REVISTA DA EMERJ

ASPECTOS DA PRIVACIDADE NA SOCIEDADE DE VIGILÂNCIA: PROTEÇÃO DE DADOS E SISTEMAS DE VIDEOMONITORAMENTO

Privacy aspects in the surveillance society: data protection and video surveillance systems

Ana Flávia Sales Moreira*
Andréa Cristiane Sales Moreira**
Clarisse Sales Moreira***

Resumo: O presente trabalho busca analisar a relevância e as repercussões da proteção de dados pessoais na prática da videovigilância, considerada uma das mais genuínas expressões da sociedade de vigilância. Para tal, parte de uma análise comparativa do desenvolvimento da sociedade de vigilância e da área de proteção de dados pessoais, em conjunto com o exame das diversas funcionalidades decorrentes do videomonitoramento, expondo a tensão orgânica entre os três elementos. Superada essa questão, o presente trabalho dedica-se ao contexto normativo aplicável ao videomonitoramento no ordenamento jurídico nacional e europeu. Por fim, deslinda as principais controvérsias resultantes da aplicação dos preceitos de proteção de dados à videovigilância, bem como analisa os desdobramentos práticos dessa relação, com base nas orientações emitidas no contexto europeu de proteção de dados.

Palavras-chave: proteção de dados pessoais; privacidade; videomonitoramento; Circuito Fechado de TV; sociedade de vigilância.

Abstract: The present work seeks to analyze the implications and relevance of data protection law in the practice of video surveillance, an instrument considered one of the clearest displays of the surveillance society. For this purpose, the study conducts a comparative analysis of the development of surveillance society and data protection, along with the assessment of the various functions related to video surveillance, exposing the organic tension between these three elements. Furthermore, it analyzes the legislation applicable to video monitoring in the Brazilian and European legal systems. Finally, it unravels the main case-law regarding the application of data protection to video surveillance in Europe and Brazil, as well as tackles the practical consequences of the enforcement of the discussed legislation, based on the guidelines issued by European data protection institutions.

Keywords: data protection; privacy; video surveillance; Closed Circuit Television; surveillance society.

* Mestre em Direito e Business pela Universidade Bucerius Law School na Alemanha.
** Mestre em Sistema de Gestão Ambiental pela Universidade Federal Fluminense (UFF).
*** Especialista em Direito Público e Privado pela Escola da Magistratura do Estado do Rio de Janeiro (EMERJ).

Submissão em: 07/02/2024 | Aprovação em: 25/07/2024 e 27/11/2024
Editor: Antonio Aurélio Abi Ramia

INTRODUÇÃO

O videomonitoramento é parte incontestável da vida moderna, tornando-se elemento esperado da "paisagem social" (Machado, 1990, p.24) contemporânea. Os sistemas de videovigilância são empregados tanto pelo setor público quanto privado numa variedade de locais: desde aeroportos, vias públicas e bancos; até centros comerciais, ambientes de trabalho, escolas e padarias. Esse é o cenário da vigilância líquida descrita por Zygmunt Bauman (2014), no qual o monitoramento torna-se "dimensão-chave do mundo moderno". O presente trabalho tem como base principal a monografia da autora Ana Flávia Sales Moreira, defendida na Universidade do Estado do Rio de Janeiro, no ano de 2021.

Segundo os autores Fréderic Dufaux e Touradj Ebrahimi (2006), se por um lado as pessoas valorizam a sensação de segurança trazida pelo uso desses sistemas, por outro, há um receio em relação à perda de privacidade.

Em 2018, com a aprovação da Lei nº 13.709 – a Lei Geral de Proteção de Dados –, e sua posterior entrada em vigor em setembro de 2020, o Brasil entrou na lista de jurisdições que possuem um diploma legal acerca da proteção de dados pessoais.

Nesse sentido, vivemos um cenário aparentemente paradoxal no país: enquanto realizamos progressos inéditos na seara da proteção de dados, também vivemos em um frágil estado de segurança pública, o qual faz indivíduos e organizações recorrerem a mecanismos de mitigação que dependem do tratamento frequentemente exacerbado de dados pessoais. O videomonitoramento é um dos mais comuns desses instrumentos, materializado por diversas ferramentas como o Circuito Fechado de Televisão (CFTV), câmeras de celulares, *webcams*, *dashcams*, etc. Outrossim, a utilização dessas ferramentas também pode adquirir caráter econômico, especialmente no âmbito do tratamento de dados biométricos.

Como elementos pertencentes à realidade da sociedade contemporânea, sistemas de videovigilância estão presentes em todo o mundo e tornaram-se quase indispensáveis para seus usuários, sejam eles organizações governamentais, empresas ou pessoas físicas. A importância prática dessas ferramentas não pode ser negada, mas é necessário reconhecer que a utilização irrestrita do videomonitoramento pode gerar impactos significativos a direitos fundamentais dos cidadãos.

Como seu nome já antecipa, a Lei Geral de Proteção de Dados (LGPD) é uma lei de caráter generalista. Em sua estrutura, a lei traz o referencial normativo essencial para a compreensão e organização do tema da proteção de dados no Brasil.

Nessa conjuntura, a Autoridade Nacional de Proteção de Dados (ANPD) brasileira publicou, no dia 28 de outubro de 2021, no Diário Oficial da União, a Resolução CD/ANPD nº 01, que dispõe sobre a atividade de fiscalização da adequação à LGPD. Este trabalho se propõe a estudar os limites

do tratamento de dados pessoais por meio do videomonitoramento. A experiência europeia será essencial para esse fim.

O primeiro capítulo dedica-se a um estudo interseccional da vigilância e da proteção de dados, buscando analisar o cenário no qual ambos os fenômenos se desenvolveram, bem como elucidar o papel da videovigilância nesse contexto.

No segundo capítulo, objetiva-se examinar um breve panorama do contexto legislativo brasileiro e europeu de proteção de dados pessoais em relação ao videomonitoramento.

Por fim, o terceiro capítulo analisa as tentativas de respostas jurídicas ao uso do videomonitoramento no mundo factual, com levantamento de casos relevantes no âmbito da jurisdição europeia e brasileira.

1 A ASCENSÃO DA PRIVACIDADE NA SOCIEDADE DE VIGILÂNCIA

Sociedades de vigilância consistem em sociedades cujo funcionamento depende essencialmente da extensa coleta e do processamento sistemático de informações dos indivíduos e organizações a elas pertencentes (The Surveillance Studies Network, 2016). No ambiente acadêmico, o termo foi cunhado pelo professor Gary Marx (1985) e, posteriormente, desdobrou-se no principal objeto de uma ampla categoria de estudos *interdiEu to sciplinares* denominados “estudos sobre a vigilância”

Diversas atividades comuns no dia a dia classificam-se como vigilância, a exemplo de programas de fidelidade, monitoramento de movimentações financeiras, coleta de *cookies* e o videomonitoramento (Wood, 2006). Na realidade, todo ato de comunicação eletrônica contém um aspecto de vigilância, pois tudo que fazemos é registrado: desde a efetuação de ligações ao uso de cartões de créditos, e até mesmo o aluguel de um livro numa biblioteca. Embora seja um elemento anterior à modernidade, com o auxílio de novas tecnologias, a vigilância tornou-se um aspecto corriqueiro do gerenciamento da vida moderna (Lyon, 1994, p.4).

A vigilância é uma prática complexa: se por um lado confere maior eficiência ao funcionamento de organizações e à persecução de interesses públicos, por outro, trata-se de um poderoso mecanismo de controle social que – quando indevidamente implementado ou regulamentado – pode ensejar uma série de violações a direitos fundamentais.

A expansão do videomonitoramento por meio dos sistemas de Circuito Fechado de Televisão (CFTV) é uma das manifestações mais claras da sociedade de vigilância. Naturalmente, a primeira função associada ao videomonitoramento é a prevenção e o controle do crime e a segurança nacional. A ferramenta é considerada um dos principais mecanismos contra ameaças à segurança disponíveis atualmente (Young, 2015, p.359). Contudo, o barateamento e a expansão dessa tecnologia a tornou

acessível de modo a sair da esfera da segurança pública e privada, adentrando diversas outras áreas, do gerenciamento familiar e trabalhista à publicidade.

