado numa caixa negra). O princípio da minimização dos dados deve ser considerado neste contexto (artigo 5.º, n.º 1, alínea c)). Importa também ter em mente a possibilidade de o responsável pelo tratamento utilizar, em vez de videovigilância, pessoal de segurança capaz de reagir e intervir imediatamente.

3.1.3 Ponderação dos interesses

30. Partindo do princípio de que a videovigilância é necessária para proteger os interesses legítimos de um responsável pelo tratamento, um sistema de videovigilância só pode ser acionado se aos interesses legítimos do responsável pelo tratamento ou de terceiros (por exemplo, proteção de bens ou da integridade física) não se sobrepuserem os interesses ou os direitos e liberdades fundamentais do titular dos dados. O responsável pelo tratamento tem de considerar 1) em que medida o controlo afeta os interesses e os direitos e liberdades fundamentais dos indivíduos e 2) se este controlo resulta em violações ou consequências negativas no que diz respeito aos direitos do titular dos dados. Na verdade, a ponderação dos interesses é obrigatória. Os direitos e liberdades fundamentais, por um lado, e os

[11] Além disso, poderá estar sujeita à legislação nacional em alguns Estados-Membros.

interesses legítimos do responsável pelo tratamento, por outro, têm de ser cuidadosamente avaliados e ponderados.

> Exemplo: Uma empresa de estacionamento privado tem registado problemas recorrentes com furtos nos carros estacionados. A zona de estacionamento é um espaço aberto, de fácil acesso a qualquer pessoa, mas está claramente identificada com sinais e delimitada por bloqueadores rodoviários. A empresa de estacionamento tem um interesse legítimo (evitar furtos nos carros dos clientes) em controlar a área durante o período do dia em que têm ocorrido os problemas. Os titulares dos dados são controlados num período de tempo limitado, não se encontram na área em questão para fins recreativos e também têm interesse em evitar os furtos. Neste caso, o interesse legítimo do responsável pelo tratamento prevalece sobre o interesse dos titulares dos dados de não serem controlados.
>
> Exemplo: Um restaurante decide instalar câmaras de vídeo nos lavabos para controlar o asseio das instalações sanitárias. Neste caso, os direitos dos titulares dos dados prevalecem claramente sobre os interesses do responsável pelo tratamento, pelo que as câmaras não podem ser instaladas nesse local.

31.

3.1.3.1 Tomada de decisões caso a caso

32. Sendo a ponderação dos interesses obrigatória nos termos do regulamento, a decisão tem de ser tomada caso a caso (ver artigo 6.º, n.º 1, alínea f)). É insuficiente referir situações abstratas ou comparar casos similares. O responsável pelo tratamento tem de avaliar os riscos de interferência com os direitos do titular dos dados, sendo o critério decisivo a intensidade da intervenção no que diz respeito aos direitos e liberdades do indivíduo.

33. A intensidade pode ser definida, nomeadamente, pelo tipo de informação recolhida (conteúdo informativo), pelo âmbito (densidade da informação, extensão espacial e geográfica), pelo número de titulares dos dados em causa, quer como um número específico, quer em percentagem da população relevante, pela situação em questão, pelos interesses reais do grupo de titulares dos dados, pelos meios alternativos e pela natureza e âmbito da avaliação dos dados.

34. Os fatores de ponderação importantes podem incluir o tamanho da área que está sob vigilância e a quantidade de titulares de dados sob vigilância. O uso de videovigilância numa zona remota (por exemplo, para observar vida selvagem ou para proteger infraestruturas críticas, como uma antena de rádio privada) tem de ser avaliado de forma diferente do uso de videovigilância numa zona pedonal ou num centro comercial.

> Exemplo: Ao instalar uma câmara de trânsito (por exemplo, com o objetivo de recolher provas em caso de acidente), é importante assegurar que a câmara não está constantemente a gravar o trânsito, bem como as pessoas que se encontram junto à estrada. Caso contrário, o interesse de possuir gravações de vídeo como prova no caso mais hipotético de um acidente rodoviário não poderá justificar esta grave interferência com os direitos dos titulares dos dados[11].

35.

3.1.3.2 Expectativas razoáveis dos titulares dos dados

36. De acordo com o considerando 47, a existência de um interesse legítimo requer uma avaliação cuidada. Neste caso, há que ter em conta as expectativas razoáveis do titular dos dados no momento e no contexto do tratamento dos seus dados pessoais. No que diz respeito ao controlo sistemático, a relação entre o titular dos dados e o responsável pelo tratamento pode variar significativamente e

pode afetar as expectativas razoáveis do titular dos dados. A interpretação do conceito de expectativas razoáveis não se deve basear apenas nas expectativas subjetivas em questão. Pelo contrário, o critério decisivo tem de ser a possibilidade razoável de um terceiro prever e concluir que seria sujeito a controlo nessa situação específica.

37. Por exemplo, um trabalhador no seu local de trabalho provavelmente não espera, na maioria dos casos, ser controlado pelo seu empregador[12]. Além disso, não é de esperar a realização de controlo num jardim privado, em espaços habitados ou em gabinetes de exame e tratamento. No mesmo sentido, não é razoável esperar que seja realizado controlo em instalações sanitárias ou saunas, uma vez que o controlo deste tipo de espaços constitui uma forte interferência nos direitos do titular dos dados. Os titulares dos dados têm a expectativa razoável de que não será realizada qualquer videovigilância nesses espaços. Por outro lado, o cliente de um banco poderá esperar ser objeto de vigilância no interior do banco ou junto de uma caixa multibanco.

38. Os titulares dos dados também podem ter a expectativa de não ser controlados no interior de espaços públicos, especialmente se esses espaços forem normalmente utilizados para atividades de recuperação, reabilitação e lazer, bem como em lugares onde os indivíduos permanecem e/ou comunicam, como áreas de repouso, mesas de restaurantes, parques, cinemas e ginásios. Neste caso, os interesses ou direitos e liberdades do titular dos dados sobrepõem-se frequentemente aos interesses legítimos do responsável pelo tratamento.

> Exemplo: Em casas de banho, os titulares dos dados não esperam ser objeto de vigilância. A videovigilância para prevenir acidentes, por exemplo, não é proporcionada.

39.

40. Os sinais que informam o titular dos dados sobre a videovigilância são irrelevantes quando se determina o que o titular dos dados pode esperar objetivamente. Isto significa que, por exemplo, o proprietário de uma loja não pode argumentar que os clientes têm *objetivamente* a expectativa razoável de serem vigiados só porque existe um sinal à entrada a informá-los sobre a vigilância.

3.2 A necessidade de exercer funções de interesse público ou de exercer a autoridade pública de que está investido o responsável pelo tratamento – artigo 6.º, n.º 1, alínea e)

41. Os dados pessoais podem ser tratados por meio de videovigilância nos termos do artigo 6.º, n.º 1, alínea e), se o tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública[13]. O exercício da autoridade pública poderá não permitir esse tratamento, mas outras bases legislativas, nomeadamente questões de «saúde e segurança» tendo em vista a proteção de visitantes e trabalhadores, poderão proporcionar uma margem de manobra limitada para o tratamento, sem deixar de ter em conta as obrigações e os direitos dos titulares dos dados previstos no RGPD.

[12] Ver também: Grupo de Trabalho do Artigo 29.º, Parecer 2/2017 sobre o tratamento de dados no local de trabalho, WP 249, adotado em 8 de junho de 2017.

[13] O fundamento jurídico para o tratamento referido é definido pelo direito da União ou pelo direito do Estado-Membro e a finalidade do tratamento «deve ser necessária ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento» (artigo 6.º, n.º 3).

42. Os Estados-Membros podem manter ou introduzir legislação nacional específica relativa à videovigilância para adaptar a aplicação das regras do RGPD, determinando com maior precisão os requisitos específicos para o tratamento, desde que o façam em conformidade com os princípios estabelecidos no RGPD (por exemplo, em matéria de limitação da conservação ou de proporcionalidade).

3.3 Consentimento – artigo 6.º, n.º 1, alínea a)

43. O consentimento tem de ser uma manifestação de vontade, livre, específica, informada e explícita, conforme descrito nas orientações relativas ao consentimento[14].

44. No que diz respeito ao controlo sistemático, o consentimento do titular dos dados só pode servir de base jurídica em conformidade com o artigo 7.º (ver considerando 43) em casos excecionais. Pela sua própria natureza, esta tecnologia controla um número desconhecido de pessoas em simultâneo. O responsável pelo tratamento dificilmente conseguirá provar que o titular dos dados deu o seu consentimento antes do tratamento dos seus dados pessoais (artigo 7.º, n.º 1). Pressupondo que o titular dos dados retira o seu consentimento, será difícil ao responsável pelo tratamento provar que já não são tratados dados pessoais (artigo 7.º, n.º 3).

> Exemplo: Os atletas podem solicitar monitorização durante exercícios individuais para analisar as suas técnicas e o seu desempenho. Por outro lado, quando um clube desportivo toma a iniciativa de monitorizar uma equipa inteira com o mesmo objetivo, o consentimento muitas vezes não será válido, pois os atletas individuais podem sentir-se pressionados a dar o seu consentimento tendo em conta que uma eventual recusa poderia prejudicar os colegas de equipa.

