

Projeto de Lei n.º 531/XVII/1.ª (CH)

Primeira alteração à Lei n.º 95/2021, de 29 de dezembro (Regula a utilização e o acesso pelas forças e serviços de segurança e pela Autoridade Nacional de Emergência e Proteção Civil a sistemas de videovigilância para captação, gravação e tratamento de imagem e som), em matéria de prevenção da prática de atos terroristas

Data de admissão: 15 de abril de 2026

Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias (1.ª)

ÍNDICE

- I. A INICIATIVA
- II. APRECIÇÃO DOS REQUISITOS CONSTITUCIONAIS, REGIMENTAIS E FORMAIS
- III. ENQUADRAMENTO JURÍDICO NACIONAL
- IV. ENQUADRAMENTO JURÍDICO NA UNIÃO EUROPEIA E INTERNACIONAL
- V. ENQUADRAMENTO PARLAMENTAR
- VI. CONSULTAS E CONTRIBUTOS
- VIII. ENQUADRAMENTO BIBLIOGRÁFICO

I. A INICIATIVA

A iniciativa legislativa em apreço visa proceder à primeira alteração à [Lei n.º 95/2021](#)¹, de 29 de dezembro, diploma que regula a utilização e o acesso pelas forças e serviços de segurança e pela Autoridade Nacional de Emergência e Proteção Civil a sistemas de videovigilância para captação, gravação e tratamento de imagem e som, revogando a [Lei n.º 1/2005](#), de 10 de janeiro, no sentido de permitir a captação e tratamento de dados biométricos para efeito de prevenção de atos terroristas.

Os proponentes recordam que o referido diploma legal diverge da iniciativa que lhe deu origem² quanto à possibilidade de tratamento de dados biométricos para efeito de prevenção de atos terroristas, uma vez que tal possibilidade estava prevista na [Proposta de Lei n.º 111/XIV/1.ª \(GOV\)](#), mas não consta do articulado da [Lei n.º 95/2021](#), de 29 de dezembro.³

Acrescentam que «alguns sinais de aumento do nível de ameaça terrorista mereceram atenção por parte da Europol, que advertiu para um risco mais elevado de situações de terrorismo na União Europeia devido à escalada do conflito no Médio Oriente».

Consideram igualmente que a implementação das linhas de ação em que se concretiza o eixo «prevenção» da Estratégia Nacional de Combate ao Terrorismo⁴ são «difícilmente realizáveis sem recurso à captação e tratamento de dados biométricos» e realçam que a videovigilância foi determinante no combate ao terrorismo em diversas ocasiões, exemplificando com casos concretos.

Em concreto, a iniciativa é composta por três artigos preambulares: o primeiro definidor do objeto; o segundo introduzindo alterações no artigo 16.º da [Lei n.º 95/2021](#), de 29 de

¹ Texto sem alterações retirado do sítio na Internet do Diário da República. Todas as referências legislativas nesta parte da nota técnica são feitas para o portal oficial do Diário da República, salvo indicação em contrário.

² A Lei n.º 95/2021, de 29 de dezembro, teve origem na [Proposta de Lei n.º 111/XIV/2.ª \(GOV\)](#) - *Regula a utilização de sistemas de vigilância por câmaras de vídeo pelas forças e serviços de segurança*.

³ O n.º 3 do artigo 18.º (Recolha e tratamento de dados) da Proposta de Lei n.º 111/XIV/2.ª (GOV) previa que o «tratamento de dados biométricos apenas é possível para os fins previstos na alínea e) do artigo 3.º, mediante autorização de entidade judicial», sendo que a alínea e) do artigo 3.º da referida Proposta de Lei estabelecia que «os sistemas de videovigilância apenas podem ser usados, no âmbito da presente lei, para a prossecução dos fins previstos na Lei de Segurança Interna, aprovada pela Lei n.º 53/2008, de 29 de agosto, na sua redação atual, e em concreto para: (...) e) Prevenção de atos terroristas». Na sequência da [discussão e votação na especialidade](#) da Proposta de Lei n.º 111/XIV/1.ª (GOV), o artigo 18.º (Recolha e tratamento de dados) foi renumerado como artigo 16.º (Recolha e tratamento de dados), numeração que se mantém no articulado da [Lei n.º 95/2021](#), de 29 de dezembro.

⁴ Aprovada pela [Resolução do Conselho de Ministros n.º 40/2023](#), de 3 de maio

dezembro, no sentido de ser permitida a captação e tratamento de dados biométricos para efeitos de prevenção de atos terroristas; o terceiro estabelecendo o momento de entrada em vigor da iniciativa, caso seja aprovada e promulgada.

II. APRECIÇÃO DOS REQUISITOS CONSTITUCIONAIS, REGIMENTAIS E FORMAIS

▪ Conformidade com os requisitos constitucionais e regimentais

A iniciativa em apreciação é apresentada pelo Grupo Parlamentar do CHEGA, ao abrigo e nos termos da alínea b) do artigo 156.º, do n.º 1 artigo 167.º e da alínea g) do n.º 2 do artigo 180.º da [Constituição da República Portuguesa](#) (Constituição), bem como da alínea f) do artigo 8.º, da alínea b) do n.º 1 do artigo 4.º e do n.º 1 do artigo 119.º do [Regimento da Assembleia da República](#) (Regimento)⁵, que consagram o poder de iniciativa da lei.

A iniciativa assume a forma de projeto de lei, em conformidade com o disposto no n.º 2 do artigo 119.º do Regimento. Encontra-se redigida sob a forma de artigos, é precedida de uma breve exposição de motivos e tem uma designação que traduz sinteticamente o seu objeto principal, cumprindo assim os requisitos formais previstos no n.º 1 do artigo 124.º do Regimento.

Cumpra também os requisitos formais previstos no n.º 2 do artigo 119.º e no n.º 1 do artigo 123.º do Regimento e observa os limites à admissão da iniciativa estabelecidos no n.º 1 do artigo 120.º do Regimento, uma vez que parece não infringir a Constituição ou os princípios nela consignados e define concretamente o sentido das modificações a introduzir na ordem legislativa.