Ainda, o monitoramento por câmeras adotou uma face mais sofisticada por meio de novas tecnologias, tais como o reconhecimento facial, o uso de mapas de calor e as ferramentas de geolocalização. A videovigilância também possui meios além do uso do CFTV, podendo ser conduzida por intermédio de câmeras de celulares; *webcams*; *dashcams*; e, mais recentemente, *drones*, tecnologia utilizada para diversas finalidades de vigilância: conflitos bélicos, segurança pública (G1, 2019), monitoramento de comportamentos antissociais, como aglomerações na pandemia de covid-19 (Normand, 2020), e até mesmo investigações de evasão fiscal (Guichard, 2018).

Concomitantemente, destaca-se uma tendência mundial de maior preocupação com a salvaguarda à privacidade, em particular no âmbito da proteção de dados pessoais. Por conseguinte, observa-se a crescente introdução de legislação dispondo sobre a proteção de dados pessoais. Até janeiro de 2020, 142 países possuem leis de proteção de dados pessoais (Greenleaf; Cottier, 2020, p.24).

Nesse sentido, a realidade contemporânea compreende diversos aspectos não muito distantes das sociedades distópicas retratadas por autores como Franz Kafka em *O Processo*; George Orwell em *1984* e Aldous Huxley em *Admirável Novo Mundo*, mas também adota salvaguardas que buscam a limitação dessa intensa prática de vigilância. A tensão orgânica entre privacidade e vigilância é mais evidente do que nunca.

2 O VIDEOMONITORAMENTO NA LGPD E GDPR: VIDEOMONITORAMENTO NOS SISTEMAS LEGAIS BRASILEIRO E EUROPEU

2.1 Breve panorama do videomonitoramento nos sistemas legais brasileiro e europeu

Diante do contexto de vigilância, privacidade e proteção dos dados pessoais examinados no capítulo anterior, a instituição de leis sobre a matéria adquiriu uma importância ainda maior no século XXI. A União Europeia, após décadas de evolução legislativa, aprovou em 2016 o que seria o mais amplo regulamento do bloco sobre a matéria de proteção de dados pessoais.

A entrada em vigor do General Data Protection Regulation (GDPR) gerou um “efeito dominó” (Pinheiro, 2018, p.14) no contexto legislativo de proteção de dados mundial, dado que a sua aplicação se estende a toda organização ou indivíduo que trate dados de pessoas físicas localizadas na União Europeia, a despeito da nacionalidade dessas.

> Este [GDPR], por sua vez, ocasionou um "efeito dominó", visto que passou a exigir que os demais países e as empresas que buscassem manter relações comerciais com a UE também deveriam ter uma legislação de mesmo nível que o GDPR. Isso porque o Estado que não possuísse lei de mesmo nível passaria a poder sofrer algum tipo de barreira econômica ou dificuldade de fazer negócios com os países da UE. Considerando o contexto econômico atual, esse é um luxo que a maioria das nações, especialmente as da América Latina, não poderia se dar (Pinheiro, 2018, p.14).

Logo, o GDPR se aplicará também a organizações que operem fora da UE, desde que ofereçam serviços que impliquem no tratamento de dados de pessoas localizadas no território do bloco.

A aplicação extraterritorial do regulamento exigiu que toda empresa que oferecesse serviços ao mercado europeu estivesse em conformidade com o GDPR, afetando diretamente a economia global. O GDPR tornou-se a principal referência regulatória mundial no âmbito da proteção de dados pessoais. Essa conjuntura aumentou a pressão para aprovação de um regulamento nacional, que resultou na aprovação da LGPD em 10 de julho de 2018, a qual adotou como base o modelo europeu de proteção de dados pessoais.

> Tais elementos aumentaram a pressão não só para a aprovação da lei geral, mas também moldaram as discussões que culminaram numa redação muito similar à GDPR, até mesmo superior em alguns pontos, como na abordagem dada a dados anonimizados quando estes forem utilizados para a formação de perfis comportamentais (Leite, 2018).

No plano do videomonitoramento, a Europa possui histórico legislativo mais robusto, relacionando a videovigilância e a proteção de dados pessoais. Embora o GDPR tenha entrado em vigor em 2018, com base na antecessora Diretiva 95/46/CE, o bloco já possuía diretrizes[1] e jurisprudência sobre a questão antes mesmo da aprovação do regulamento. O Reino Unido – o país ocidental com o maior número de câmeras de monitoramento (Bischoff, 2021) – possui uma entidade específica para garantir que a videovigilância ocorra em conformidade com os códigos de conduta ingleses (Surveillance Camera Commissioner, [201-?]).

Historicamente, as tentativas de legislar sobre o videomonitoramento no Brasil são orientadas por uma visão expansiva do uso da ferramenta (Firmino *et al.*, 2013).

A legislação existente é esparsa, preponderante no nível estadual e municipal, e apresenta o videomonitoramento como um mecanismo neutro e necessário para a promoção de segurança pública no país, regulamentando somente os aspectos técnicos decorrentes do emprego dessa tecnologia. De antemão, observa-se a ausência de referências acerca da proteção dos sujeitos do monitoramento, ou seja, dos titulares dos dados pessoais.

A realidade da videovigilância no Brasil revela-se ainda mais contrastante diante da ausência de regulamentação acerca dos limites da prática. A tendência é que a presença das câmeras de

[1] *Cf.* The EDPS Video-Surveillance Guidelines, 2010; EDPS Follow Up Report, 2013.

monitoramento siga um crescimento exponencial, a exemplo do PL nº 5662/19, que busca tornar obrigatória a instalação de sistemas de videomonitoramento em municípios cuja população supere 30 mil habitantes (Brasil, 2019), e o PL nº 42/20 (Ceará, 2020), que propõe o compartilhamento simultâneo das imagens capturadas pelo videomonitoramento na esfera privada para auxiliar a ação policial cearense. São Paulo segue como a cidade com o maior número de câmeras, sendo apurada a existência de pelo menos 1,5 milhão de câmeras na capital paulista (Lepri, 2013), além de um sofisticado sistema de auxílio ao monitoramento (Portal do Governo [SP], 2017).

Com a introdução da LGPD, os tempos de emprego irrestrito do videomonitoramento chegaram a seu fim. A LGPD foi um divisor de águas no campo da proteção de dados no Brasil, trazendo princípios que irradiam para toda operação de tratamento de dados pessoais, além de direitos dos titulares e responsabilidades dos agentes de tratamento que afetam diretamente a utilização do videomonitoramento (Mendes, 2019, p. 42).

2.2 A experiência europeia

Enquanto o Brasil possuía regulamentação majoritariamente técnica até a introdução da LGPD, o videomonitoramento no contexto da proteção de dados pessoais é parte da discussão legislativa europeia desde os anos 1980, com a celebração da Convenção 108 do Conselho da Europa (Lim, 2010).

Antes da introdução do GDPR, a União Europeia já possuía a Diretiva 95/46/CE, na qual princípios relativos à proteção de dados como conhecemos hoje já eram previstos.

O GDPR foi promulgado devido à necessidade de atualização da Diretiva 95/46/CE em face do advento de novas tecnologias que alteraram os meios de tratamento de dados pessoais (Šidlauskas, 2019, p. 60). Como adiantado, um dos principais impactos do novo regulamento decorre de sua extensa aplicação extraterritorial, afetando todas as organizações que tratam dados de pessoas localizadas no território do bloco.

> Diferentemente da Diretiva, a Regulação é autoaplicável e não requer a aprovação de leis nacionais compatíveis com suas determinações. Seu objetivo é eliminar inconsistências em leis nacionais, ampliar o escopo de proteção à privacidade e modernizar a legislação para desafios tecnológicos, econômicos e políticos atuais, como aqueles decorrentes do advento da internet (Vainzof, 2019, p. 22).

Além disso, diversos códigos de conduta e leis nacionais anteriores ao GDPR já regulamentavam a prática (Lim, 2010), destacando-se a legislação britânica.