45.

46. Se o responsável pelo tratamento quiser basear-se no consentimento, tem o dever de se certificar de que cada titular dos dados que entra na área que está sob videovigilância deu o seu consentimento. Este consentimento tem de cumprir as condições previstas no artigo 7.º. A entrada numa zona assinalada como estando sob vigilância (por exemplo, se a pessoa for convidada a atravessar um átrio ou um portão específico para entrar numa zona sob vigilância) não constitui uma declaração nem um ato positivo claro para efeitos de consentimento, a menos que cumpra os critérios dos artigos 4.º e 7.º conforme descrito nas orientações relativas ao consentimento[15].

47. Dado o desequilíbrio de poder entre empregadores e trabalhadores, na maioria dos casos os empregadores não devem basear-se no consentimento para efetuar o tratamento de dados pessoais, uma vez que é improvável que este tenha sido dado de livre vontade. As orientações relativas ao consentimento devem ser tidas em consideração neste contexto.

48. O direito do Estado-Membro ou as convenções coletivas (incluindo «acordos setoriais») podem prever regras específicas para o tratamento de dados pessoais dos trabalhadores no contexto laboral (ver artigo 88.º).

---

[14] Grupo de Trabalho do Artigo 29.º (GT29), «Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679» (WP 259 rev.01). – aprovadas pelo CEPD

[15] Grupo de Trabalho do Artigo 29.º (GT29), «Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679» (WP 259) – aprovadas pelo CEPD – que devem ser tidas em conta.

4 DIVULGAÇÃO DE GRAVAÇÕES DE VÍDEO A TERCEIROS

49. Em princípio, as regras gerais do RGPD aplicam-se à divulgação de gravações de vídeo a terceiros.

4.1 Divulgação de gravações de vídeo a terceiros em geral

50. O termo «divulgação» é definido no artigo 4.º, ponto 2, como transmissão (por exemplo, comunicação individual), difusão (por exemplo, publicação em linha) ou qualquer outra forma de disponibilização. O termo «terceiro» é definido no artigo 4.º, ponto 10. Quando a divulgação é efetuada para países terceiros ou organizações internacionais, também se aplicam as disposições especiais dos artigos 44.º e seguintes.

51. Qualquer divulgação de dados pessoais é um tipo separado de tratamento de dados pessoais relativamente ao qual o responsável pelo tratamento tem de ter uma base jurídica nos termos do artigo 6.º.

> Exemplo: Um responsável pelo tratamento que pretenda carregar uma gravação para a Internet tem de utilizar uma base jurídica para esse tratamento, por exemplo obtendo o consentimento do titular dos dados em conformidade com o artigo 6.º, n.º 1, alínea a).

52.

53. A transmissão de gravações de vídeo a terceiros para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos é possível nos termos das regras do artigo 6.º, n.º 4.

> Exemplo: É instalada videovigilância de uma cancela (num parque de estacionamento) com o objetivo de resolver questões relacionadas com danos. Ocorre um dano e a gravação é transferida para um advogado para agir judicialmente. Neste caso, a finalidade da gravação é a mesma que a da transferência.
>
> Exemplo: É instalada videovigilância de uma cancela (num parque de estacionamento) com o objetivo de resolver questões relacionadas com danos. A gravação é publicada na Internet apenas por razões de diversão. Neste caso, a finalidade mudou e não é compatível com a finalidade inicial. Além disso, seria problemático identificar uma base jurídica para este tratamento (publicação).

54.

55. Um terceiro destinatário terá de fazer a sua própria análise jurídica, nomeadamente identificando a sua base jurídica ao abrigo do artigo 6.º para o tratamento (por exemplo, a receção do material).

4.2 Divulgação de gravações de vídeo a autoridades de aplicação da lei

56. A divulgação de gravações de vídeo às autoridades de aplicação da lei é também um processo independente, que requer uma justificação distinta para o responsável pelo tratamento.

57. Nos termos do artigo 6.º, n.º 1, alínea c), o tratamento é lícito se for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito. Embora a legislação aplicável em matéria de forças policiais esteja sob o controlo exclusivo dos Estados-Membros, existem muito provavelmente regras gerais que regulam a transferência de provas para as autoridades de aplicação da lei em todos os Estados-Membros. A transmissão dos dados pelo responsável pelo tratamento é regida pelo RGPD. Se a legislação nacional exigir que o responsável pelo tratamento coopere com as autoridades de aplicação da lei (por exemplo, de investigação), a base jurídica para a transmissão dos dados é a obrigação jurídica prevista no artigo 6.º, n.º 1, alínea c).

58. Por conseguinte, a limitação das finalidades prevista no artigo 6.º, n.º 4, raramente é problemática, uma vez que a divulgação remete explicitamente para a legislação dos Estados-Membros. Não é, pois, necessária uma consideração dos requisitos especiais para uma mudança de finalidade na aceção das alíneas a) a e).

> Exemplo: O proprietário de uma loja grava imagens na entrada do estabelecimento. As gravações mostram uma pessoa a roubar a carteira de outra pessoa. A polícia pede ao responsável pelo tratamento que entregue o material a fim de auxiliar na investigação. Nesse caso, o proprietário da loja utilizaria a base jurídica prevista no artigo 6.º, n.º 1, alínea c) (obrigação jurídica), em conjugação com a legislação nacional pertinente, para o processamento da transferência.

59.

> Exemplo: Uma câmara é instalada numa loja por razões de segurança. O proprietário da loja acredita ter gravado algo suspeito e decide enviar o material para a polícia (sem qualquer indicação de que existe algum tipo de investigação em curso). Neste caso, o proprietário da loja tem de avaliar se se encontram reunidas as condições, que, na maioria dos casos, são as previstas no artigo 6.º, n.º 1, alínea f). Isto acontece geralmente se o proprietário da loja tiver uma suspeita razoável de que foi cometido um crime.

60.

61. O tratamento dos dados pessoais pelas próprias autoridades de aplicação da lei não segue o RGPD (ver artigo 2.º, n.º 2, alínea d)), mas sim a Diretiva sobre a Proteção de Dados na Aplicação da Lei – Diretiva (UE) 2016/680.

5 TRATAMENTO DE CATEGORIAS ESPECIAIS DE DADOS

62. Os sistemas de videovigilância geralmente recolhem quantidades maciças de dados pessoais suscetíveis de revelar informações de natureza altamente pessoal e até mesmo categorias especiais de dados. Na verdade, dados aparentemente não significativos originalmente recolhidos por vídeo podem ser utilizados para inferir outras informações com o intuito de atingir finalidades diferentes (por exemplo, registar os hábitos de um indivíduo). No entanto, a videovigilância nem sempre é considerada como tratamento de categorias especiais de dados pessoais.

> Exemplo: Gravações de vídeo que mostrem um titular de dados de óculos ou numa cadeira de rodas não são, por si só, consideradas categorias especiais de dados pessoais.

63.

64. No entanto, se as gravações forem objeto de tratamento com o intuito de deduzir categorias especiais de dados, aplica-se o artigo 9.º.

> Exemplo: Poderiam, por exemplo, deduzir-se opiniões políticas a partir de imagens que mostrem titulares de dados identificáveis a participar num evento, numa manifestação, etc. Esta situação seria abrangida pelo artigo 9.º.
>
> Exemplo: A instalação de uma câmara de vídeo num hospital para monitorizar o estado de saúde de um doente seria considerada como tratamento de categorias especiais de dados pessoais (artigo 9.º).

65.

66. De um modo geral, por princípio, sempre que se instala um sistema de videovigilância, deve ter-se devidamente em conta o princípio da minimização dos dados. Assim, mesmo nos casos em que o artigo 9.º, n.º 1, não se aplica, o responsável pelo tratamento deve sempre tentar minimizar o risco de captação de imagens que revelem outros dados sensíveis (para além do artigo 9.º), independentemente do objetivo.

> Exemplo: Um sistema de videovigilância que efetua a vigilância de uma igreja não se enquadra, por si só, no artigo 9.º. No entanto, o responsável pelo tratamento tem de proceder a uma avaliação especialmente cuidada nos termos do artigo 6.º, n.º 1, alínea f), tendo em conta a natureza dos dados, bem como o risco de captação de outros dados sensíveis (para além do artigo 9.º), ao avaliar os interesses do titular dos dados.

67.

68. Se for utilizado um sistema de videovigilância para tratar categorias especiais de dados, o responsável pelo tratamento deve identificar tanto uma exceção para o tratamento de categorias especiais de dados ao abrigo do artigo 9.º (ou seja, uma exceção à regra geral de não tratamento de categorias especiais de dados) como uma base jurídica ao abrigo do artigo 6.º.