A iniciativa deu entrada a 31 de março de 2026, acompanhada pela respetiva [ficha de avaliação prévia de impacto de género](#), foi admitida e baixou na generalidade à Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias (1.ª), a 15 de abril de 2026, por despacho do Presidente da Assembleia da República.

⁵ Textos consolidados da Constituição e do Regimento disponíveis no sítio da *Internet* da Assembleia da República.

▪ Verificação do cumprimento da lei formulário

A Lei n.º 74/98, de 11 de novembro, alterada e republicada pela Lei n.º 43/2014, de 11 de julho, de ora em diante designada como lei formulário, contém um conjunto de normas sobre a publicação, identificação e formulário dos diplomas que são relevantes em caso de aprovação da presente iniciativa.

O título da presente iniciativa legislativa – «Primeira alteração à Lei n.º 95/2021, de 29 de dezembro (Regula a utilização e o acesso pelas forças e serviços de segurança e pela Autoridade Nacional de Emergência e Proteção Civil a sistemas de videovigilância para captação, gravação e tratamento de imagem e som), em matéria de prevenção da prática de atos terroristas» - traduz sinteticamente o seu objeto, mostrando-se conforme ao disposto no n.º 2 do artigo 7.º da lei formulário. Em caso de aprovação, o título poderá ser objeto de aperfeiçoamento formal, em sede de apreciação na especialidade ou em redação final.

A iniciativa pretende alterar a [Lei n.º 95/2021, de 29 de dezembro](#)⁶ e elenca a informação prevista no n.º 1 do artigo 6.º da lei formulário⁷.

No que respeita ao início de vigência, o projeto de lei estabelece, no último artigo, que a entrada em vigor ocorre no dia seguinte ao da publicação, mostrando-se assim conforme com o previsto no n.º 1 do artigo 2.º da lei formulário, segundo o qual os atos legislativos «entram em vigor no dia neles fixado, não podendo, em caso algum, o início de vigência verificar-se no próprio dia da publicação».

Nesta fase do processo legislativo, a iniciativa em apreço não nos suscita outras questões em face da lei formulário.

III. ENQUADRAMENTO JURÍDICO NACIONAL

⁶ Diploma disponível no sítio da *internet* do *Diário da República*. Todas as referências legislativas são feitas para este portal oficial, salvo indicação em contrário

⁷ «Os diplomas que alterem outros devem indicar o número de ordem da alteração introduzida e, caso tenha havido alterações anteriores, identificar aqueles diplomas que procederam a essas alterações, ainda que incidam sobre outras normas.»

A [Lei n.º 95/2021, de 29 de dezembro](#)⁸, regula a utilização e o acesso pelas forças e serviços de segurança e pela Autoridade Nacional de Emergência e Proteção Civil a sistemas de videovigilância para captação, gravação e tratamento de imagem e som,⁹ revogando a [Lei n.º 1/2005](#), de 10 de janeiro¹⁰.

De acordo com o [artigo 3.º](#) desta lei, os sistemas de videovigilância apenas podem ser usados para a prossecução dos fins previstos na Lei de Segurança Interna, aprovada pela [Lei n.º 53/2008, de 29 de agosto](#)¹¹¹²¹³, e, em concreto, para: proteção de edifícios e infraestruturas públicas e respetivos acessos; proteção de infraestruturas críticas, pontos sensíveis ou instalações com interesse para a defesa e a segurança e respetivos acessos; apoio à atividade operacional das forças e serviços de segurança em operações policiais complexas, nomeadamente em eventos de grande dimensão ou de outras operações de elevado risco ou ameaça; proteção da segurança das pessoas, animais e bens, em locais públicos ou de acesso público, e a prevenção da prática de factos qualificados pela lei como crimes, em locais em que exista razoável risco da sua ocorrência; prevenção de atos terroristas; resposta operacional a incidentes de segurança em curso; controlo de tráfego e segurança de pessoas, animais e bens na circulação rodoviária; prevenção e repressão de infrações estradais; controlo de

⁸ Texto sem alterações retirado do sítio na *Internet* do Diário da República. Todas as referências legislativas nesta parte da nota técnica são feitas para o portal oficial do Diário da República, salvo indicação em contrário. Consultas efetuadas a 20/04/2026.

⁹ [Trabalhos preparatórios](#). Todas as referências a trabalhos preparatórios são feitas para o portal na *Internet* da Assembleia da República, salvo indicação em contrário. Consultas efetuadas a 20/04/2026. Origem na [Proposta de Lei n.º 111/XIV/2.ª \(GOV\)](#) - Regula a utilização de sistemas de vigilância por câmaras de vídeo pelas forças e serviços de segurança.

¹⁰ O uso de câmaras de vídeo pelas forças e serviços de segurança em locais públicos foi regulada pela primeira vez pela Lei Orgânica n.º 2/2004, de 12 de maio, que estabeleceu o regime temporário da organização da ordem pública e da justiça no contexto extraordinário da fase final do Campeonato Europeu de Futebol - Euro 2004. Coube à Lei n.º 1/2005, de 10 de janeiro, aprovar a utilização de câmaras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum. [Diplomas sobre videovigilância em vigor: [Lei n.º 51/2006, de 29 de agosto](#), regula a instalação e utilização de sistemas de vigilância eletrónica rodoviária e a criação e utilização de sistemas de informação de acidentes e incidentes pela EP - Estradas de Portugal, E. P. E., e pelas concessionárias rodoviárias; [Lei n.º 33/2007, de 13 de agosto](#), regula a instalação e utilização de sistemas de videovigilância em táxis; [Lei n.º 34/2013, de 16 de maio](#), que estabelece o regime do exercício da atividade de segurança privada (artigo 31.º regula a utilização de sistemas de videovigilância no âmbito daquela atividade); [Decreto-Lei n.º 135/2014, de 8 de setembro](#), regime jurídico dos sistemas de segurança privada dos estabelecimentos de restauração e de bebidas que disponham de salas ou de espaços destinados a dança ou onde habitualmente se dance.]

¹¹ Texto consolidado.

¹² [Trabalhos preparatórios](#).