Em linhas gerais, esta seção se dedica a (i) analisar o tratamento dado pelo GDPR em relação à videovigilância e (ii) mapear as principais diretrizes elaboradas no contexto europeu, seja no contexto do bloco, seja das autoridades de proteção de dados nacionais.

2.2.1. Tratamento do GDPR

Como antecipado, o Brasil adotou o modelo europeu de proteção de dados, com base em diplomas como a Convenção 108, a Diretiva 46/95/CE e no próprio GDPR (Mendes; Doneda, 2018, p.470). Por esse motivo, a LGPD e o GDPR possuem diversas semelhanças. Nesse sentido, a experiência europeia é de notória relevância para a compreensão da legislação brasileira.

Dentre as semelhanças, observa-se a definição de dados pessoais, a categoria especial de dados sensíveis, os fundamentos e a aplicabilidade das leis. Destaca-se que, em seu art. 2 (2), o GDPR exclui de seu âmbito de aplicação o tratamento de dados pessoais para fins exclusivamente particulares[2] ou relacionados à segurança pública e persecução penal.

Contudo, a não aplicação do GDPR à utilização de dados no âmbito exclusivamente particular pode ser excepcionada na hipótese de videomonitoramento doméstico desproporcional, ou seja, quando as câmeras utilizadas extrapolarem os limites da residência e filmarem outros locais, como vias públicas, violando o princípio da finalidade e da necessidade.

Nesse sentido, essa situação se tornou um dos objetos mais recorrentes de aplicação de multas pelas entidades europeias. Essa questão é de notória relevância para a compreensão do âmbito de aplicação da LGPD.

Notadamente, a experiência europeia se diferencia na questão da proteção de dados no âmbito da segurança pública e persecução penal. Enquanto o Brasil encontra-se num vácuo legislativo devido à ausência de lei, a União Europeia não enfrentou a mesma situação, tendo promulgado lei específica sobre a matéria em 2016, a Diretiva 2016/680/CE, simultaneamente com a aprovação do GDPR.

O artigo 5 (1) (b) do GDPR exige que as finalidades de toda a operação de tratamento sejam definidas detalhadamente, sendo descrições genéricas ou indeterminadas proibidas pelo regulamento. Em relação às bases legais previstas, o GDPR possui um rol mais estrito, totalizando seis bases legais, em comparação com as dez hipóteses da lei brasileira. Nos termos de seu art. 6º, o regulamento europeu delimita as seguintes hipóteses autorizativas: (i) obtenção de consentimento do titular; (ii) execução de um contrato do qual o titular é parte; (iii) cumprimento de obrigação legal pelo controlador; (iv) persecução de interesse público ou tarefa de autoridade oficial; (v) proteção de interesses vitais do titular ou de terceiros; e (vi) interesse legítimo do controlador.

> Na teoria, nos mesmos contornos da lei brasileira, toda base legal pode fundamentar o tratamento de dados decorrente da videovigilância. Contudo, como apontado pelo Conselho Europeu de Proteção de Dados (EDPB), as duas hipóteses mais comuns são (i) o legítimo interesse; e (ii) a necessidade de executar uma tarefa para persecução de interesse público ou no exercício de uma autoridade oficial (European Data Protection Board, 2020, p. 9, §16).

[2] O termo utilizado pelo GDPR é o "processamento de dados pessoais por indivíduos para fins puramente pessoais ou domésticos".

Assim como na LGPD, a base legal do legítimo interesse no regulamento europeu exige a condução do teste do legítimo interesse, que consiste na avaliação da finalidade do tratamento; do balanceamento dos interesses do controlador e do titular; e da adoção de salvaguardas para a mitigação dos riscos do tratamento. Ademais, as condições de aplicação da base legal da execução de políticas públicas poderão ser especificadas nas leis nacionais dos Estados-Membros (European Data Protection Board, 2020 p. 13, §42).

Destaca-se que a eventual divulgação das imagens captadas por câmeras de monitoramento será considerada uma operação de tratamento autônoma sob o regulamento, exigindo uma base legal específica para autorizá-la. Tal exigência se aplica independentemente dos destinatários da divulgação, sejam eles particulares ou instituições estatais.

Quando o videomonitoramento for utilizado para deduzir dados sensíveis, o controlador deverá observar não somente o art. 6º, mas também o art. 9(2) do GDPR, o dispositivo que define as hipóteses excepcionais que autorizam o processamento dessa categoria de dados. O EDPB recomenda que, mesmo com a obtenção de consentimento do titular, o controlador observe o princípio de minimização de dados, reduzindo a coleta ao estritamente necessário.

> 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 (European Data Protection Board, 2020 p. 17, §68).

Para a qualificação de tratamento de dados biométricos, o art. 9º, em conjugação com a definição do art. 4.14 da lei europeia, exigem que tais dados sejam utilizados "para identificar uma pessoa de forma inequívoca" (European Data Protection Board, 2020 p. 18, §75). Segundo o EDPB (2020, p. 18, §77), esse tipo de tratamento, quando conduzido por empresas particulares para fins próprios, exigirá a obtenção de consentimento explícito do titular na maioria dos casos. O videomonitoramento conjugado com a coleta de dados biométricos – ou seja, quando a finalidade da atividade é identificar uma pessoa de forma inequívoca – exigirá que a operação seja amparada por uma base legal nos termos do art. 9(2) do GDPR. A título exemplificativo, não basta obter o consentimento de apenas algumas pessoas para garantir a licitude do tratamento. O EDP (2020, p. 21, §85) descreve o exemplo de um hotel que utiliza a tecnologia de reconhecimento facial para alertar ao gerente a chegada de hóspedes *VIPs*, os quais consentiram explicitamente para tal tratamento ao registrarem seus dados biométricos previamente à hospedagem. Esses sistemas somente poderiam ser lícitos caso todos os hóspedes, além dos *VIPs*, consentissem explicitamente para a operação.

Uma distinção importante entre a LGPD e o GDPR diz respeito à necessidade de elaboração de relatório de impacto à proteção de dados pessoais, denominado *Data Protection Impact*

Assessment (DPIA), na legislação europeia. Embora ambas as leis mencionem o documento e seu conteúdo mínimo, a LGPD somente dispõe sobre a possibilidade de solicitação do DPIA pela ANPD, enquanto o GDPR delimita as situações nas quais sua elaboração será obrigatória.

Segundo o GDPR, será necessária a feitura de DPIA nas seguintes hipóteses: (i) quando o tratamento for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas naturais; (ii) quando ocorre uma análise ampla e sistemática de aspectos pessoais relacionados a pessoas naturais, baseada em tratamento automatizado; (iii) no tratamento em grande escala de dados sensíveis; (iv) no monitoramento sistemático de uma área acessível ao público em grande escala. Notadamente, devido à natureza do videomonitoramento, reconhece-se que diversas hipóteses de uso da ferramenta exigirão um DPIA (European Data Protection Board, 2020 p. 33, §137).

Devido à generalidade proposital do GDPR, as autoridades de proteção de dados europeias emitiram uma série de diretrizes acerca de como o tratamento de dados pessoais deve proceder ao utilizar câmeras de segurança em ambientes públicos e privados. Esse arcabouço regulatório será abordado no próximo item.

2.2.2. Diretrizes regionais e nacionais

Antes mesmo da promulgação do GDPR, a Europa já possuía extenso arcabouço normativo especificamente dispondo sobre sistemas de videomonitoramento.

Em 2010, sob a vigência da Diretiva 95/46/CE, a Autoridade Europeia para a Proteção de Dados (EDPS), autoridade de proteção de dados independente da União Europeia, responsável por monitorar e implementar a legislação de proteção de dados e privacidade no âmbito de instituições e órgãos do bloco, emitiu diretrizes direcionadas ao videomonitoramento (The European Data Protection Supervisor, 2010). O documento estabelece parâmetros de grande relevância atual para a videovigilância, tais como orientações sobre *privacy by design*; escolha da base legal adequada; avaliação do risco de implementação da prática; prazo de retenção das gravações, medidas de segurança; como proceder em face da requisição de informações por titulares e até mesmo modelos para auxiliar a elaboração de políticas e códigos de conduta sobre o tema. Em 2013, a EDPS publicou um relatório realizando uma comparação sistemática de como as instituições europeias implementaram as orientações do documento de 2010 (The European Data Protection Supervisor, 2013).