69. Por exemplo, o artigo 9.º, n.º 2, alínea c), («Se o tratamento for necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular») poderia ser utilizado – teórica e excecionalmente –, mas o responsável pelo tratamento teria de o justificar como uma necessidade absoluta para salvaguardar os interesses vitais de uma pessoa e comprovar que o titular dos dados em questão estava «[...] física ou legalmente incapacitado de dar o seu consentimento». Além disso, o responsável pelo tratamento não poderá usar o sistema por nenhum outro motivo.

70. Neste caso, é importante observar que nem todas as isenções enumeradas no artigo 9.º são suscetíveis de serem utilizadas para justificar o tratamento de categorias especiais de dados através de videovigilância. Mais concretamente, os responsáveis pelo tratamento desses dados no contexto da videovigilância não podem basear-se no artigo 9.º, n.º 2, alínea e), que permite o tratamento se este se referir a dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular. O simples facto de o titular dos dados entrar no enquadramento da câmara não significa que pretenda tornar públicas categorias especiais de dados que lhe digam respeito.

71. Além disso, o tratamento de categorias especiais de dados requer uma vigilância reforçada e contínua de certas obrigações; por exemplo, um elevado nível de segurança e uma avaliação de impacto da proteção de dados, quando necessário.

> Exemplo: Um empregador não deve usar registos de videovigilância que mostrem uma manifestação com o objetivo de identificar os manifestantes.

72.

5.1 Considerações gerais relativas ao tratamento de dados biométricos

73. A utilização de dados biométricos, mais concretamente o reconhecimento facial, implica riscos acrescidos para os direitos dos titulares dos dados. É crucial que o recurso a este tipo de tecnologias se faça no devido respeito pelos princípios da licitude, da necessidade, da proporcionalidade e da minimização dos dados, tal como estabelecido no RGPD. Embora a utilização destas tecnologias possa ser considerada particularmente eficaz, os responsáveis pelo tratamento devem, antes de mais, avaliar o seu impacto nos direitos e liberdades fundamentais e ponderar a utilização de meios menos intrusivos para atingir a finalidade legítima do tratamento.

74. Para ser considerado tratamento de dados biométricos na aceção do RGPD, o tratamento de dados em bruto, nomeadamente características físicas, fisiológicas ou comportamentais de uma pessoa singular, tem de incluir uma medição dessas características. Uma vez que os dados biométricos são o resultado dessas medições, o RGPD prevê, no seu artigo 4.º, ponto 14, que são «[...] resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular [...]». As gravações de vídeo de um indivíduo não podem, contudo, ser consideradas, por si só, como dados biométricos nos termos do artigo 9.º, uma vez que não foram processadas por meios técnicos específicos de modo a contribuir para a identificação do indivíduo[16].

75. Para que o tratamento seja considerado um tratamento de categorias especiais de dados pessoais (artigo 9.º), é necessário que os dados biométricos sejam tratados «para identificar uma pessoa de forma inequívoca».

76. Em suma, à luz do artigo 4.º, ponto 14, e do artigo 9.º, há que ter em conta três critérios:

- **a natureza dos dados:** dados relacionados com as características físicas, fisiológicas ou comportamentais de uma pessoa singular,
- **o meio e a forma de tratamento:** dados «resultantes de um tratamento técnico específico»,

[16] O considerando 51 do RGPD apoia esta análise, prevendo que «[o] tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular.».

- **a finalidade do tratamento:** os dados devem ser utilizados para identificar uma pessoa de forma inequívoca.

77. A utilização da videovigilância, incluindo a funcionalidade de reconhecimento biométrico, instalada por entidades privadas para os seus próprios fins (por exemplo, comercialização, estatísticas ou até mesmo segurança) exigirá, na maioria dos casos, o consentimento explícito de todas os titulares dos dados (artigo 9.º, n.º 2, alínea a)), embora também possa ser aplicável outra exceção adequada prevista no artigo 9.º .

Exemplo: Para melhorar os seus serviços, uma empresa privada substitui os pontos de controlo da identificação de passageiros no interior de um aeroporto (entrega de bagagem, embarque) por sistemas de videovigilância que utilizam técnicas de reconhecimento facial para verificar a identidade dos passageiros que optaram por consentir em tal procedimento. Uma vez que o tratamento se enquadra no artigo 9.º, os passageiros, que terão previamente dado o seu consentimento explícito e informado, terão de se inscrever num terminal automático, por exemplo, para criar e registar o seu modelo facial associado ao seu cartão de embarque e identidade. Os pontos de verificação com reconhecimento facial têm de ser claramente separados, por exemplo instalando o sistema dentro de um pórtico, para que os modelos biométricos das pessoas que não deram o seu consentimento não sejam captados. Apenas os passageiros que tenham dado previamente o seu consentimento e que tenham efetuado a inscrição utilizarão o pórtico equipado com o sistema biométrico.

Exemplo: Um responsável pelo tratamento gere o acesso ao seu edifício através de um método de reconhecimento facial. As pessoas só podem utilizar esta forma de acesso se tiverem dado previamente o seu consentimento explícito e informado (de acordo com o artigo 9.º, n.º 2, alínea a)). No entanto, a fim de garantir que o sistema não capta ninguém que não tenha dado previamente o seu consentimento, o método de reconhecimento facial deve ser acionado pelo próprio titular dos dados, por exemplo premindo um botão. Para garantir a licitude do tratamento, o responsável pelo tratamento deve sempre oferecer uma forma alternativa de acesso ao edifício, sem tratamento biométrico, tal como cartões de identificação ou chaves.

78.

79. Neste tipo de casos, em que são gerados modelos biométricos, os responsáveis pelo tratamento devem garantir que, uma vez obtido um resultado com ou sem correspondência, todos os modelos intermédios feitos na hora (com o consentimento explícito e informado do titular dos dados) para serem comparados com os criados pelos titulares dos dados no momento da inscrição são apagados imediatamente e de forma segura. Os modelos criados para a inscrição só devem ser conservados para a realização da finalidade do tratamento e não devem ser armazenados nem arquivados.

80. No entanto, quando a finalidade do tratamento é, por exemplo, distinguir uma categoria de pessoas de outra, mas não identificar ninguém de forma inequívoca, o tratamento não se enquadra no artigo 9.º.

Exemplo: O proprietário de uma loja gostaria de personalizar o seu anúncio publicitário com base nas características de género e de idade do cliente captadas por um sistema de videovigilância. Se o sistema não gerar modelos biométricos para identificar as pessoas de forma inequívoca, mas apenas detetar essas características físicas para classificar a pessoa, o tratamento não se enquadra no artigo 9.º (desde que não seja efetuado o tratamento de nenhum outro tipo de categorias especiais de dados).

81.

82. Contudo, o artigo 9.º aplica-se se o responsável pelo tratamento conservar dados biométricos (geralmente através de modelos que são criados pela extração de determinadas características da forma bruta dos dados biométricos – por exemplo, as medidas faciais de uma imagem) com o objetivo de identificar uma pessoa de forma inequívoca. Se um responsável pelo tratamento desejar detetar um titular dos dados que volte a entrar naquele espaço ou que entre noutro espaço (por exemplo, para projetar publicidade personalizada de forma contínua), a finalidade consistirá em identificar de forma inequívoca uma pessoa singular, o que significa que a operação em questão será, desde o início, abrangida pelo artigo 9.º. Este poderia ser o caso se um responsável pelo tratamento conservasse modelos gerados para apresentar mais publicidade personalizada em vários painéis em diferentes locais dentro da loja. Uma vez que o sistema utiliza características físicas para detetar indivíduos específicos que voltam a entrar no enquadramento da câmara (como os visitantes de um centro comercial) e para os localizar, este seria um método de identificação biométrica, pois teria por objetivo o reconhecimento através do uso de um tratamento técnico específico.

> Exemplo: O proprietário de uma loja instalou um sistema de reconhecimento facial dentro da sua loja a fim de personalizar a publicidade que é apresentada a cada indivíduo. O responsável pelo tratamento tem de obter o consentimento explícito e informado de todos os titulares dos dados antes de utilizar este sistema biométrico e de apresentar publicidade personalizada. O sistema seria ilegal se captasse visitantes ou transeuntes que não tivessem consentido na criação do seu modelo biométrico, mesmo que o seu modelo fosse apagado no menor espaço de tempo possível. Na verdade, estes modelos temporários constituem dados biométricos tratados para identificar de forma inequívoca uma pessoa que pode não desejar receber publicidade personalizada.

83.

84. O Comité Europeu para a Proteção de Dados (CEPD) observa que alguns sistemas biométricos são instalados em ambientes não controlados[17], o que significa que o sistema envolve a captação, em tempo real, dos rostos de qualquer indivíduo que passe em frente à câmara criando modelos biométricos, incluindo de pessoas que não deram o seu consentimento para a utilização do dispositivo biométrico. Estes modelos são comparados com os criados em relação a titulares dos dados que deram o seu consentimento prévio durante um processo de inscrição (isto é, os utilizadores do dispositivo biométrico) para que o responsável pelo tratamento reconheça se a pessoa é ou não um utilizador do dispositivo biométrico. Neste caso, o sistema é frequentemente concebido para estabelecer uma distinção entre os indivíduos que pretende reconhecer a partir de uma base de dados e os indivíduos que não estão inscritos. Uma vez que o objetivo consiste em identificar pessoas singulares de forma inequívoca, continua a ser necessária uma exceção nos termos do artigo 9.º, n.º 2, do RGPD para qualquer pessoa que seja captada pela câmara.