¹³ [As medidas consagradas por esta lei destinam-se «em especial, a proteger a vida e a integridade das pessoas, a paz pública e a ordem democrática, designadamente contra o terrorismo, a criminalidade violenta ou altamente organizada, a sabotagem e a espionagem, a prevenir e reagir a acidentes graves ou catástrofes, a defender o ambiente e a preservar a saúde pública.»](#) n.º 3 do [artigo 1.º](#)

circulação de pessoas nas fronteiras externas; proteção florestal e deteção de incêndios rurais; e apoio em operações externas de busca e salvamento.

Admite-se ainda a instalação de sistemas de videovigilância em instalações policiais de atendimento ao público (n.º 2 do mesmo artigo).

A instalação de câmaras fixas e portáteis carece de autorização do membro do Governo que exerce a direção sobre a força ou serviço de segurança requerente ou da [Autoridade Nacional de Emergência e Proteção Civil](#) (ANEPC) e, ainda, de parecer prévio da [Comissão Nacional de Proteção de Dados](#) (CNPd), que se pronuncia sobre a conformidade do pedido face às regras referentes à segurança do tratamento dos dados recolhidos, bem como acerca das medidas especiais de segurança a implementar (n.ºs 1 e 3 do [artigo 5.º](#) e n.º 1 do [artigo 9.º](#)).

A utilização de câmaras de vídeo rege-se pelo princípio da proporcionalidade ([artigo 4.º](#)), referindo-se ainda que «na ponderação, caso a caso, da finalidade concreta a que o sistema de videovigilância se destina, deve ser considerada a possibilidade e o grau de afetação de direitos pessoais, decorrentes da utilização de câmaras de vídeo» (n.º 3). Sendo «vedada a utilização de câmaras de vídeo quando a captação de imagens e de sons abranja o interior de casa ou edifício habitado ou sua dependência, ou de estabelecimentos hoteleiros e similares, salvo consentimento dos proprietários e de quem o habite legitimamente, ou autorização judicial» e «a captação de imagens e sons quando essa captação afete, de forma direta e imediata, a esfera da reserva da vida íntima e privada» (n.ºs 5 e 6).

Relevante no que diz respeito à presente iniciativa é o [artigo 16.º](#) (Recolha e tratamento de dados) que prevê que o tratamento dos dados pode ter subjacente um sistema de gestão analítica dos dados captados, por aplicação de critérios técnicos, de acordo com os fins a que os sistemas se destinam, não sendo permitida a captação e tratamento de dados biométricos¹⁴.

¹⁴ Os dados biométricos são considerados dados sensíveis, pelo que só é legítimo proceder ao seu tratamento em duas situações: se houver uma lei que expressamente preveja esse tratamento e que, adicionalmente, estabeleça garantias para a defesa dos direitos dos titulares; ou se for obtido o consentimento do titular dos dados, nos termos legalmente exigíveis para o consentimento, ou seja, assegurando que o consentimento é explícito, informado, específico e dado livremente (CNPd). Nos termos do n.º 6 do [artigo 28.º](#) da Lei n.º 58/2019, de 8 de agosto: O tratamento de dados biométricos dos trabalhadores só é considerado legítimo para controlo de assiduidade e para controlo de acessos às instalações do empregador, devendo assegurar-se que apenas se utilizem representações dos dados

A responsabilidade¹⁵ pelo tratamento de imagens e sons ([artigo 17.º](#)) é da força ou serviço de segurança requerente ou da ANEPC com jurisdição na área de captação, regendo-se esse tratamento pelo disposto na [Lei n.º 59/2019, de 8 de agosto](#)¹⁶, que aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, transpondo a [Diretiva \(UE\) 2016/680](#) do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

Quando uma gravação, realizada de acordo com a lei em causa, registre a prática de factos com relevância criminal, a força ou serviço de segurança que utilize o sistema elabora auto de notícia, que remete ao Ministério Público juntamente com a respetiva autorização e o suporte original das imagens e sons, no mais curto prazo possível ou, no máximo, até 72 horas após o conhecimento da prática dos factos ([artigo 18.º](#)). A conservação das gravações obedece ao previsto no [artigo 19.º](#).

O exercício dos direitos de acesso e de eliminação¹⁷ são assegurados a todas as pessoas que figurem em gravações obtidas de acordo com esta lei, salvo nas seguintes situações, em que pode, fundamentadamente, ser recusado: quando seja suscetível de constituir perigo para a defesa do Estado ou para a segurança pública; quando prejudique investigações, inquéritos, processos judiciais, ou a prevenção, deteção, investigação ou repressão de infrações penais; para execução de sanções penais¹⁸. Estes direitos são exercidos perante o responsável pelo tratamento dos dados recolhidos, diretamente ou através da CNPD ([artigo 20.º](#)).

Compete à área governativa da administração interna a elaboração de um relatório bianual sobre a instalação e utilização de sistemas de videovigilância. E, ainda, através da Inspeção-Geral da Administração Interna, emitir recomendações que visem a melhoria dos procedimentos de recolha e tratamento de dados pessoais, através dos

biométricos e que o respetivo processo de recolha não permita a reversibilidade dos referidos dados. O [artigo 20.º](#) Código do Trabalho determina a licitude da utilização de meios de vigilância a distância no local de trabalho, mediante o emprego de equipamento tecnológico, sempre que tenha por finalidade a proteção e segurança de pessoas e bens ou quando particulares exigências inerentes à natureza da atividade o justifiquem. Ver também as considerações gerais relativas ao tratamento de dados biométricos nas [Diretrizes 3/2019](#) sobre tratamento de dados pessoais através de dispositivos de vídeo, do Comité Europeu para a Proteção de Dados e o seu [Parecer 18/2018](#) (no que respeita a dados biométricos).

¹⁵ Extensiva aos contratos celebrados com terceiros (nos termos do n.º 2).

¹⁶ Aplica-se em tudo o que não esteja especificamente previsto na Lei n.º 95/2021.

¹⁷ Nos termos dos artigos 13.º a 19.º da Lei n.º 59/2019, de 8 de agosto.

¹⁸ Nos termos dos artigos 16.º e 17.º da Lei n.º 59/2019, de 8 de agosto.

sistemas de videovigilância, sem prejuízo das atribuições e competências da CNPD ([artigo 21.º](#)).