No âmbito do Conselho da Europa[3], diversas resoluções foram publicadas acerca do tema, a exemplo de resoluções sobre o videomonitoramento em áreas pública (Council Of Europe, 2008) e

[3] Destaca-se que o Conselho da Europa não é órgão integrante da União Europeia e não deve ser confundido com o Conselho Europeu, órgão executivo do bloco. O Conselho da Europa é composto por 47 países e abarca, notadamente, a

no âmbito de investigações criminais (Council Of Europe, 2017), além de diretrizes sobre o uso de reconhecimento facial (Council Of Europe, 2021).

Após a promulgação do GDPR, o documento regulatório de maior relevância sobre o tema são as "Diretrizes 3/2019 sobre tratamento de dados pessoais através de dispositivos de vídeo" (European Data Protection Board, 2020), emitidas pelo Conselho Europeu de Proteção de Dados[4] (EDPB) em 2019, e posteriormente atualizadas em janeiro de 2020.

No plano nacional, as autoridades de proteção de dados de diversos países também publicaram orientações ou códigos de conduta específicos para a operacionalização da videovigilância. Destacam-se as diretrizes emitidas pelas autoridades de proteção de dados da Alemanha (LfDI, 2020)[5], Irlanda (Data Protection Commission, [20--?]), Eslovênia (Information Commissioner, 2019), Gibraltar (Gilbratar Regulatory Authority, 2020), entre muitos outros.

Destaca-se que, em alguns países, as autoridades atuam de forma incisiva sobre a videovigilância. A título exemplificativo, em Portugal, antes da promulgação do GDPR, a instalação de sistemas de videomonitoramento de grande escala exigia a autorização da Comissão Nacional de Proteção de Dados (CNPD, 2020). Embora tal autorização não seja mais necessária, o CNPD continua contribuindo para a fiscalização da atividade.

Notadamente, como adiantado, o Reino Unido possui ampla regulamentação sobre sistemas de videomonitoramento, incluindo uma organização exclusivamente responsável pela fiscalização da prática no país, denominada *Surveillance Camera Commissioner*. O órgão possui um código de conduta (Surveillance Camera Commissioner, 2013), ferramentas de autoavaliação e outras instruções destinadas a temas mais específicos, como o uso da tecnologia de reconhecimento facial por autoridades policiais (Surveillance Camera Commissioner, 2020). Para tanto, a *Information Commissioner's Office*, equivalente à autoridade nacional de proteção de dados do país, publicou uma série de documentos sobre o tema, como um código de conduta (Information Commissioner's Office, 2017) próprio, um guia para o uso doméstico da ferramenta (Information Commissioner's Office, [20--?]); e um guia de como elaborar um relatório de impacto especificamente para o uso de CFTV (Information Commissioner's Office, 2020).

Convenção 108 de 1981, a Convenção Europeia dos Direitos Humanos e órgão responsável pela implementação da última, o Tribunal Europeu dos Direitos Humanos. Não obstante, o Conselho da Europa e a UE compartilham valores e possuem funções complementares, sendo as diretrizes emitidas pelo Conselho de grande relevância para a compreensão do GDPR e demais normas internacionais de proteção de dados pessoais.

[4] Sucessor do Article 29 Working Party, o Conselho Europeu de Proteção de Dados Europeu é a instituição da União Europeia responsável pela aplicação uniforme do GDPR no bloco.

[5] Diferentemente do Brasil, a Alemanha possui uma pluralidade de autoridades de proteção de dados, cada uma competente por um estado da Federação. Nesse sentido, as autoridades se reúnem frequentemente para emitir diretrizes uniformes sobre temas relevantes em âmbito nacional. Uma dessas diretrizes diz respeito ao uso de CFTV na esfera privada.

No próximo capítulo, as orientações supracitadas serão fundamentais para abordar os principais desdobramentos práticos do videomonitoramento, visto que são uma valiosa fonte de soluções e parâmetros para uma futura regulamentação nacional sobre a atividade.

3 DESAFIOS EM FACE DO VIDEOMONITORAMENTO: CASOS RELEVANTES EM ÂMBITOS EUROPEU E NACIONAL

Devido à entrada em vigor da legislação de proteção de dados anteriormente ao Brasil, a União Europeia já possui uma experiência farta em relação ao tema, expressa através da publicação de diversos estudos e diretrizes de Autoridades de Proteção de Dados, além de uma extensa jurisprudência deslindando as principais controvérsias sobre a matéria.

Vários questionamentos derivam da videovigilância no contexto da proteção de dados de seus sujeitos: como garantir a proteção de dados na implementação de novos sistemas de videovigilância? Quais são os mecanismos de mitigação necessários para o tratamento desses dados pessoais? Como os dados coletados devem ser armazenados? Quem poderá acessá-los? Por quanto tempo esses dados devem ser armazenados? Como os titulares poderão exercer seus direitos em face da videovigilância, tais como a requisição de acesso aos dados? Como avaliar os riscos relativos à videovigilância?

As questões são complexas e exigem uma análise minuciosa da realidade do videomonitoramento em conjugação com as previsões legais acerca da proteção de dados pessoais.

Nesta seção, busca-se, de forma sucinta, resumir as principais questões que já foram enfrentadas judicialmente e quais soluções foram encontradas pelas instituições responsáveis pela salvaguarda dos diplomas de proteção de dados pessoais na Europa e no Brasil.

Contudo, é importante notar que noções como segurança e privacidade no Brasil e nos países da União Europeia são intrinsecamente distintas, bem como as diferentes realidades econômicas dos operadores do videomonitoramento em cada localidade. Por exemplo, enquanto a sensação de segurança à noite chega a 85% da população numa ampla gama de países do continente europeu, a mesma percepção no Brasil somente atinge 34% da população (OECD, 2020). Portanto, embora a experiência europeia seja de grande riqueza para o desenvolvimento da doutrina e jurisprudência pátrias, as especificações da realidade brasileira deverão ser levadas em consideração para uma aplicação legislativa em consonância com as necessidades nacionais.

3.1 Casos relevantes no âmbito europeu

No contexto europeu, destacam-se julgamentos de diferentes entidades regionais: do Tribunal Europeu de Direitos Humanos (TEDH); do Tribunal de Justiça da União Europeia (TJUE) e das autoridades nacionais de proteção de dados.

No âmbito do Tribunal Europeu de Direitos Humanos, destacam-se dois casos que se tornaram referências para a discussão dos limites da videovigilância na Europa: *Peck v. the United Kingdom*, julgado em janeiro de 2003, e *Köpke v. Germany*, julgado em outubro de 2010.

O primeiro caso, *Peck v. the United Kingdom*, teve início com a divulgação não autorizada do vídeo de um homem em estado de perturbação mental, captado pelo CFTV do distrito de Brentwood Borough, no Reino Unido (Council Of Europe, 2003). A divulgação foi de iniciativa da operadora do CFTV e do próprio distrito, que utilizou o vídeo como estratégia de promoção do uso de sistemas de videomonitoramento para a proteção dos habitantes, fato que resultou na reprodução das imagens por outros meios de comunicação locais. Após o exaurimento da reclamação nas instâncias nacionais, o homem objeto da gravação recorreu ao Tribunal de Estrasburgo, o qual determinou que a utilização não autorizada de imagens captadas por sistemas de videomonitoramento público para promover campanhas de prevenção ao crime constituiria uma violação do direito à vida privada, nos termos do art. 8º da Convenção Europeia dos Direitos Humanos.