[17] Isto significa que o dispositivo biométrico está situado num espaço aberto ao público e é capaz de atuar sobre qualquer pessoa que passe no local, por oposição aos sistemas biométricos em ambientes controlados, que só podem ser utilizados com o consentimento das pessoas.

Exemplo: Um hotel usa videovigilância para alertar automaticamente o gerente do hotel da chegada de um VIP quando o rosto do hóspede é reconhecido. Estes VIP deram previamente o seu consentimento explícito para o uso do reconhecimento facial antes de serem registados numa base de dados criada para o efeito. Estes sistemas de tratamento de dados biométricos seriam ilegais, a menos que todos os outros hóspedes captados pelo sistema (a fim de identificar os VIP) tivessem consentido no tratamento de acordo com o artigo 9.º, n.º 2, alínea a), do RGPD.

Exemplo: Um responsável pelo tratamento instala um sistema de videovigilância com reconhecimento facial na entrada de uma sala de concertos gerida por si. O responsável pelo tratamento deve definir entradas claramente separadas; uma com um sistema biométrico e outra sem este sistema (por exemplo, com leitura ótica dos bilhetes). As entradas equipadas com dispositivos biométricos devem ser instaladas e estar acessíveis de forma a evitar que o sistema capte modelos biométricos de espetadores que não tenham dado o seu consentimento.

85.

86. Por último, quando o consentimento é exigido pelo artigo 9.º do RGPD, o responsável pelo tratamento não deve fazer depender o acesso aos seus serviços da aceitação do tratamento biométrico. Por outras palavras, e nomeadamente quando o tratamento biométrico é utilizado para fins de autenticação, o responsável pelo tratamento tem de oferecer uma solução alternativa que não implique o tratamento biométrico – sem restrições ou custos adicionais para o titular dos dados. Esta solução alternativa também é necessária para as pessoas que não satisfaçam as condições do dispositivo biométrico (impossibilidade de inscrição ou leitura dos dados biométricos, situação de deficiência que dificulte a sua utilização, etc.), devendo, além disso, para um eventual caso de indisponibilidade do dispositivo biométrico (como uma avaria do dispositivo), ser implementada uma «solução de reserva» que assegure a continuidade do serviço proposto, limitada, contudo, a utilização em casos excecionais. Em casos excecionais, pode surgir uma situação em que o tratamento de dados biométricos seja a atividade central de um serviço contratualmente prestado, por exemplo, um museu que monta uma exposição para demonstrar o modo de utilização de um dispositivo de reconhecimento facial. Nesse caso, o titular dos dados não poderá rejeitar o tratamento dos dados biométricos caso deseje participar na exposição. Nesta situação, o consentimento exigido pelo artigo 9.º continua a ser válido se os requisitos do artigo 7.º forem cumpridos.

5.2 Medidas propostas para minimizar os riscos no tratamento de dados biométricos

87. Em conformidade com o princípio da minimização dos dados, os responsáveis pelo tratamento devem assegurar que os dados extraídos de uma imagem digital para construir um modelo não são excessivos e contêm apenas as informações necessárias para a finalidade especificada, evitando assim qualquer tratamento ulterior. Devem ser instituídas medidas para garantir que os modelos não podem ser transferidos através de sistemas biométricos.

88. É provável que a identificação e a autenticação/verificação exijam o armazenamento do modelo para utilização numa comparação posterior. O responsável pelo tratamento deve escolher o local mais apropriado para o armazenamento dos dados. Num ambiente sob controlo (átrios ou postos de controlo delimitados), os modelos devem ser armazenados num dispositivo individual guardado pelo utilizador e sob o seu controlo exclusivo (num *smartphone* ou no cartão de identificação) ou – quando necessário para fins específicos e na presença de necessidades objetivas – numa base de dados centralizada de forma cifrada e com uma chave/senha apenas do conhecimento da pessoa para impedir o acesso não autorizado ao modelo ou ao local de armazenamento. Se o responsável pelo

tratamento não puder evitar o acesso aos modelos, deve tomar medidas apropriadas para garantir a segurança dos dados armazenados. Tal poderá incluir a cifragem do modelo utilizando um algoritmo de encriptação.

89. Em todo o caso, o responsável pelo tratamento deve tomar todas as precauções necessárias para preservar a disponibilidade, a integridade e a confidencialidade dos dados tratados. Para o efeito, o responsável pelo tratamento deve, nomeadamente, adotar as seguintes medidas: compartimentar os dados durante a transmissão e o armazenamento, armazenar os modelos biométricos e os dados brutos ou dados de identidade em bases de dados distintas, cifrar os dados biométricos, nomeadamente modelos biométricos, e definir uma política de cifragem e gestão de chaves, integrar uma medida organizativa e técnica de deteção de fraude, associar um código de integridade aos dados (por exemplo, assinatura ou *hash*) e proibir qualquer acesso externo aos dados biométricos. Estas medidas terão de evoluir com o avanço das tecnologias.

90. Além disso, os responsáveis pelo tratamento devem proceder à eliminação dos dados brutos (imagens faciais, sinais vocais, marcha, etc.) e garantir a eficácia dessa eliminação. Se deixar de haver uma base lícita para o tratamento, os dados brutos têm de ser eliminados. Na verdade, na medida em que os modelos biométricos derivam desses dados, pode considerar-se que a constituição de bases de dados pode representar uma ameaça igual, ou até mesmo maior (porque pode nem sempre ser fácil ler um modelo biométrico sem o conhecimento do modo como foi programado, enquanto os dados brutos serão as peças constituintes de qualquer modelo). Caso o responsável pelo tratamento tenha de conservar esses dados, há que explorar métodos de ruídos aditivos (por exemplo, marca de água) para tornar a criação do modelo ineficaz. O responsável pelo tratamento também deve apagar os dados biométricos e os modelos em caso de acesso não autorizado ao terminal de comparação de leitura ou ao servidor de armazenamento e apagar quaisquer dados que não sejam úteis para o tratamento posterior no final da vida útil do dispositivo biométrico.

6 DIREITOS DO TITULAR DOS DADOS

91. Devido ao caráter do tratamento de dados quando se utiliza videovigilância, alguns direitos do titular dos dados ao abrigo do RGPD justificam uma maior clarificação. Contudo, este capítulo não é exaustivo, e todos os direitos previstos no RGPD são aplicáveis ao tratamento de dados pessoais através de videovigilância.

6.1 Direito de acesso

92. O titular dos dados tem o direito de confirmar, junto do responsável pelo tratamento, se os seus dados pessoais estão ou não a ser objeto de tratamento. No caso da videovigilância, isto significa que, se não houver qualquer tipo de conservação ou transferência de dados, uma vez passado o momento do controlo em tempo real, o responsável pelo tratamento só pode transmitir a informação de que já não estão a ser tratados dados pessoais (para além das obrigações gerais de informação previstas no artigo 13.º. Ver *secção 7 – Obrigações em matéria de transparência e informação*). Contudo, se os dados ainda estiverem a ser tratados no momento do pedido (ou seja, se os dados forem de algum outro modo conservados ou tratados de forma contínua), o titular dos dados deve obter acesso e informações em conformidade com o artigo 15.º.

93. Existem, no entanto, algumas limitações que, em alguns casos, podem aplicar-se em relação ao direito de acesso.

- Artigo 15.º, n.º 4, do RGPD – prejuízo dos direitos de terceiros

94. Uma vez que vários titulares de dados podem ser captados na mesma sequência de videovigilância, uma triagem implicaria o tratamento adicional de dados pessoais de outros titulares de dados. Se o titular dos dados desejar receber uma cópia do material (artigo 15.º, n.º 3), isso pode prejudicar os direitos e as liberdades de outros titulares dos dados que figurem nesse material. Para evitar esta situação, o responsável pelo tratamento deve ter em consideração que, em alguns casos, devido à natureza intrusiva das gravações de vídeo, não deve transmitir gravações a partir das quais seja possível identificar outros titulares de dados. A proteção dos direitos de terceiros não deve, contudo, ser utilizada como desculpa para impedir pedidos legítimos de acesso por parte de indivíduos, devendo o responsável pelo tratamento, nesses casos, aplicar medidas técnicas para satisfazer o pedido de acesso (por exemplo, edição de imagens, como mascaramento ou codificação). No entanto, os responsáveis pelo tratamento não são obrigados a aplicar estas medidas técnicas se puderem garantir, de outro modo, que são capazes de responder a um pedido nos termos do artigo 15.º dentro do prazo estipulado pelo artigo 12.º, n.º 3.

- Artigo 11.º, n.º 2, do RGPD – o responsável pelo tratamento não consegue identificar o titular dos dados

95. Se as gravações de vídeo não forem pesquisáveis para localizar dados pessoais (ou seja, o responsável pelo tratamento teria provavelmente de examinar uma grande quantidade de material armazenado para encontrar o titular dos dados em questão), o responsável pelo tratamento pode não conseguir identificar o titular dos dados.