A área governativa da administração interna publicita, através de plataforma eletrónica, todos os sistemas de videovigilância com câmaras fixas autorizados, onde conste a data e o local da instalação, o seu requerente e o fim a que se destina, devendo ser disponibilizada no [portal ePortugal.gov.pt](#), informação sobre a utilização de sistemas de videovigilância pelas forças e serviços de segurança, com hiperligação para a plataforma eletrónica ([artigo 23.º](#)).

A fiscalização do tratamento de dados recolhidos neste contexto é da competência da CNPD (n.º 1 do [artigo 24.º](#) da referida lei).

A Lei n.º 95/2021, de 29 de dezembro, foi regulamentada pelo [Decreto-Lei n.º 2/2023, de 2 de janeiro](#), que veio definir as normas de colocação, ativação, sinalização e utilização das câmaras portáteis de uso individual (CPUI), assim como a forma de transmissão, armazenamento e acesso aos dados recolhidos e as características e requisitos técnicos mínimos das mesmas.¹⁹

Neste contexto releva também a [Lei n.º 58/2019, de 8 de agosto](#), que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) [2016/679](#) do Parlamento 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 (Regulamento Geral sobre a Proteção de Dados).

Tendo presente a iniciativa em causa cumpre também fazer referência à [Lei n.º 52/2003, de 22 de agosto](#)²⁰, Lei de combate ao terrorismo (em cumprimento da Decisão Quadro n.º 2002/475/JAI, do Conselho, de 13 de junho), bem como à Estratégia Nacional de Combate ao Terrorismo (ENCT) que foi aprovada pela [Resolução do Conselho de Ministros n.º 40/2023, de 3 de maio](#).

A ENCT está organizada em torno de quatro eixos estratégicos - prevenir, proteger, perseguir e responder - cuja materialização assenta na contínua implementação dos

¹⁹ E também pelo [Despacho n.º 12141/2023, de 29 de novembro](#), renova a autorização de utilização do sistema de videovigilância na cidade de Lisboa, por um período de três anos, contabilizados a partir de 4 de janeiro de 2024.

²⁰ Alterou o artigo 1.º do Código de Processo Penal e o artigo 5.º do Código Penal e revogou os artigos 300.º e 301.º do Código Penal.

diversos planos de ação²¹ em vigor, bem como na definição de outras medidas concretas. É objeto de revisão quinquenal, da responsabilidade do Secretário-Geral do Sistema de Segurança Interna, sem prejuízo de revisões extraordinárias, sempre que as circunstâncias o exijam, tendo em vista a sua adequação à constante evolução da ameaça terrorista e aos desafios daí decorrentes. A sua execução é sujeita a uma avaliação anual, da responsabilidade da Unidade de Coordenação Antiterrorismo

Já o [Relatório Anual de Segurança Interna 2025](#) refere que, no ano de 2025, a Unidade de Coordenação Antiterrorismo (UCAT) integrada no Sistema de Segurança Interna veiculou 2441 comunicações, em sede de cooperação nacional e internacional, no âmbito da prevenção e do combate ao terrorismo, radicalização e fenómenos conexos. Afirma-se concretamente que o terrorismo e o extremismo continuam a integrar o leque de prioridades, estimando-se o agravamento destas ameaças, quer no plano interno, quer no contexto europeu.

Por fim, cumpre fazer referência à jurisprudência do Tribunal Constitucional (TC), designadamente, sobre videovigilância,²². Temática que também tem sido objeto de pronúncia pelos tribunais da Relação e Supremo Tribunal de Justiça²³, com foco na prova e nos princípios de necessidade, proporcionalidade²⁴ e ponderação entre segurança e direito à imagem e à reserva da intimidade da vida privada e familiar.²⁵

Do mesmo modo, poderão relevar neste contexto os Pareceres da CNPD: [2021/143](#) sobre a Proposta de Lei n.º 111/XIV/2.^a (GOV); [2022/102](#) e [2024/19](#), sobre tratamento de dados pessoais realizado através de um *sistema de gestão de analítica dos dados captados*; [2025/14](#), sobre a [Proposta de Lei n.º 45/XVI/1.^a \(ALRA\)](#), que estabelece a primeira alteração à Lei n.º 95/2021, de 29 de dezembro; e [2026/2](#) (nos termos do n.º 3 do artigo 5.º da Lei n.º. 95/2021, de 29 de dezembro). A CNPD tem salientado que a implementação de sistemas de videovigilância, especialmente com inteligência artificial,

²¹ Plano de Ação de Prevenção da Radicalização e dos Extremismos Violentos e do Recrutamento para o Terrorismo; Plano de Ação para a Proteção e Segurança das Infraestruturas Críticas; Plano de Ação da Comunicação; Plano de Ação Nacional para a Prevenção e Resposta a Incidentes de Segurança Químicos, Biológicos, Radiológicos e Nucleares (QBRN).

²² Por exemplo: [Acórdãos n.ºs 876/2014, 464/2019, 393/2019, 752/2024, 506/2024 e 393/2025](#).

²³ Acórdãos dos Tribunais [da Relação do Porto de 16-10-2024](#), [da Relação de Coimbra de 28-01-2026](#); [da Relação de Lisboa de 16/11/2011](#) e [do STJ de 28/09/2011](#); [de 2022-11-10](#) e [de 2022-04-28](#). Ver também jurisprudência sobre [prova digital](#) - Gabinete do cibercrime do MP.

²⁴ [Artigo 18.º](#), n.º 2 da Constituição.