O caso *Köpke v. Germany* (Council Of Europe, 2010) trata da utilização oculta do videomonitoramento no ambiente de trabalho. No caso, uma empregadora suspeitava que uma colaboradora estava se apropriando de parte da receita. Para sanar a dúvida, a empregadora instalou uma câmera oculta para monitorar a funcionária, fato que resultou na confirmação dos roubos. Após ter, sem êxito, contestado sua demissão nas cortes alemãs, a ex-funcionária recorreu ao TEDH, alegando violação de seu direito à privacidade. A Corte decidiu pela inadmissibilidade da requisição, afirmando que a Alemanha corretamente ponderou o direito à privacidade da funcionária em face do direito de proteção à propriedade da empregadora, não importando em violação do art. 8º da Convenção Europeia dos Direitos Humanos, visto que a ação da empregadora se limitou ao estritamente necessário.

Em 2019, o TEDH adotou o mesmo entendimento em um caso com contornos similares: por meio de uma avaliação da proporcionalidade do uso da videovigilância, a Corte entendeu que o monitoramento por câmeras ocultas não havia violado o direito à privacidade dos empregados (Council Of Europe, 2019).

Em 2014, o Tribunal de Justiça da União Europeia, ainda no âmbito da Diretiva 95/46, proferiu importante decisão acerca da extensão da videovigilância para fins particulares (União Europeia, 2014). No caso, um homem havia instalado um sistema de monitoramento em casa, cujo

perímetro incluía a gravação de parte da rua. Nesse sentido, o TJUE determinou que, quando o videomonitoramento é instalado por um indivíduo para proteger sua propriedade, mas inclui o monitoramento de áreas públicas como ruas e calçadas, essa prática não será considerada tratamento de dados para fins exclusivamente particulares.

Tal decisão é de grande relevância para compreender que a exceção prevista pelo GDPR (e pela LGPD) em relação ao videomonitoramento para fins exclusivamente particulares não é absoluta: quando a filmagem envolver ambientes além da residência particular, o regulamento será aplicável.

Com base neste mesmo fundamento, após a promulgação do GDPR, observa-se uma prática uniforme das autoridades nacionais europeias na aplicação de multas em face do uso desproporcional do videomonitoramento. Essas sanções visam punir a recorrente utilização da ferramenta por estabelecimentos e particulares abrangendo áreas públicas, consequentemente extrapolando o perímetro necessário para atingir as finalidades dos controladores.

A título exemplificativo, a primeira multa aplicada pela autoridade de proteção de dados austríaca após a entrada em vigor do GDPR tratava do uso de videomonitoramento excessivo numa cafeteria (Áustria , 2018). No caso, o perímetro das câmeras abrangia uma ampla área além da entrada da propriedade, incluindo ruas e um estacionamento público. A autoridade austríaca multou o estabelecimento no importe de 5.280,00 euros, sob a justificativa de coleta excessiva dos dados, ou seja, os dados coletados eram desnecessários para atingir a finalidade do controlador. A decisão também aponta outras irregularidades, como ausência de placas informativas sobre o monitoramento; de protocolos sobre o uso da tecnologia e de descarte dos dados num período razoável.

Diversas outras decisões de autoridades nacionais sancionaram condutas relativas à videovigilância em desconformidade com a legislação de proteção de dados, tais como o tratamento desprovido de base legal (Landesbeauftragte für den Datenschutz Niedersachsen, 2021); a ausência de adoção de medidas de segurança pelo controlador (Data Guidance,' 2021), o monitoramento no ambiente de trabalho (EDPB , 2019) e a utilização indevida da tecnologia de reconhecimento facial (Autoriteit Persoonsgegevens, 2018).

3.2. Casos relevantes no âmbito nacional

No Brasil, as principais controvérsias judicializadas que tratam da intersecção entre proteção de dados e videomonitoramento dizem respeito à conjugação dessa ferramenta com a tecnologia do reconhecimento facial. Este trabalho abordará os dois principais casos recentes sobre o tema: (i) o caso das portas interativas no metrô de São Paulo e (ii) a utilização do reconhecimento facial para *marketing* numa loja da Hering em São Paulo.

3.2.1 O caso “portas interativas” da ViaQuatro

A primeira controvérsia iniciou-se em abril de 2018, quando a ViaQuatro – concessionária responsável pela manutenção da Linha 4 do metrô de São Paulo – implementou a tecnologia de portas interativas digitais, que consiste na utilização do reconhecimento facial por meio de câmeras instaladas nas portas dos vagões para identificar as emoções diante da publicidade exibida, bem como o gênero e a faixa etária dos passageiros. Por intermédio de uma breve nota de imprensa, a ViaQuatro afirmou que o objetivo das portas interativas era mensurar os dados coletados para a otimização de estratégias de publicidade futuras (Uol, 2018). A tecnologia foi alvo imediato de críticas (Montagner, 2018) devido a várias problemáticas, como a ausência de solicitação do consentimento dos titulares; de especificação a respeito dos dados coletados, da finalidade do tratamento, das medidas de segurança aplicadas e do possível compartilhamento com terceiros; e até mesmo do debate com a sociedade civil (Souza, 2018).

Por conseguinte, o Instituto Brasileiro de Defesa do Consumidor (Idec) moveu ação civil pública exigindo a cessação imediata da coleta de dados pelo sistema das portas interativas e o pagamento de indenização de R$ 100 milhões por danos coletivos. O Idec apontou uma série de irregularidades na atividade da ViaQuatro, destacando-se a implementação forçada do sistema, sem a solicitação do consentimento dos passageiros, que eram obrigados a aceitar a coleta dos dados mediante a essencialidade do serviço do metrô.

Anterior à entrada em vigor da LGPD, o Idec utilizou uma interpretação conjunta do regime de proteção de dados pessoais à época, baseando-se na CF, no CC, no CDC, na Lei de Acesso à Informação e no Marco Civil da Internet. A prática violaria os deveres de informação, transparência e proporcionalidade previstos no Código de Defesa do Consumidor e no Código de Defesa dos Usuários de Serviços Públicos, bem como os direitos à imagem e privacidade instituídos na CF. O Idec ressalta também a possibilidade de obtenção de vantagem manifestamente excessiva da ViaQuatro em face dos passageiros. Ainda, a prática da ViaQuatro violaria a cautela necessária com os dados de crianças e adolescente usuárias do metrô.

Por sua vez, a Via Quatro afirmou que não haveria tratamento de dados pessoais, pois os dados coletados pelo sistema de portas interativas seriam “totalmente desvinculados à identidade de uma pessoa”, sendo utilizados somente para fins estatísticos.

Em setembro de 2018, a Justiça paulista acatou o pedido de tutela de urgência do Idec e determinou a interrupção do uso da tecnologia das portas interativas (Idec, 2018). Em maio de 2021, o Tribunal de Justiça de São Paulo condenou a Via Quatro pelo uso do reconhecimento facial e ao pagamento de indenização no montante de R$ 100 mil por danos morais coletivos (Soprana; Amâncio, 2021).

A decisão é fortemente fundamentada pela LGPD, sob a égide de que, caso a Via Quatro deseje seguir com o uso da referida tecnologia, terá que se submeter futuramente a esta lei. Primeiramente, a decisão rejeita a alegação da Ré sobre a ausência de tratamento de dados pessoais, afirmando ser incontroversa a captação de imagens e dados biométricos, ambos reconhecidos como dados pessoais pela LGPD. Nesse sentido, o juízo ressalta a classificação dos dados biométricos como dados sensíveis, exigindo tratamento especial, devendo adequar-se a uma das hipóteses autorizativas do art. 11 da LGPD.

> Apesar da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados LGPD) ser posterior ao início da captação das imagens objeto dos autos, a questão concernente à obrigação de fazer e de não fazer pleiteada pela autora e do tratamento dos dados captados, com efeitos futuros, está submetida à sua regência. (...) Desta forma, o reconhecimento facial ou mesmo a mera detecção facial, sem que seja possível a identificação concreta do indivíduo, mas com acesso à sua imagem e face, parece já esbarrar no conceito de dado biométrico, legalmente considerado como dado pessoal sensível, daí porque merece tratamento especial à luz da Lei nº 13.709/2018. Anote-se que a LGPD estabeleceu proteção especial aos dados pessoais sensíveis, autorizando o seu tratamento somente na hipótese de consentimento claro e específico pelo titular do dado, ou, sem o consentimento do titular, nas situações elencadas no rol do inciso II d artigo 11 da LGPD, não se vislumbrando nenhuma das hipóteses no caso em tela (Brasil, 2021, p.2290-2291).