96. Por estas razões, o titular dos dados deve (além de se identificar a si próprio, inclusive por meio de um documento de identificação ou pessoalmente), no seu pedido ao responsável pelo tratamento, especificar quando – dentro de um prazo razoável e proporcional à quantidade de titulares de dados registados – entrou na área sob vigilância. O responsável pelo tratamento deve

notificar previamente o titular dos dados sobre quais as informações de que precisa para responder ao pedido. Se o responsável pelo tratamento puder demonstrar que não está em condições de identificar o titular dos dados, deve informá-lo, se possível, desse facto. Nesta situação, na sua resposta ao titular dos dados, o responsável pelo tratamento deve informá-lo sobre a área exata sob vigilância, verificar as câmaras que estavam a ser utilizadas, etc., de modo que o titular dos dados tenha a plena compreensão de quais os dados pessoais que lhe dizem respeito que possam ter sido objeto de tratamento.

Exemplo: Se um titular dos dados solicitar uma cópia dos seus dados pessoais tratados através de videovigilância à entrada de um centro comercial com 30 000 visitantes por dia, deve especificar quando é que passou na área sob vigilância, num intervalo de aproximadamente uma hora. Se o responsável pelo tratamento ainda estiver a efetuar o tratamento do material, deve fornecer uma cópia das gravações de vídeo. Se outros titulares dos dados puderem ser identificados no mesmo material, então essa parte do material deve ser anonimizada (por exemplo, desfocando a cópia ou partes da mesma) antes de esta ser transmitida ao titular dos dados que apresentou o pedido.

Exemplo: Se apagar automaticamente todas as gravações, por exemplo no prazo de dois dias, o responsável pelo tratamento não pode fornecer as gravações ao titular dos dados após esses dois dias. Se o responsável pelo tratamento receber um pedido após esses dois dias, o titular dos dados deve ser informado desse facto.

97.

- Artigo 12.º do RGPD – pedidos excessivos

98. Em caso de pedidos excessivos ou manifestamente infundados de um titular dos dados, o responsável pelo tratamento pode exigir o pagamento de uma taxa razoável de acordo com o artigo 12.º, n.º 5, alínea a), do RGPD, ou recusar-se a dar seguimento ao pedido (artigo 12.º, n.º 5, alínea b), do RGPD). O responsável pelo tratamento tem de ser capaz de demonstrar o caráter manifestamente infundado ou excessivo do pedido.

6.2 Direito ao apagamento dos dados e direito de se opor

6.2.1 Direito ao apagamento dos dados (direito a ser esquecido)

99. Se o responsável pelo tratamento continuar a efetuar o tratamento de dados pessoais para além do controlo em tempo real (por exemplo, conservando os dados), o titular dos dados pode solicitar que os dados pessoais sejam apagados ao abrigo do artigo 17.º do RGPD.

100. Perante um pedido neste sentido, o responsável pelo tratamento é obrigado a apagar os dados pessoais sem demora injustificada se se aplicar uma das circunstâncias enumeradas no artigo 17.º, n.º 1, do RGPD (e nenhuma das exceções enumeradas no artigo 17.º, n.º 3, do RGPD). Tal inclui a obrigação de apagar os dados pessoais quando já não forem necessários para a finalidade para a qual foram inicialmente conservados, ou quando o tratamento for ilícito (ver também *secção 8 – Prazos de conservação e obrigação de apagamento*). Além disso, dependendo da base jurídica do tratamento, os dados pessoais devem ser apagados:

- por razões de *consentimento*, sempre que o consentimento seja retirado (e não exista outro fundamento jurídico para o tratamento),
- por razões de *interesse legítimo*:

- sempre que o titular dos dados exerça o direito de se opor (ver *secção 6.2.2*) e não existam interesses legítimos imperiosos prevalecentes que justifiquem o tratamento, ou
- em caso de comercialização direta (incluindo definição de perfis) sempre que o titular dos dados se oponha ao tratamento.

101. Se o responsável pelo tratamento tiver divulgado as gravações ao público (por exemplo, difundindo-as ou transmitindo-as em contínuo na Internet), é necessário tomar medidas razoáveis para informar outros responsáveis pelo tratamento (que estarão nessa altura a efetuar o tratamento dos dados pessoais em questão) sobre o pedido nos termos do artigo 17.º, n.º 2, do RGPD. As medidas razoáveis devem incluir medidas de caráter técnico, tendo em consideração a tecnologia disponível e o custo da sua aplicação. Na medida do possível, o responsável pelo tratamento deve notificar – após o apagamento dos dados pessoais – qualquer pessoa a quem os dados pessoais tenham sido anteriormente transmitidos, em conformidade com o artigo 19.º do RGPD.

102. Para além da obrigação de apagar os dados pessoais a pedido do titular dos dados, o responsável pelo tratamento também é obrigado, ao abrigo dos princípios gerais do RGPD, a limitar os dados pessoais conservados (ver *secção 8*).

103. No caso da videovigilância, importa salientar que, por exemplo, ao desfocar a imagem sem possibilidade de recuperação retroativa dos dados pessoais previamente nela contidos, os dados pessoais são considerados apagados em conformidade com o RGPD.

> Exemplo: Uma loja de conveniência tem tido problemas com vandalismo, sobretudo no exterior da loja, pelo que está a utilizar videovigilância do lado exterior da entrada que está em contacto direto com as paredes. Um transeunte solicita que os seus dados pessoais sejam apagados a partir desse preciso momento. O responsável pelo tratamento é obrigado a responder ao pedido sem demora injustificada e, no máximo, no prazo de um mês. Como as gravações em questão já não correspondem à finalidade para a qual foram inicialmente conservadas (não ocorreu vandalismo durante o tempo em que o titular dos dados passou pela loja), não existe, no momento do pedido, nenhum interesse legítimo em conservar os dados que prevaleça sobre os interesses dos titulares dos dados. O responsável pelo tratamento tem de apagar os dados pessoais.

104.

6.2.2 Direito de se opor

105. No caso da videovigilância baseada no *interesse legítimo* (artigo 6.º, n.º 1, alínea f), do RGPD) ou se o tratamento for necessário ao exercício de funções de *interesse público* (artigo 6.º, n.º 1, alínea e), do RGPD), o titular dos dados tem o direito de – a qualquer momento – se opor ao tratamento, por motivos relacionados com a sua situação particular, em conformidade com o artigo 21.º do RGPD. A menos que o responsável pelo tratamento apresente razões imperiosas e legítimas que prevaleçam sobre os direitos e interesses do titular dos dados, o tratamento dos dados do indivíduo que se opôs deve cessar. O responsável pelo tratamento deve ser obrigado a responder aos pedidos do titular dos dados sem demora injustificada e, no máximo, no prazo de um mês.

106. No contexto da videovigilância, esta oposição poderia ser feita à entrada, durante a permanência ou após a saída da área sob vigilância. Na prática, isto significa que, a menos que o responsável pelo tratamento apresente razões imperiosas e legítimas, a vigilância de uma área onde seja possível identificar pessoas singulares só é lícita se:

(1) O responsável pelo tratamento puder impedir imediatamente a câmara de tratar dados pessoais quando solicitado; ou

(2) A área sob vigilância estiver de tal modo limitada que o responsável pelo tratamento consiga obter a aprovação do titular dos dados antes de entrar na área e não se trate de uma área à qual o titular dos dados tenha direito de acesso como cidadão.

107. Está fora do âmbito destas diretrizes identificar o que se entende por interesse legítimo *imperioso* (artigo 21.º do RGPD).

108. Ao utilizar a videovigilância para fins de comercialização direta, o titular dos dados tem o direito de se opor ao tratamento numa base discricionária, uma vez que o direito de se opor é absoluto nesse contexto (artigo 21.º, n.^{os} 2 e 3, do RGPD).

> Exemplo: Uma empresa está com problemas relacionados com violações de segurança na sua entrada pública e está a utilizar videovigilância com base em motivos de interesse legítimo, com o objetivo de detetar os intrusos. Um visitante opõe-se ao tratamento dos seus dados através do sistema de videovigilância por motivos relacionados com a sua situação particular. No entanto, a empresa rejeita, neste caso, o pedido justificando que as imagens conservadas são necessárias no âmbito de uma investigação interna em curso, o que lhe confere razões imperiosas e legítimas para continuar a efetuar o tratamento dos dados pessoais.

109.

7 OBRIGAÇÕES EM MATÉRIA DE TRANSPARÊNCIA E INFORMAÇÃO[18]

110. Desde há muito que o direito europeu em matéria de proteção de dados pressupõe que os titulares dos dados devem ter conhecimento de que está implementada videovigilância, obtendo informações pormenorizadas sobre os locais sob vigilância[19]. No RGPD, as obrigações gerais em matéria de transparência e informação estão estabelecidas no artigo 12.º e seguintes. As «Orientações relativas à transparência na aceção do Regulamento 2016/679» (WP 260) do Grupo de Trabalho do Artigo 29.º, que foram aprovadas pelo CEPD em 25 de maio de 2018, contêm informações mais pormenorizadas. De acordo com o WP 260, n.º 26, é o artigo 13.º do RGPD que é aplicável se for efetuada recolha de dados pessoais «[...] junto de um titular dos dados através de observação (p. ex. utilizando dispositivos automatizados de captação de dados ou *software* de captação de dados como câmaras [...]».