²⁵ [Artigo 26.º](#), n.º 1 da Constituição.

deve ser acompanhada de uma avaliação de impacto²⁶ sobre a proteção de dados, e, concretamente, sobre o artigo 18.º (recolha e tratamento de dados) da Proposta de Lei n.º 111/XIV/2.ª (GOV), sublinhou que: «parece querer prever-se é o tratamento de dados biométricos de todos aqueles que se encontrem ou circulem no espaço público ou em espaço aberto ao público - numa lógica de recolha em massa de dados biométricos. Mas a norma não define aquilo que, neste quadro, seria crucial: se os dados biométricos vão constar de uma base de dados centralizada e quem será o responsável por tal sistema de informação», tendo concluído: «Em suma, o artigo 18.º da Proposta prevê um sistema de vigilância em massa por recurso genérico a tecnologias de análise de dados e de reconhecimento facial, o que representa uma restrição de direitos fundamentais dos cidadãos, sem cumprir os ditames do Estado de Direito, sequer quanto à imprescindível clareza e transparência quanto à previsão dessas restrições, e sem prever quaisquer garantias daqueles direitos, e por isso se revela violadora das exigências fixadas nos n.ºs 2 e 3 do artigo 18.º da CRP, sendo suscetível de afetar o conteúdo essencial do direito ao respeito pela vida privada e violando manifestamente o princípio da proporcionalidade.»

IV. ENQUADRAMENTO JURÍDICO NA UNIÃO EUROPEIA E INTERNACIONAL

▪ Âmbito da União Europeia

O [Tratado sobre o Funcionamento da União Europeia](#) prevê no artigo 16.º, n.º 1, que «Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito». O mesmo princípio pode ser igualmente encontrado no artigo 8.º da [Carta dos Direitos Fundamentais da UE](#), sob a epígrafe «proteção de dados» que determina que tais dados «devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por

²⁶ De acordo com informação disponibilizada pela CNPD: «A realização de uma avaliação de impacto sobre a proteção de dados (AIPD) é uma obrigação legal prevista no artigo 35.º do [RGPD](#) sempre que o tratamento de dados pessoais em causa assim o exigir, designadamente quando forem tratados em larga escala os dados pessoais previstos no artigo 9.º ou no artigo 10.º do RGPD; quando houver um controlo sistemático de zonas acessíveis ao público em larga escala (por exemplo, através de sistemas de videovigilância); quando forem feitas definições de perfis (*profiling*) e, subsequentemente, forem tomadas decisões automatizadas que afetem significativamente a pessoa singular. É também obrigatória a realização de uma AIPD no âmbito do procedimento legislativo ou regulamentar, a qual deve ser remetida à CNPD a acompanhar o pedido de parecer sobre essas disposições em preparação pelo órgão com poder legislativo ou regulamentar (cf. artigo 18.º, n.º 4, da [Lei 43/2004](#).»

lei» e que «Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação» (n.º 2), ficando o cumprimento destas regras «sujeito a fiscalização por parte de uma autoridade independente».

O [Regulamento \(UE\) 2016/679](#) do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) estabelece, no seio da União Europeia, as regras de proteção de dados.

Neste sentido, o artigo 4.º, n.º 1 do referido instrumento legal define «dados pessoais» como sendo a «informação relativa a uma pessoa singular identificada ou identificável (“titular dos dados”); considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular». O mesmo artigo define «Tratamento», como «uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição».

O [Regulamento \(EU\) 2024/1689](#) do Parlamento Europeu e do Conselho, de 13 de junho de 2024, cria regras harmonizadas em matéria de inteligência artificial (IA). O artigo 5.º estabelece as práticas de IA proibidas, entre as quais a «utilização de sistemas de identificação biométrica à distância “em tempo real” em espaços acessíveis ao público para efeitos da aplicação da lei, a menos e na medida em que essa utilização seja estritamente necessária» para um dos fins definidos, nomeadamente a «prevenção de uma ameaça específica, substancial e iminente à vida ou à segurança física de pessoas singulares ou de uma ameaça real e atual ou real e previsível de um ataque terrorista» (subalínea *ii*) da alínea *h*)).

A [Diretiva \(UE\) 2016/680](#) do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho, visa proteger os dados pessoais das pessoas singulares quando são tratados pelas autoridades policiais e judiciárias.

A [Autoridade Europeia para a Proteção de Dados](#) adotou, em janeiro de 2020, um conjunto de [orientações](#) sobre o tratamento de dados pessoais obtidos através de dispositivos de vídeo analisando a forma como o Regulamento Geral sobre a Proteção de Dados (RGPD) se aplica ao tratamento de dados pessoais por dispositivos de vídeo e como pode ser assegurada uma aplicação coerente do RGPD a este respeito. Mais recentemente, em abril de 2023, adotou [orientações](#) sobre o uso de tecnologia de reconhecimento facial no domínio da aplicação da lei.

Num [relatório sobre inteligência artificial e policiamento](#) datado de 2024, a Europol referiu que «para distinguir entre aplicações de identificação biométrica retrospectiva e em tempo real, é necessário reconhecer o papel destas últimas em cenários de resposta rápida, especialmente a sua utilidade na prevenção de ataques terroristas, na localização de crianças desaparecidas e na prevenção ou combate a crimes graves. No entanto, é igualmente necessário reconhecer os desafios e as considerações éticas associados à biometria em tempo real, que realçam a necessidade imperativa de uma implementação responsável e de um quadro regulamentar para garantir a privacidade e prevenir o uso indevido».

Na sequência da adoção da [Estratégia Europeia de Segurança Interna \(ProtectEU\)](#), a Comissão Europeia apresentou, em fevereiro de 2026, uma [nova agenda para a prevenção e a luta contra o terrorismo](#), definindo a via para reforçar a resposta coletiva da Europa à luz da evolução das ameaças terroristas e extremistas violentas, através de um conjunto de iniciativas transeuropeias para intensificar a preparação e resposta às ameaças e para melhorar a proteção das pessoas e das empresas da UE. Neste âmbito, «a Comissão, em conjunto com a Europol, reforçará a sua cooperação com países terceiros essenciais, a fim de obter dados biográficos e biométricos sobre indivíduos que possam representar uma ameaça terrorista, incluindo combatentes terroristas

estrangeiros, os quais poderão depois ser introduzidos no Sistema de Informação Schengen».

- **Âmbito internacional**

- Países analisados**

Apresenta-se, de seguida, o enquadramento internacional referente a: Espanha e Reino Unido.