Dessa forma, a única base legal possível para a prática da Via Quatro seria a do consentimento, o qual não foi coletado dos titulares.

Ademais, o juízo ressalta a necessidade de a finalidade do tratamento ter propósitos legítimos, específicos e informados ao titular, fato que não se verificou no caso.

> A situação exposta no caso concreto é muito diferente da captação de imagens por sistemas de segurança com objetivo de melhoria na prestação do serviço, segurança dos usuários ou manutenção da ordem, o que seria não só aceitável, mas necessário diante da obrigação da fornecedora de serviço público zelar pela segurança de seus usuários dentro de suas dependências. É evidente que a captação da imagem ora discutida é utilizada para fins publicitários e consequente cunho comercial, já que, em linhas gerais, se busca detectar as principais características dos indivíduos que circulam em determinados locais e horários, bem como emoções e reações apresentadas à publicidade veiculada no equipamento (Brasil, 2021, p. 2291).

Destaca também a falha da concessionária em cumprir seu dever de informação e transparência previsto no CDC, visto que os passageiros não foram avisados em nenhum momento acerca do tratamento de seus dados.

Esse caso, como pioneiro na judicialização do tema, demonstra o começo de uma possível sequência de hipóteses em que o Judiciário será chamado a decidir sobre os limites da implementação do videomonitoramento "*per se*", ou seja, implementado sem considerar o direito dos titulares sujeitos à prática. Utilizar a videovigilância implica, automaticamente, na necessidade de observância aos preceitos essenciais da proteção de dados, bem como ao tratamento diferenciado para o uso da tecnologia de reconhecimento facial, devido ao tratamento de dados sensíveis.

3.2.2 O caso “Hering”

Em outubro de 2018 (New Trade, 2018), a marca de vestuário Hering inaugurou uma “loja conceito” em São Paulo, na qual instalou um sistema de câmeras com reconhecimento facial para captar as reações às roupas expostas e traçar perfis de seus visitantes, além de analisar as áreas mais visitadas da loja por meio da análise de ondas de calor. Ocorre que a prática não era informada aos clientes, bem como não havia coleta do consentimento destes.

Nessa conjuntura, em fevereiro de 2019, o Idec notificou a Hering solicitando esclarecimentos acerca da finalidade do tratamento, dos meios de coleta e do possível compartilhamento dos dados (Idec, 2019). Após tomar conhecimento da denúncia do Idec, a Secretaria Nacional do Consumidor (Senacon), no âmbito do Departamento de Proteção e Defesa do Consumidor (DPDC), iniciou investigações acerca da prática da loja.

Diante da ação, a gestão da marca alegou que “diferentemente do que foi apontado, [a Hering] não realiza reconhecimento facial, mas, sim, detecção facial, por meio da qual estima apenas o gênero, a faixa etária e o humor dos consumidores, de forma anônima” (O Globo, 2019). Em linhas similares à argumentação da ViaQuatro no caso das portas interativas, a Hering afirmou que os dados seriam meramente estatísticos, não havendo tratamento de dados pessoais e, consequentemente, não haveria necessidade de coleta do consentimento.

Em agosto de 2020, a Hering foi condenada pela Senacon a pagar multa de R$ 58.767,00 em face da prática abusiva de utilização de tecnologias de reconhecimento facial sem o consentimento prévio de seus consumidores (Gov.br, 2020). Embora anterior à vigência da LGPD, a decisão fundamentou-se na violação do direito à imagem como direito da personalidade, segundo o Código Civil, e no dever de informação, previsto pelo Código de Defesa do Consumidor.

O caso foi emblemático, visto que resultou na primeira condenação devido ao uso de reconhecimento facial no Brasil (Idec, 2020).

CONCLUSÃO

Em suma, a força do videomonitoramento na modernidade é incontestável. Trata-se de uma das faces mais evidentes da sociedade de vigilância, sendo uma ferramenta poderosa para lidar com as mais diversas questões, desde o auxílio à segurança pública e privada ao desenho de campanhas publicitárias. Conforme demonstrado ao longo do presente artigo, é um instrumento complexo de monitoramento que, quando utilizado de modo irrestrito, tem elevado potencial de violação de direitos e garantias fundamentais de seus sujeitos. Notadamente, a conjugação do videomonitoramento com

a tecnologia de reconhecimento facial é capaz de exacerbar esses efeitos negativos, como demonstrado numa série de casos de discriminação ensejados por essa.

A evolução histórica da legislação sobre o videomonitoramento no Brasil em muito se assemelha com o progresso internacional da legislação de proteção de dados pessoais: iniciou-se num plano técnico até reconhecer a necessidade de proteção dos dados das pessoas afetadas pela aceleração das práticas de *dataveillance* possibilitadas pelas novas tecnologias.

Com o advento da LGPD, o cenário legislativo preponderantemente técnico e de escasso debate público sobre a matéria, observado anteriormente, tem se transformado, com a notória participação de entidades da sociedade civil, em diversas discussões importantes sobre o videomonitoramento. A LGPD realocou o centro da discussão da perspectiva socioeconômica atribuída ao uso de dados pessoais, para agora também considerar a pessoa humana objeto da vigilância. Assim, a lei devolve ao titular dos dados o seu devido protagonismo, buscando reduzir a assimetria entre agentes e sujeitos inerente à vigilância.

Contudo, embora a LGPD seja um marco importante, sua entrada em vigor não remedia, por si só, as implicações do videomonitoramento na proteção de dados pessoais.

A promulgação dessa lei também enseja diversas dúvidas acerca de sua aplicação à matéria. A experiência internacional demonstra a existência de diversos pontos que precisarão ser regulamentados pela LGPD, como a operacionalização dos direitos dos titulares, a definição dos prazos de retenção e descarte, as medidas de segurança que deverão ser observadas e inúmeras outras implicações práticas. Dessa forma, ressalta-se a necessidade da atuação da ANPD para regulamentar o tema, de modo a incluir a proteção de dados pessoais na operacionalização do monitoramento por câmeras.

Ademais, a videovigilância para fins de segurança pública e persecução penal é uma problemática que deve ser urgentemente abordada, visto que uma das principais hipóteses de utilização dessa ferramenta encontra-se desprovida de parâmetros legais para a sua efetivação.

Apesar destes diversos avanços, destaca-se que o debate público sobre o videomonitoramento ainda é preponderantemente limitado à segurança pública e patrimonial, desconsiderando as implicações de proteção de dados decorrentes do uso exacerbado desse instrumento. Portanto, a eficácia da LGPD no mundo real e, consequentemente, na prática do videomonitoramento, exige uma mudança integral da cultura das organizações e da própria sociedade civil em relação à privacidade e proteção de dados no Brasil.

Para tanto, a conscientização e orientação de titulares e controladores será determinante para a efetiva transformação do uso de tecnologias de vigilância, tais como o videomonitoramento, em âmbito nacional.

REFERÊNCIAS

AN INTRODUCTION to the surveillance society. **The Surveillance Studies Network**, [*s.l.*], 2016. Disponível em: https://www.surveillance-studies.net/?page_id=119. Acesso em: 10 fev. 2021.

AP informeert branche over norm camera's in reclamezuilen. **Autoriteit Persoonsgegevens**, Nieuwsbericht, [*s.l.*], 26 June 2018. Disponível em: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-informeert-branche-over-norm-camera%E2%80%99s-reclamezuilen. Acesso em: 11 maio 2021.

APÓS denúncia do Idec, Hering é condenada por uso de reconhecimento facial. **Idec**, [*s.l.*], 26 ago. 2020. Disponível em: https://idec.org.br/noticia/apos-denuncia-do-idec-hering-e-condenada-por-uso-de-reconhecimento-facial. Acesso em: 10 maio 2021.