111. Atendendo ao volume de informações que é necessário fornecer ao titular dos dados, os responsáveis pelo tratamento podem adotar uma abordagem estruturada quando escolhem utilizar uma combinação de métodos para garantir a transparência (WP 260, n.º 35; WP 89, p. 22). Em relação à videovigilância, as informações mais importantes devem ser apresentadas no próprio sinal de aviso (primeiro nível da estrutura), enquanto os detalhes adicionais obrigatórios podem ser fornecidos por outros meios (segundo nível).

7.1 Informações do primeiro nível (sinal de aviso)

112. O primeiro nível da estrutura diz respeito à forma inicial como o responsável pelo tratamento entra em contacto com o titular dos dados. Nesta fase, os responsáveis pelo tratamento podem usar um sinal de aviso que contenha as informações relevantes. Essas informações podem ser fornecidas em combinação com um ícone a fim de dar, de modo facilmente visível, inteligível e claramente legível, uma perspetiva geral significativa do tratamento previsto (artigo 12.º, n.º 7, do RGPD). O formato da informação deverá ser adaptado ao local em questão (WP 89, p. 22).

7.1.1 Posicionamento do sinal de aviso

113. A informação deve ser posicionada de tal forma que o titular dos dados possa reconhecer facilmente as circunstâncias da vigilância antes de entrar na área sob vigilância (aproximadamente ao nível dos olhos). Não é necessário revelar a posição exata da câmara de vigilância desde que os locais sob vigilância e o contexto da vigilância sejam inequivocamente esclarecidos (WP 89, p. 22). O titular dos dados deve ser capaz de estimar qual é a área captada por uma câmara, a fim de poder evitar a vigilância ou adaptar o seu comportamento, se necessário.

7.1.2 Conteúdo do primeiro nível da estrutura

114. O primeiro nível da estrutura (sinal de aviso) deve veicular em geral as informações mais importantes, designadamente informações pormenorizadas sobre as finalidades do tratamento, a identidade do responsável pelo tratamento e a existência dos direitos do titular dos dados, juntamente com informações sobre o tratamento com maior impacto[20]. Tal pode incluir, por exemplo, os interesses legítimos perseguidos pelo responsável pelo tratamento (ou por um terceiro) e os contactos do

[18] Poderão aplicar-se requisitos específicos previstos na legislação nacional.

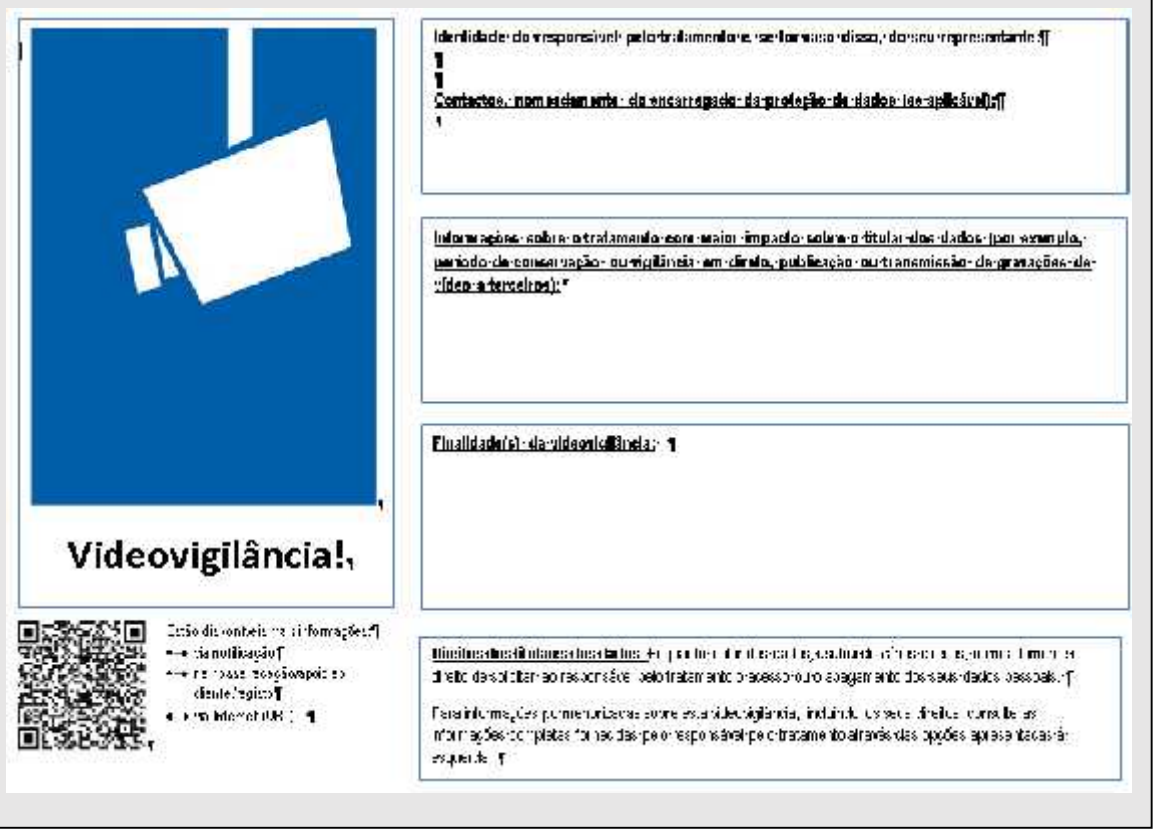
[19] Ver WP 89, Parecer 4/2004 sobre o Tratamento de Dados Pessoais por meio de Videovigilância, do Grupo de Trabalho do Artigo 29.º.

[20] Ver WP 260, n.º 38.

encarregado da proteção de dados (se for caso disso). Além disso, tem de fazer referência ao segundo nível da estrutura, mais pormenorizado, e ao local onde está disponível.

115. O sinal deve conter também informações sobre um eventual tratamento que possa vir a surpreender o titular dos dados (WP 260, n.º 38). Pode ser o caso, por exemplo, de transmissões a terceiros, sobretudo se estes estiverem localizados fora da UE, e sobre o prazo de conservação dos dados. Se estas informações não forem indicadas, o titular dos dados deve poder confiar que é efetuada apenas vigilância em direto (sem qualquer registo ou transmissão de dados a terceiros).

116. Exemplo (sugestão não vinculativa):



7.2 Informações do segundo nível

117. As informações do segundo nível também devem ser disponibilizadas num local facilmente acessível para o titular dos dados, por exemplo como uma ficha informativa completa disponível num local central (por exemplo, balcão de informação, receção ou caixa) ou incluídas num cartaz facilmente acessível. Como atrás se refere, o sinal de aviso do primeiro nível tem de fazer uma referência clara às informações do segundo nível. Além disso, é desejável que as informações do primeiro nível façam referência a uma fonte digital (por exemplo, código QR ou endereço de um sítio Web) do segundo nível. No entanto, as informações também devem ser facilmente acessíveis de forma não digital. Deve ser possível aceder às informações do segundo nível sem entrar na área sob vigilância, sobretudo se as informações forem fornecidas por via digital (por exemplo, através de uma hiperligação). Outro meio apropriado poderia ser um número de telefone. Independentemente do modo como é transmitida, a informação deve conter todos os elementos obrigatórios nos termos do artigo 13.º do RGPD.

118. Além destas opções, e também para as tornar mais eficazes, o CEPD promove o uso de meios tecnológicos para transmitir informações aos titulares dos dados. Estes podem incluir, por exemplo, câmaras de localização geográfica e a inclusão de informações em aplicações de mapas ou sítios Web para que os indivíduos possam facilmente, por um lado, identificar e especificar as fontes de vídeo relacionadas com o exercício dos seus direitos e, por outro lado, obter informações mais pormenorizadas sobre a operação de tratamento.

> Exemplo: O proprietário de uma loja efetua vigilância do seu estabelecimento. Para cumprir o artigo 13.º, é suficiente colocar um sinal de aviso num local bem visível, à entrada da sua loja, que contenha as informações do primeiro nível. Além disso, tem de fornecer uma ficha informativa que contenha o segundo nível de informação na caixa ou em qualquer outro local central e de fácil acesso no seu estabelecimento.

119.

8 PRAZOS DE CONSERVAÇÃO E OBRIGAÇÃO DE APAGAMENTO

120. Os dados pessoais não podem ser conservados por um período superior ao necessário para as finalidades para as quais são tratados (artigo 5.º, n.º 1, alíneas c) e e), do RGPD). Em alguns Estados-Membros, podem existir disposições específicas relativas aos prazos de conservação no que diz respeito à videovigilância, em conformidade com o artigo 6.º, n.º 2, do RGPD.