ESPAÑA

No [artigo 129 bis](#) da [Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal](#)²⁷, permite-se ao juiz ou tribunal ordenar a colheita de amostras biológicas e a realização de análises para a obtenção de identificadores de ADN e a sua inscrição na base de dados policial, nos casos em que se trata de condenados pela prática de um crime grave contra a vida, a integridade das pessoas, a liberdade, a liberdade ou indemnidade sexual, de terrorismo, ou qualquer outro crime grave que implique um risco grave para a vida, a saúde ou a integridade física das pessoas, quando das circunstâncias do facto, antecedentes, avaliação da sua personalidade, ou de outra informação disponível se possa considerar que existe um perigo relevante de reincidência criminal.

Ressalva-se que, nestes casos, apenas poderão ser realizados os testes necessários para obter os identificadores que forneçam, exclusivamente, informação genética reveladora da identidade da pessoa e do seu sexo e que se o visado se opuser à colheita das amostras, poderá ser imposta a sua execução forçada mediante recurso às medidas coercivas mínimas indispensáveis para a sua execução, que deverão ser sempre proporcionais às circunstâncias do caso e respeitar a sua dignidade.

Por sua vez, a [Ley Orgánica 7/2021, de 26 de mayo](#)²⁸, de proteção de dados pessoais tratados para fins de prevenção, deteção, investigação e acusação de infrações penais e de execução de sanções penais tem como objetivo estabelecer, segundo o [artigo 1.º](#) as normas relativas à proteção das pessoas físicas no que diz respeito ao tratamento

²⁷ Texto consolidado retirado do portal legislativo espanhol [boe.es](#). Todas as referências legislativas relativas a Espanha são feitas para este portal oficial, salvo indicação em contrário (consultas efetuadas a 27/04/2026).

²⁸ Texto consolidado.

de dados de carácter pessoal por parte das autoridades competentes, para fins de prevenção, deteção, investigação e acusação de infrações penais ou de execução de sanções penais, incluindo a proteção e prevenção contra ameaças à segurança pública.

O [artigo 2.º](#) define o âmbito de aplicação desta lei. Segundo este, será aplicável ao tratamento total ou parcialmente automatizado de dados pessoais, assim como ao tratamento não automatizado de dados pessoais contidos ou destinados a ser incluídos num ficheiro, realizado pelas autoridades competentes, com fins de prevenção, deteção, investigação e acusação de infrações penais e de execução de sanções penais, incluindo a proteção e prevenção contra ameaças à segurança pública. Assim, as autoridades de proteção de dados não serão competentes para controlar estas operações de tratamento.

Segundo o [artigo 4](#), é considerada uma autoridade competente, além das autoridades judiciais da jurisdição penal e do Ministério Público, qualquer autoridade pública que tenha competências legalmente atribuídas para o tratamento de dados pessoais com algum dos fins previstos *supra*.

Cumprir referir que, para efeitos desta lei, incluem toda a informação relativa a uma pessoa singular identificada ou identificável (“o titular dos dados”) e considera-se, por sua vez, pessoa singular identificável toda a pessoa cuja identidade possa ser determinada, direta ou indiretamente, em particular mediante um identificador, como por exemplo um nome, um número de identificação, dados de localização, um identificador em linha ou um ou vários elementos próprios da identidade física, fisiológica, genética, psíquica, económica, cultural ou social dessa pessoa ([artigo 5.º](#)).

No tocante aos dados biométricos, definidos no mesmo artigo como dados pessoais obtidos a partir de um tratamento técnico específico, relativos às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa, como imagens faciais ou dados impressões digitais, o [artigo 13.º](#) regula o seu tratamento.

Desta forma, o tratamento de dados genéticos, dados biométricos destinados a identificar de forma unívoca uma pessoa singular, dados relativos à saúde ou à vida sexual ou à orientação sexual de uma pessoa singular só será permitido quando seja estritamente necessário, com sujeição às garantias adequadas para os direitos e

liberdades do titular dos dados e quando se verifique alguma das seguintes circunstâncias:

- a) Esteja previsto por uma norma com força de lei ou pelo Direito da União Europeia.
- b) Seja necessário para proteger os interesses vitais, bem como os direitos e liberdades fundamentais do titular dos dados ou de outra pessoa singular.
- c) Esse tratamento diga respeito a dados que o titular tenha tornado manifestamente públicos.

É permitido às autoridades competentes tratar dados biométricos destinados a identificar de forma unívoca uma pessoa singular com fins de prevenção, investigação e deteção de infrações penais, incluindo a proteção e prevenção de ameaças à segurança pública.

Cumpra ainda referir a [Ley Orgánica 1/2020, de 16 de septiembre](#)²⁹, sobre a utilização dos dados do Registo de Nomes de Passageiros para a prevenção, deteção, investigação e acusação de crimes de terrorismo e crimes graves, que permite, no [artigo 1](#), com o propósito de garantir e proteger a vida e a segurança dos cidadãos,

- a) A transferência de dados do registo de nomes dos passageiros (doravante dados PNR) e
- b) Recolher, utilizar, armazenar, tratar, proteger, aceder e conservar os dados PNR, a transmitir esses dados às autoridades competentes, bem como o intercâmbio dos mesmos com os Estados-membros da União Europeia, com a Europol e com países terceiros.

Determina o [artigo 2](#) que Esta lei orgânica será aplicável, em todos os casos, aos dados PNR correspondentes às pessoas que viajem em voos internacionais, tanto dentro como fora da União Europeia, com partida do território espanhol ou chegada ao mesmo, ou que nele façam escala e o [artículo 4](#) apresenta a definição de delitos de terrorismo e delitos graves, para efeitos desta lei.

REINO UNIDO

²⁹ Texto consolidado.

O [Protection of Freedoms Act 2012](#) (POFA 2012)³⁰ introduziu um novo quadro jurídico que regula a retenção e eliminação de dados biométricos pela polícia.

Lê-se, na sua [explanatory note](#), que o quadro existente para a recolha, conservação e destruição de impressões digitais, impressões de calçado, amostras de ADN e perfis derivados dessas amostras está estabelecido na [Parte V](#) da [Police and Criminal Evidence Act 1984](#) (“PACE”)³¹.