ÁREAS temáticas: Videovigilância. **CNPD**, 2020. Disponível em: https://www.cnpd.pt/organizacoes/areas-tematicas/videovigilancia/. Acesso em: 1 maio 2021.

ÁUSTRIA. Datenschutzbehörde. **DSB-D550.038/0003-DSB/2018**. Viena, 18 Sept. 2018. Disponível em: https://www.dsb.gv.at/recht-entscheidungen/entscheidungen-der-datenschutzbehoerde.html. Acesso em: 10 maio 2021.

BAUMAN, Z. **Vigilância Líquida**. São Paulo: Zahar, 2014.

BISCHOFF, P. Surveillance camera statistics: which cities have the most CCTV cameras?. **Comparitech**, [*s.l.*], 17 May 2021. Disponível em: https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/. Acesso em: 17 maio 2021.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 5662/2019**. Dispõe sobre a obrigatória a criação de um Sistema de Monitoramento por câmeras em municípios com mais de 30 mil habitantes e cria Sistema Nacional Integrado. Brasília: Câmara dos Deputados, 2019. Disponível em: https://www.camara.leg.br/propostas-legislativas/2226793/.Acesso em: 20 mar. 2021.

BRASIL. Tribunal de Justiça do Estado de São Paulo. Ação Civil Pública Cível - Transporte Ferroviário nº 1090663-42.2018.8.26.0100. Requerente: Idec - Instituto Brasileiro de Defesa do Consumidor. Requerido: Concessionaria da Linha 4 do Metro de São Paulo S.a. (Via Quatro). Juiz(a) de Direito: Dr(a). Patrícia Martins Conceição, São Paulo 7 maio 2021.

CEARÁ (Estado). Assembleia Legislativa do Estado do Ceará. **Projeto de Lei nº 42/2020**, **de 23 de julho de 2020**. Dispõe sobre o uso compartilhado, em tempo real, com o sistema de videomonitoramento da segurança pública estadual de imagens de câmeras privadas captadas do ambiente externo a imóveis, públicos e privados, situados no estado do Ceará, e dá outras providências. Fortaleza: Assembleia Legislativa do Estado do Ceará, 2020. Disponível em: https://www2.al.ce.gov.br/legislativo/tramit2020/8531.htm. Acesso em: 3 maio 2021.

COUNCIL OF EUROPE. **Guidelines on facial recognition**. Estrasburgo: Council of Europe, 2021. Disponível em: https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3. Acesso em: 1 maio 2021.

COUNCIL OF EUROPE. **Resolution 1604:** video surveillance of public areas. Estrasburgo: Council of Europe, 2008. Disponível em: PACE - Resolution 1604 (2008) - Video surveillance of public areas (coe.int). Acesso em: 1 maio 2021.

COUNCIL OF EUROPE. **Surveillance by intelligence services fundamental rights safeguards and remedies in the EU**. Estrasburgo: Council of Europe, v. 2, 2017.

COUNCIL OF EUROPE. Tribunal Europeu de Direitos Humanos. **Application n. 44647/98**. Requerente: Geoffrey Dennis Peck. Requerido: Reino Unido. Pres.: Matti Pellonpää. Estrasburgo, 28 Apr. 2003. Disponível em: https://bit.ly/3bN6s9f. Acesso em: 10 maio 2021.

COUNCIL OF EUROPE. Tribunal Europeu de Direitos Humanos. **Application n. 420/07**. Requerente: Karin Köpke. Requerido: Alemanha. Pres.: Peer Lorenzen. Estrasburgo, 5 Oct. 2010. Disponível em: https://hudoc.echr.coe.int/eng?i=001-101536. Acesso em: 10 maio 2021.

COUNCIL OF EUROPE. Tribunal Europeu de Direitos Humanos. **Application n. 1874/13 e 8567/13**. Requerentes: López Ribalda e Outros. Requerido: Espanha. Pres.: Peer Lorenzen. Estrasburgo, 17 Oct. 2019. Disponível em: https://bit.ly/2RFXrbl. Acesso em: 10 maio 2021.

CROATIA: AZOP issues administrative penalty against security company for security violation. **Data Guidance**. [*s.l.*], 26 Apr. 2021. Disponível em: https://www.dataguidance.com/news/croatia-azop-issues-administrative-penalty-against. Acesso em: 11 maio 2021.

DATA PROTECTION COMMISSION. **Guidance on the Use of CCTV** – For Data Controllers, [*s.l.*], [20--?]. Disponível em: https://www.dataprotection.ie/en/dpc-guidance/guidance-use-cctv-data-controllers. Acesso em: 1 maio 2021.

DUFAUX, F; EBRAHIMI, T. Scrambling for Video Surveillance with Privacy. *In*: **IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)**, New York, 2006. Disponível em: https://ieeexplore.ieee.org/document/1640607. Acesso em: 20 fev. 2021.

EUROPEAN DATA PROTECTION BOARD. **Diretrizes 3/2019 sobre tratamento de dados pessoais através de dispositivos de vídeo**. 2. ed. Bruxelas: European Data Protection Board, 29 jan. 2020. Disponível em: https://edps.europa.eu/sites/default/files/publication/10-03-17_video-surveillance_guidelines_en.pdf. Acesso em: 05 maio 2021.

FIRMINO, Rodrigo José *et al*. Fear, security, and the spread of CCTV in brazilian cities: legislation, debate, and the market. **Journal of Urban Technology**, [*s.l.*], v. 20, n. 3, p. 65-84, 2013.

GILBRATAR REGULATORY AUTHORITY. **Guidance on the EU General Data Protection Regulation 2016/679 & Data Protection Act 2004**, v. 2, 10 Nov. 2020.
GREENLEAF, G; COTTIER, B. 2020 ends a decade of 62 new data privacy laws. **Privacy Laws & Business International Report**, [*s.l.*], n. 123, 2020, p. 24. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3572611. Acesso em: 10 fev. 2021.

GUICHARD, G. Le fisc interdit de drone pour contrôler les propriétés des contribuables. **Le Figaro**, [*s.l.*], 18 jan. 2018. Disponível em: https://www.lefigaro.fr/impots/2018/01/18/05003-20180118ARTFIG00044-le-fisc-interdit-de-drone-pour-controler-les-proprietes-des-contribuables.php. Acesso em: 10 fev. 2021.

HERING inaugura loja conceito no Shopping Morumbi, em São Paulo. **New Trade**, [*s.l.*], 15 out. 2018. Disponível em: https://newtrade.com.br/varejo/hering-inaugura-loja-conceito-no-shopping-morumbi-em-sao-paulo/. Acesso em: 10 maio 2021.

HERING terá que explicar o que faz com dados de reconhecimento facial de clientes. **O Globo**, [*s.l.*], 2 set. 2019. Disponível em: https://oglobo.globo.com/economia/hering-tera-que-explicar-que-faz-com-dados-de-reconhecimento-facial-de-clientes-23921786. Acesso em: 10 maio 2021.

HERING terá que explicar o que faz com dados de reconhecimento facial. **Idec**, [*s.l.*], 26 fev. 2019. Disponível em: https://idec.org.br/idec-na-imprensa/hering-tera-que-explicar-o-que-faz-com-dados-de-reconhecimento-facial-de-clientes. Acesso em: 10 maio 2021.

INFORMATION COMMISSIONER (Eslovênia). **Guidelines on video surveillance**. Ljubljana: Information Commissioner, 13 Feb. 2019. Disponível em: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Guidelines_videosurveillance_eng.pdf. Acesso em: 1 maio 2021.

INFORMATION COMMISSIONER'S OFFICE. **Data protection impact assessments guidance for carrying out a data protection impact assessment on surveillance camera systems**. 3. ed. Wilmslow: Office of the Information Commissioner, 2020. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/881538/SCC___ICO_DPIA_guidance_V3_FINAL_PDF.pdf. Acesso em: 1 maio 2021.

INFORMATION COMMISSIONER'S OFFICE. **Domestic CCTV systems:** guidance for people using CCTV. Wilmslow: Office of the Information Commissioner, [20--?]. Disponível em: https://ico.org.uk/your-data-matters/domestic-cctv-systems-guidance-for-people-using-cctv/. Acesso em: 1 maio 2021.