121. A necessidade ou não de conservar os dados pessoais deve ser determinada num prazo curto. As finalidades legítimas da videovigilância são, geralmente, a proteção da propriedade ou a preservação de provas. Normalmente, os danos ocorridos podem ser reconhecidos no prazo de um ou dois dias. Para facilitar a demonstração da conformidade com o quadro de proteção de dados, é do interesse do responsável pelo tratamento tomar antecipadamente medidas organizativas (por exemplo, nomear, se necessário, um representante para a análise e a proteção do material de vídeo). Tendo em consideração os princípios do artigo 5.º, n.º 1, alíneas c) e e), do RGPD, nomeadamente a minimização dos dados e a limitação da conservação, os dados pessoais devem, na maioria dos casos (por exemplo, para efeitos de deteção de vandalismo), ser apagados, de preferência automaticamente, após alguns dias. Quanto mais longo for o prazo de conservação definido (sobretudo quando ultrapassa as 72 horas), mais argumentos sobre a legitimidade da finalidade e a necessidade de conservação têm de ser apresentados. Se o responsável pelo tratamento, para além de utilizar a videovigilância para vigiar as suas instalações, também tencionar conservar os dados, deve assegurar que essa conservação é realmente necessária para atingir a sua finalidade. Se assim for, o prazo de conservação tem de ser claramente definido e estipulado individualmente para cada finalidade específica. Cabe ao responsável pelo tratamento definir o prazo de conservação em conformidade com os princípios da necessidade e da proporcionalidade e demonstrar o cumprimento das disposições do RGPD.

> Exemplo: O proprietário de uma pequena loja aperceber-se-ia normalmente de qualquer ato de vandalismo no próprio dia. Assim sendo, um prazo de conservação normal de 24 horas é suficiente. No entanto, os fins de semana ou férias mais prolongadas, em que a loja está fechada, poderiam ser argumentos a favor de um prazo de conservação mais longo. Se for detetado um dano, o proprietário também pode precisar de conservar as gravações por um período mais longo, a fim de tomar medidas judiciais contra o infrator.

122.

9 MEDIDAS TÉCNICAS E ORGANIZATIVAS

123. Tal como referido no artigo 32.º, n.º 1, do RGPD, para além de o tratamento de dados pessoais durante a videovigilância dever ser permitido por lei, os responsáveis pelo tratamento e os subcontratantes também devem garantir a sua segurança. As **medidas técnicas e organizativas** aplicadas devem ser **proporcionais aos riscos para os direitos e liberdades das pessoas singulares** resultantes de destruição, perda e alteração acidentais ou ilícitas, e da divulgação ou acesso não autorizados aos dados da videovigilância. De acordo com os artigos 24.º e 25.º do RGPD, os responsáveis pelo tratamento devem aplicar medidas técnicas e organizativas também para salvaguardar todos os princípios de proteção de dados durante o tratamento e estabelecer meios que permitam aos titulares dos dados exercerem os seus direitos definidos nos artigos 15.º a 22.º do RGPD. Os responsáveis pelo tratamento devem adotar um quadro e políticas a nível interno que garantam essa aplicação, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, incluindo a realização de avaliações de impacto da proteção de dados, quando necessário.

9.1 Síntese do sistema de videovigilância

124. Um sistema de videovigilância (SVV)[21] consiste em sistemas analógicos e digitais e *software* que captam imagens de uma cena, tratam as imagens e apresentam-nas a um operador. Os seus componentes estão agrupados nas seguintes categorias:

- Ambiente de vídeo: captação de imagens, interconexões e tratamento de imagens:
  - a finalidade da captação da imagem é a geração de uma imagem do mundo real num formato que possa ser utilizado pelo resto do sistema,
  - as interconexões descrevem todas as transmissões de dados dentro do ambiente de vídeo, ou seja, as conexões e comunicações. Exemplos de conexões são cabos, redes digitais e transmissões sem fio. As comunicações descrevem todos os sinais de vídeo e dados de controlo, que podem ser digitais ou analógicos,
  - o tratamento de imagens inclui a análise, o armazenamento e a apresentação de uma imagem ou de uma sequência de imagens.
- Do ponto de vista da gestão do sistema, um SVV tem as seguintes funções lógicas:
  - gestão de dados e gestão de atividades, incluindo o tratamento de comandos do operador e atividades geradas pelo sistema (procedimentos de alarme, alertas para os operadores),
  - interfaces com outros sistemas, que podem incluir a ligação a outros sistemas, de segurança (controlo de acesso, alarme de incêndio) ou não (sistemas de gestão de edifícios, reconhecimento automático de matrículas).
- A segurança do SVV consiste na confidencialidade, integridade e disponibilidade do sistema e dos dados:
  - a segurança do sistema inclui a segurança física de todos os seus componentes e o controlo do acesso ao SVV,
  - a segurança dos dados inclui a prevenção da perda ou da manipulação dos dados.

[21] O RGPD não contém uma definição de sistema de videovigilância. Pode ser encontrada uma descrição técnica, por exemplo, na norma EN 62676-1-1:2014 – Sistemas de videovigilância para utilização em aplicações de segurança eletrónica – Parte 1-1: Requisitos do sistema.

125.

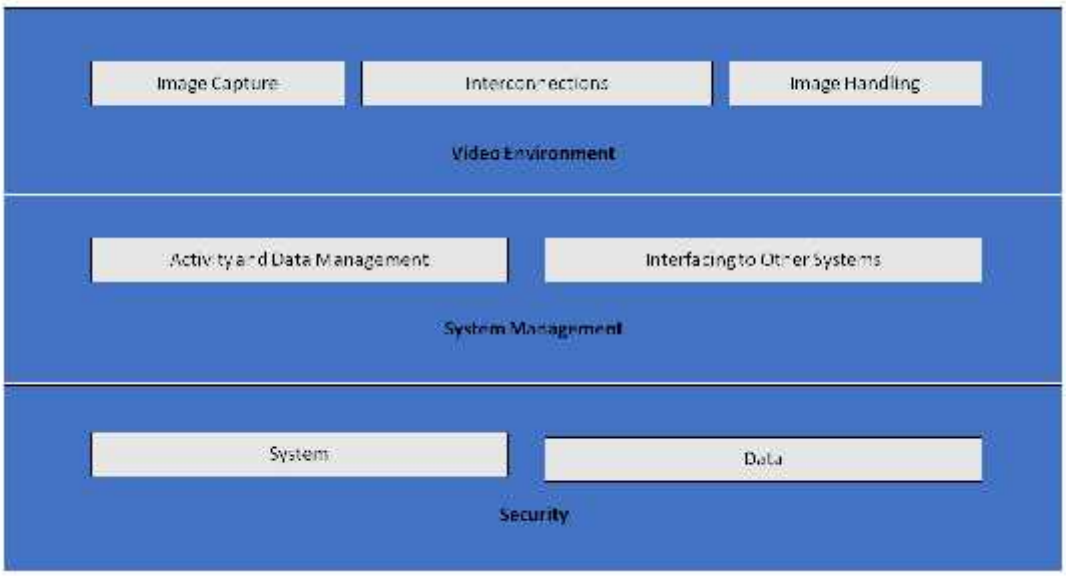


Image Capture	Captação de imagens
Interconnections	Interconexões
Image Handling	Tratamento de imagens
Video Environment	Ambiente de vídeo
Activity and Data Management	Gestão de atividades e dados
Interfacing to Other Systems	Interface com outros sistemas
System Management	Gestão do sistema
System	Sistema
Data	Dados
Security	Segurança

Figura 1 – Sistema de videovigilância

9.2 Proteção de dados desde a conceção e por defeito

126. Tal como referido no artigo 25.º do RGPD, os responsáveis pelo tratamento têm de aplicar medidas técnicas e organizativas adequadas de proteção dos dados logo que começam a planear a videovigilância – antes de iniciarem a recolha e o tratamento das gravações. Estes princípios enfatizam a necessidade de tecnologias integradas de reforço da privacidade, de configurações predefinidas que minimizem o tratamento dos dados e de instrumentos que permitam a proteção mais elevada possível dos dados pessoais[22].

127. Os responsáveis pelo tratamento devem integrar salvaguardas em matéria de proteção de dados e privacidade não só nas especificações de projeto da tecnologia, mas também nas práticas organizativas. No que diz respeito a estas últimas, o responsável pelo tratamento deve adotar uma estrutura de gestão apropriada e estabelecer e aplicar políticas e procedimentos relacionados com a videovigilância. Do ponto de vista técnico, a especificação e a conceção do sistema devem incluir requisitos em matéria de tratamento de dados pessoais em conformidade com os princípios

[22] WP 168, Parecer intitulado «The Future of Privacy» (O futuro da privacidade), contributo conjunto do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados e do Grupo de Trabalho «Polícia e Justiça» para a consulta da Comissão Europeia sobre o quadro jurídico do direito fundamental à proteção dos dados pessoais (adotado em 1 de dezembro de 2009).

enunciados no artigo 5.º do RGPD (licitude do tratamento, limitação das finalidades e dos dados, minimização dos dados por defeito na aceção do artigo 25.º, n.º 2, do RGPD, integridade e confidencialidade, responsabilidade, etc.). Caso planeie adquirir um sistema de videovigilância comercial, o responsável pelo tratamento tem de incluir estes requisitos na especificação de compra. O responsável pelo tratamento tem de garantir o cumprimento destes requisitos aplicando-os a todos os componentes do sistema e a todos os dados por ele tratados, durante todo o seu ciclo de vida.