As alterações à PACE introduzidas pela Criminal Justice and [Public Order Act 1994](#)³² permitiram que fossem recolhidas amostras de ADN de qualquer pessoa acusada, chamada a responder por notificação judicial, advertida ou condenada por um crime registável; e permitiram que os perfis obtidos a partir dessas amostras fossem conservados e comparados de forma especulativa com outros perfis obtidos de vítimas ou de locais de crime. Um crime registável é definido na [secção 118](#) da PACE. Na prática, todos os crimes puníveis com pena de prisão são crimes registáveis, assim como cerca de 60 outros crimes não puníveis com prisão que estão especificados em regulamentos adotados. Se a pessoa fosse absolvida, as amostras e os perfis tinham de ser destruídos.

A [Criminal Justice and Police Act 2001](#)³³ alterou ainda a PACE, eliminando a obrigação de destruir uma amostra de ADN ou o perfil correspondente quando um suspeito não fosse acusado ou fosse absolvido do crime de que era suspeito. O poder de recolher e conservar amostras de ADN e perfis foi posteriormente alargado pela [Criminal Justice Act 2003](#)³⁴, que permitiu a recolha de uma amostra de ADN de qualquer pessoa detida por um crime registável numa esquadra de polícia, independentemente de vir ou não a ser acusada. Qualquer dessas amostras, bem como o perfil delas derivado, podia ser conservado por tempo indeterminado.

Em dezembro de 2008, no caso [S and Marper v United Kingdom](#) no [Tribunal Europeu dos Direitos Humanos](#) (“TEDH”)³⁵ decidiu que as disposições da PACE que permitiam a

³⁰ Texto consolidado retirado do portal legislativo do Reino Unido [Legislation.gov.uk](#). Todas as referências legislativas relativas ao Reino Unido são feitas para este portal oficial, salvo indicação em contrário (consultas efetuadas a 27/04/2026).

³¹ Texto consolidado.

³² Texto consolidado.

³³ Texto consolidado.

³⁴ Texto consolidado.

³⁵ Portal oficial.

conservação “generalizada e indiscriminada” de ADN de pessoas não condenadas, violavam o artigo 8.º (direito à vida privada) da [Convenção Europeia dos Direitos Humanos](#) (“CEDH”)³⁶. Em resposta, foram introduzidas disposições, que correspondem aos artigos [14](#) a [23](#) da [Crime and Security Act 2010](#)³⁷, que, entre outras coisas, permitiam a conservação de impressões digitais e perfis de ADN de pessoas detidas por, mas não condenadas por, qualquer crime registável durante seis anos.

Mais tarde, o [Counter-Terrorism and Border Security Act 2019](#)³⁸, que visou melhorar a legislação existente relativa à retenção de impressões digitais e perfis de ADN, com o objetivo de reforçar a capacidade da polícia para utilizar estes dados no apoio a investigações de combate ao terrorismo, alterou vários diplomas legais no que respeita à retenção de dados biométricos para fins de combate ao terrorismo e outros fins de segurança nacional.

Nesta sequência, o Governo do Reino Unido publicou uma [Biometric Data Factsheet](#)³⁹, na qual são descritas as alterações que este ato legislativo introduz no ordenamento jurídico britânico.

Em termos gerais, o ato legislativo:

- altera a legislação relativa à retenção de dados biométricos, simplificando e tornando o regime mais eficiente, nomeadamente aumentando a duração máxima de uma *National Security Determination* (NSD) de dois para cinco anos;
- harmoniza os prazos de retenção de dados biométricos quando indivíduos são detidos por suspeita de crimes de terrorismo ao abrigo do PACE e do *Terrorism Act 2000* (TACT);
- permite que a polícia trate múltiplos conjuntos de dados biométricos recolhidos em diferentes ocasiões (mas relativos à mesma pessoa) como um único registo consolidado, possibilitando a aplicação de uma única NSD a várias impressões digitais;

³⁶ Texto consolidado retirado do portal oficial do TEDH.

³⁷ Texto consolidado.

³⁸ Texto consolidado.

³⁹ Portal oficial do [Governo do Reino Unido](#).

- autoriza os chefes de polícia a emitir NSDs que legitimem a retenção de dados biométricos recolhidos fora da sua própria área de jurisdição.

A ficha define “dados biométricos” como o termo utilizado para impressões digitais e perfis de ADN (identificadores únicos obtidos a partir de uma amostra física de ADN, a qual é destruída após a criação do perfil). Os dados biométricos podem ser utilizados para identificar uma pessoa específica e são habitualmente utilizados pela polícia em todo o tipo de processos criminais.

Desta forma, um chefe de polícia pode emitir uma NSD para autorizar a retenção, por um período até cinco anos, de dados biométricos que, de outro modo, teriam de ser apagados pela polícia, desde que tal seja necessário para fins de segurança nacional e seja considerado proporcional.

Organizações internacionais

CEPD

O [Comité Europeu para a Proteção de Dados](#)⁴⁰ - CEPD é um organismo independente da UE, dotado de personalidade jurídica e que tem sede em Bruxelas. Foi estabelecido pelo RGPD.

O Comité Europeu é composto por representantes das autoridades nacionais de proteção de dados da UE e pela Autoridade Europeia de Proteção de Dados (AEPD). As autoridades dos Estados EFTA/EEE (Islândia, Liechtenstein e Noruega) também são membros para as matérias do RGPD, mas sem direito a voto. A CNPD é membro do Comité Europeu e participa ativamente nos seus trabalhos, em particular através da participação nos vários subgrupos de peritos do Comité.

O Comité Europeu aprova diretrizes, recomendações e boas práticas e emite decisões vinculativas destinadas às autoridades nacionais de proteção de dados com vista ao controlo da coerência na aplicação do RGPD. Emite pareceres à Comissão Europeia sobre quaisquer matérias de proteção de dados, incluindo sobre legislação em preparação.

INTERPOL

⁴⁰ Portal oficial.

Segundo [comunicado](#) datado de 8 de dezembro de 2017, os dados biométricos são utilizados pelas autoridades policiais como ferramenta de apoio à identificação de pessoas no contexto da luta contra o crime e o terrorismo.