INFORMATION COMMISSIONER'S OFFICE. **In the picture:** a data protection code of practice for surveillance cameras and personal information. Wilmslow: Office of the Information Commissioner, v.1.2, 2017. Disponível em: https://www2.le.ac.uk/offices/estates/documents/design-guides/cctv-code-of-practice.pdf. Acesso em: 1 maio 2021.

JUSTIÇA impede uso de câmera que coleta dados faciais em metrô em SP. **Idec**, [*s.l.*], 18 set. 2018. Disponível em: https://idec.org.br/noticia/justica-impede-uso-de-camera-que-coleta-dados-faciais-do-metro-em-sp. Acesso em: 10 maio 2021.

LEITE, R. Lei Geral de Proteção de Dados do Brasil: análise contextual detalhada. **Jota**, [*s.l.*], 14 jul. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-140720. Acesso em: 20 mar. 2021.

LEPRI, J. São Paulo é a cidade com o maior número de câmeras do Brasil. **G1 Globo**, São Paulo, 23 out. 2013. Disponível em: http://g1.globo.com/jornal-da-globo/noticia/2013/10/sao-paulo-e-cidade-com-o-maior-numero-de-cameras-do-brasil.html. Acesso em: 5 maio 2021.

LfDI. **Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen**. [*S.l.*]: Datenschutzkonferenz, 17 Juli 2020. Disponível em: https://www.datenschutzkonferenz-online.de/media/oh/20200903_oh_v%C3%BC_dsk.pdf. Acesso em: 1 maio 2021.

LIM, L. The legal framework of video surveillance in Europe. *In*: SECURITY, European Forum for Urban. **Citizens, cities and video surveillance:** towards a democratic and responsible use of CCTV. Paris: European Forum for Urban Security, 2010.

LYON, D. **The electronic eye**: the rise of surveillance society. Minneapolis: University of Minnesota Press, 1994.

MARX, G. T. The surveillance society: the threat of 1984-style techniques. **The Futurist**, [*s.l.*], v. 6, 1985.

MENDES, L.S. A Lei Geral de Proteção de Dados: uma aplicação em três níveis. *In*: SOUZA, C. A.; MAGRANI, E.; SILVA, P. (Coord.). **Lei Geral de Proteção de Dados:** caderno especial. São Paulo: RT, 2019.

MENDES, L; DONEDA, D. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo, v. 120, p. 469-483, 2018.

MONTAGNER, C. Dados biométricos dos paulistanos são coletados no metrô sem consentimento nem debate das implicações. **Lavits**, [*s.l.*], 2 maio 2018. Disponível em: https://lavits.org/dados-biometricos-dos-passageiros-do-metro-de-sp-sao-tratados-sem-consentimento-nem-discussao-das-implicacoes/?lang=pt. Acesso em: 10 maio 2021.

MOREIRA, A. F. S. **Proteção de dados e sistemas de videomonitoramento**: contornos da privacidade na sociedade de vigilância. 2021. Trabalho de conclusão de Curso (Bacharel em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, 2021

NORMAND, J. Le drone, renfort utile mais controversé pour faire respecter le confinement. **Le Monde**, [*s.l.*], 26 mars 2020. Disponível em: https://www.lemonde.fr/economie/article/2020/03/26/le-drone-renfort-utile-mais-controverse-pour-faire-respecter-le-confinement_6034517_3234.html. Acesso em: 10 fev. 2021.

OCDE. **How's life:** measuring well-being. Paris: OECD Publishing, 2020. Disponível em: http://www.oecdbetterlifeindex.org/topics/safety. Acesso em: 10 fev. 2021.

PINHEIRO, P. P. **Proteção de dados pessoais:** comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

POLÍCIA vai usar drones para operações e investigações na Grande Vitória. **G1 Globo**, Vitória, 26. jul. 2019. Disponível em: https://g1.globo.com/es/espirito-santo/noticia/2019/07/26/policia-vai-usar-drones-para-operacoes-e-investigacoes-na-grande-vitoria.ghtml. Acesso em: 10 fev. 2021.

PORTAS da linha 4 do metrô de SP vão reconhecer seu rosto e expressões. **UOL**, Coluna Tilt, São Paulo, 13 abr. 2018. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2018/04/13/com-cameras-em-plataformas-linha-do-metro-de-sp-captara-reacoes-de-pessoas.htm. Acesso em: 28 abr. 2021.

SECRETARIA Nacional do Consumidor aplica multa a empresa por reconhecimento facial. **Gov.br**, [*s.l.*], 14 ago. 2020. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/secretaria-nacional-do-consumidor-aplica-multa-a-empresa-por-reconhecimento-facial. Acesso em: 10 maio 2021.

ŠIDLAUSKAS, A. Video surveillance and the GDPR. *In*: **Social transformations in contemporary society**, Vilnius, n. 7, 2019, p. 60.

SOPRANA, P.; AMÂNCIO, Thiago. ViaQuatro é condenada por reconhecimento facial sem autorização no Metrô de SP. **Folha de S. Paulo**, São Paulo, 11 maio 2021. Disponível em: https://www1.folha.uol.com.br/cotidiano/2021/05/viaquatro-e-condenada-por-reconhecimento-facil-sem-autorizacao-no-metro-de-sp.shtml. Acesso em: 15 maio 2021.

SOUZA, C. A. A privacidade saiu dos trilhos no metrô de São Paulo. **UOL**, Coluna Tilt, [*s.l.*], 18 abr. 2018. Disponível em: https://tecfront.blogosfera.uol.com.br/2018/04/18/a-privacidade-saiu-dos-trilhos-no-metro-de-sao-paulo/. Acesso em: 15 abr. 2021.

SURVEILLANCE CAMERA COMMISSIONER. **Facing the camera:** good practice and guidance for the police use of overt surveillance camera systems incorporating facial recognition technology to locate persons on a watchlist, in public places in England & Wales. Londres: Office of the Surveillance Camera Commissioner, Nov. 2020. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf. Acesso em: 1 maio 2021.

SURVEILLANCE CAMERA COMMISSIONER. **Surveillance Camera Code of Practice**, London, 2013. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf. Acesso em: 1 maio 2021.

THE EUROPEAN DATA PROTECTION SUPERVISOR. **Follow-up Report to the 2010 EDPS Video-Surveillance Guidelines**. Bruxelas: European Data Protection Supervisor, 2013. Disponível em: https://edps.europa.eu/sites/default/files/publication/12-02-13_report_cctv_en.pdf. Acesso em: 1 maio 2021.

THE EUROPEAN DATA PROTECTION SUPERVISOR. **The EDPS:** Supervising EU institutions and bodies & enforcing data protection principles. EDPS factsheet 3, [*s.l.*], 2013. Disponível em: https://edps.europa.eu/sites/default/files/publication/factsheet_3_en.pdf. Acesso em: 1 maio 2021.

THE EUROPEAN DATA PROTECTION SUPERVISOR. **The EDPS Video-Surveillance Guidelines**. Bruxelas: European Data Protection Supervisor, 2010. Disponível em: https://edps.europa.eu/sites/default/files/publication/10-03-17_video-surveillance_guidelines_en.pdf. Acesso em: 1 maio 2021.

UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. **CJEU, Case 212/13**. Requerido: František Ryneš. Requerente: Úřad pro ochranu osobních údajů. Rel.: M. Safjan. Bruxelas, 11 Dec. 2014. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62013CJ0212. Acesso em: 10 maio 2021.

VAINZOF, R. In: MALDONADO, V. N.; BLUM, R. O. (Coord.). **LGPD:** Lei Geral de Proteção de Dados comentada. 2. ed. São Paulo: RT, 2019.

WOOD, D. M. *et al*. **A report on the surveillance society**. Wilmslow: Office of the Information Commissioner, 2006.

YOUNG, C. S. **The science and technology of counterterrorism:** measuring physical and electronic security risk. Oxford: Butterworth-Heinemann, 2015.