9.3 Exemplos concretos de medidas pertinentes

128. A maioria das medidas que podem ser usadas para garantir uma videovigilância segura, especialmente quando são usados equipamentos digitais e *software*, não diferem das utilizadas noutros sistemas informáticos. Contudo, independentemente da solução escolhida, o responsável pelo tratamento deve proteger adequadamente todos os componentes de um sistema de videovigilância e dados em todas as etapas, ou seja, durante a conservação (dados em repouso), a transmissão (dados em trânsito) e o tratamento (dados em utilização). Para isso, é necessário que os responsáveis pelo tratamento e os subcontratantes combinem medidas organizativas e técnicas.

129. Aquando da escolha das soluções técnicas, o responsável pelo tratamento deve considerar tecnologias respeitadoras da privacidade, nomeadamente porque reforçam a segurança. Exemplos deste tipo de tecnologias são os sistemas que permitem o mascaramento ou a codificação de áreas que não sejam pertinentes para a vigilância, ou a remoção de imagens de terceiros, aquando da transmissão das gravações aos titulares dos dados[23]. Por outro lado, as soluções escolhidas não devem incluir funções que não sejam necessárias (por exemplo, movimentação ilimitada das câmaras, capacidade de *zoom*, transmissão de rádio, análise e gravações de áudio). As funções incluídas mas não necessárias devem ser desativadas.

130. Existe vasta literatura disponível sobre este tema, incluindo normas internacionais e especificações técnicas sobre a segurança física dos sistemas multimédia[24] e a segurança dos sistemas informáticos em geral[25]. Por conseguinte, a presente secção apresenta apenas uma síntese global sobre este tema.

9.3.1 Medidas organizativas

131. Para além de uma possível avaliação de impacto da proteção de dados necessária (ver *secção 10*), os responsáveis pelo tratamento devem ter em conta os seguintes temas quando criam as suas próprias políticas e procedimentos de videovigilância:

- Quem é responsável pela gestão e pela operação do sistema de videovigilância.
- Finalidade e âmbito de aplicação do projeto de videovigilância.
- Utilização adequada e proibida (onde e quando a videovigilância é permitida e onde e quando não o é; por exemplo, a utilização de câmaras ocultas e de gravação de áudio para além da gravação de vídeo)[26].

[23] A utilização destas tecnologias pode até ser obrigatória em alguns casos, a fim de assegurar o cumprimento do artigo 5.º, n.º 1, alínea c). Em todo o caso, podem servir como exemplos de boas práticas.

[24] IEC TS 62045 — Segurança multimédia – Orientações para a proteção da privacidade dos equipamentos e sistemas em utilização ou não.

[25] ISO/IEC 27000 — Série sobre sistemas de gestão da segurança da informação.

[26] Pode depender da legislação nacional e dos regulamentos do setor.

- Medidas em matéria de transparência, conforme mencionado na *secção 7 (Obrigações em matéria de transparência e informação).*
- De que modo o vídeo é gravado e por quanto tempo, incluindo o armazenamento em arquivo de gravações de vídeo relacionadas com incidentes de segurança.
- Quem deve fazer formação pertinente e quando.
- Quem tem acesso às gravações de vídeo e para que finalidades.
- Procedimentos operacionais (por exemplo, por quem e a partir de onde a videovigilância é controlada; o que fazer em caso de violação de dados).
- Que procedimentos as partes externas têm de seguir para solicitar gravações de vídeo, e quais os procedimentos para indeferir ou deferir esses pedidos.
- Procedimentos para aquisição, instalação e manutenção do SVV.
- Gestão de incidentes e procedimentos de recuperação.

9.3.2 Medidas técnicas

132. Por **segurança do sistema** entende-se a **segurança física** de todos os componentes do sistema e a respetiva integridade, ou seja, **proteção e resiliência contra interferência intencional e não intencional no seu funcionamento normal**, bem como **controlo do acesso**. Por segurança dos dados entende-se a **confidencialidade** (os dados são acessíveis apenas a indivíduos aos quais é concedido acesso), a **integridade** (prevenção contra perda ou manipulação dos dados) e a **disponibilidade** (acesso aos dados quando necessário).

133. A **segurança física** é uma parte vital da proteção de dados e a primeira linha de defesa, uma vez que protege os equipamentos de videovigilância contra furto, vandalismo, catástrofes naturais, catástrofes de origem humana e danos acidentais (por exemplo, devido a picos de corrente, temperaturas extremas e derrames de bebidas). No caso dos sistemas analógicos, a segurança física desempenha o papel principal na sua proteção.

134. A **segurança dos sistemas e dos dados**, ou seja, a proteção contra a interferência intencional e não intencional no seu funcionamento normal, pode incluir:

- A proteção de toda a infraestrutura do SVV (incluindo câmaras remotas, cabos e alimentação elétrica) contra adulteração física e furto.
- Proteção da transmissão de imagens com canais de comunicação seguros contra interceção.
- Cifragem dos dados.
- Utilização de soluções de *hardware* e *software*, tais como *firewalls*, antivírus ou sistemas de deteção de intrusões contra ciberataques.
- Deteção de falhas de componentes, *software* e interconexões.
- Meios para restaurar a disponibilidade e o acesso ao sistema no caso de um incidente físico ou técnico.

135. O **controlo do acesso** garante que apenas pessoas autorizadas podem aceder ao sistema e aos dados, sendo as restantes pessoas impedidas de o fazer. As medidas que apoiam o controlo do acesso físico e lógico incluem:

- Garantir que todas as instalações onde é efetuado o controlo por videovigilância e onde as gravações de vídeo são armazenadas estão protegidas contra o acesso não supervisionado por terceiros.
- Posicionar os monitores (especialmente quando se encontram em espaços abertos, como uma receção) de forma a apenas poderem ser vistos por operadores autorizados.
- Os procedimentos de concessão, alteração e revogação do acesso físico e lógico são definidos e aplicados.

- São implementados métodos e meios de autenticação e autorização dos utilizadores, incluindo, por exemplo, o comprimento das palavras-passe e a frequência com que são alteradas.
- As ações executadas pelo utilizador (tanto no sistema como em relação aos dados) são registadas e revistas regularmente.
- A monitorização e deteção de falhas de acesso é assegurada continuamente e as lacunas identificadas são resolvidas o mais rapidamente possível.

10 AVALIAÇÃO DE IMPACTO DA PROTEÇÃO DE DADOS

136. Nos termos do artigo 35.º, n.º 1, do RGPD, os responsáveis pelo tratamento devem proceder a avaliações de impacto da proteção de dados (AIPD) quando um certo tipo de tratamento for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares. O artigo 35.º, n.º 3, alínea c), do RGPD estipula que os responsáveis pelo tratamento são obrigados a realizar avaliações de impacto da proteção de dados se o tratamento constituir um controlo sistemático de zonas acessíveis ao público em grande escala. Além disso, de acordo com o artigo 35.º, n.º 3, alínea b), do RGPD, também é necessária uma avaliação de impacto da proteção de dados quando o responsável pelo tratamento tenciona efetuar o tratamento em grande escala de categorias especiais de dados.

137. As Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados[27] contêm aconselhamento adicional, bem como exemplos mais pormenorizados pertinentes para a videovigilância (por exemplo, relacionados com a «[u]tilização de um sistema de câmaras para controlar o comportamento dos condutores nas autoestradas»). O artigo 35.º, n.º 4, do RGPD exige que cada autoridade de controlo publique uma lista dos tipos de operações de tratamento sujeitos ao requisito de AIPD no seu país. Estas listas estão normalmente disponíveis nos sítios Web das autoridades. Tendo em conta as finalidades típicas da videovigilância (proteção de pessoas e bens; deteção, prevenção e controlo de infrações; recolha de provas e identificação biométrica de suspeitos), é razoável presumir que muitos casos de videovigilância exigirão uma AIPD. Assim, os responsáveis pelo tratamento devem consultar cuidadosamente estes documentos para determinar se essa avaliação é necessária e, em caso afirmativo, para a realizar. O resultado da AIPD realizada deve determinar a escolha do responsável pelo tratamento em relação às medidas de proteção de dados aplicadas.

138. É igualmente importante observar que, se os resultados da AIPD indicarem que o tratamento é suscetível de resultar num risco elevado apesar das medidas de segurança previstas pelo responsável pelo tratamento, será necessário consultar a autoridade de controlo competente antes de efetuar o tratamento. O artigo 36.º contém informações pormenorizadas sobre as consultas prévias.

Pelo Comité Europeu para a Proteção de Dados

A Presidente

(Andrea Jelinek)

[27] WP 248 rev.01, Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679. – aprovadas pelo CEPD