A [INTERPOL](#)⁴¹ refere que estes dados podem ajudar a identificar indivíduos que utilizam identidades falsas ou múltiplas e que a cooperação internacional e a partilha de bases de dados biométricas entre países são elementos relevantes para esse trabalho policial.

V. ENQUADRAMENTO PARLAMENTAR

▪ Iniciativas pendentes (iniciativas legislativas e petições)

Consultada a base de dados da atividade parlamentar, verifica-se que, sobre matérias conexas com o objeto do projeto de lei em análise, estão pendentes as seguintes iniciativas:

- [Proposta de Lei n.º 53/XVII/1.ª \(GOV\)](#) - Transpõe a Diretiva (UE) 2023/977, relativa ao intercâmbio de informações entre as autoridades de aplicação da lei dos Estados-Membros, e a Diretiva (UE) 2023/2123, que altera a Decisão 2005/671/JAI do Conselho no que diz respeito à sua harmonização com as regras da União em matéria de proteção de dados pessoais;

- [Proposta de Lei 45/XVI/1.ª \(ALRAA\)](#) - Primeira alteração à Lei n.º 95/2021, de 29 de dezembro, que regula a utilização e o acesso pelas forças e serviços de segurança e pela Autoridade Nacional de Emergência e Proteção Civil a sistemas de vigilância para captação, gravação e tratamento de imagem e som

▪ Antecedentes parlamentares (iniciativas legislativas e petições)

Compulsada a mesma base de dados, constata-se que, na XVI Legislatura, atendendo à rejeição da moção de confiança e à consequente demissão do Governo, foi [devolvido sem promulgação](#) o [Decreto da Assembleia da República 50/XVI](#) - Autoriza o Governo a adaptar a ordem jurídica interna ao Regulamento (UE) 2021/784 do Parlamento

⁴¹ Portal oficial.

Europeu e do Conselho, de 29 de abril de 2021, relativo ao combate à difusão de conteúdos terroristas em linha.

Importa destacar que, na XIV Legislatura, a [Proposta de Lei n.º 111/XIV/2.ª \(GOV\)](#) - *Regula a utilização de sistemas de vigilância por câmaras de vídeo pelas forças e serviços de segurança* deu origem à [Lei n.º 95/2021](#), de 29 de dezembro, diploma que os proponentes da iniciativa em análise pretendem alterar.

VI. CONSULTAS E CONTRIBUTOS

Em 22 de abril de 2026, a Comissão solicitou parecer sobre a iniciativa às seguintes entidades: [Conselho Superior de Magistratura](#), Conselho Superior do Ministério Público, Ordem dos Advogados e [Comissão Nacional de Proteção de Dados](#).

Todos os pareceres e contributos recebidos serão disponibilizados na [página da iniciativa](#).

Nos termos do disposto no artigo 134.º do RAR, a iniciativa encontra-se em [consulta pública](#) até ao início da respetiva votação na especialidade, salvo rejeição na generalidade. Os contributos que venham a ser recebidos serão igualmente disponibilizados no *site* da Assembleia da República na referida [página eletrónica](#).

VII. ENQUADRAMENTO BIBLIOGRÁFICO

BONDARENKO, Yevhen; SVOBODA, Ivo; TKACHOV, Ivan, KOZENKO, Oleksandr; VISLOVUKH, Volodymyr. The Impact of Biometric Technologies on the Efficiency of Terrorist Crime Investigation. Em Linha. *Revista Jurídica Portucalense*, n.º 38 (2025), pp. 206-223. Disponível em: <https://revistas.rcaap.pt/juridica/article/view/40228/29187> [visualizado em 2026-04-27]

Resumo: «A importância da tecnologia biométrica na investigação de crimes terroristas está a aumentar devido ao aumento das ameaças à segurança global e à necessidade de melhorar a eficácia da aplicação da lei. O principal objetivo deste artigo é analisar a aplicação de tecnologias biométricas para melhorar a eficácia da deteção e detenção de terroristas em diferentes regiões do mundo. A metodologia de investigação inclui a

análise de dados estatísticos, o cálculo de médias ponderadas e a previsão de cenários relativos a ataques terroristas. O estudo identifica os principais factores associados à biometria, incluindo o reconhecimento facial, a análise de impressões digitais e as tecnologias de digitalização da retina, e descreve o seu potencial impacto no aumento das taxas de resolução de crimes. Os resultados mostram que a utilização de sistemas biométricos reduz significativamente o número de crimes terroristas não resolvidos, melhora a coordenação da aplicação da lei e ajuda na prevenção precoce de ameaças. O artigo discute vários desafios que os países enfrentam na resolução de crimes, tais como infra-estruturas subdesenvolvidas e adoção inadequada de tecnologias modernas. O significado prático do estudo reside no facto de fornecer recomendações para melhorar a cooperação internacional e continuar a implementar tecnologias biométricas para garantir a segurança global. A investigação futura deve centrar-se na exploração de novas formas de integração das tecnologias biométricas nos sistemas de aplicação da lei e na sua adaptação à evolução das ameaças.» [Do resumo]

GOSWAMI, Parineeta. *Privacy Under the Lens of Biometrics*. Em Linha. [S.l.]: SSRN, 2025. Disponível em: <http://dx.doi.org/10.2139/ssrn.5102266> [visualizado em 2026-04-27]

Resumo: «Este capítulo explora a relação entre os direitos à privacidade e os sistemas biométricos. Aprofunda o quadro jurídico que rege os direitos à privacidade (incluindo instrumentos internacionais de direitos humanos e regulamentações regionais), como o Regulamento Geral sobre a Proteção de Dados da União Europeia. O capítulo identifica os desafios das tecnologias biométricas no que diz respeito à privacidade, tais como a vigilância por parte de entidades estatais, as vulnerabilidades de segurança e as complexidades em torno do consentimento informado. A interseção entre dados biométricos e direitos de propriedade intelectual também foi analisada, explorando questões de propriedade e controlo.» [Do resumo]

HUSZTI-ORBÁN, Krisztina; NÍ AOLÁIN, Fionnuala. Use of biometric data to identify terrorists: best practice or risky business?. Em Linha. [Minneapolis]: University of Minnesota. Human Rights Center, 2020. Disponível em: <https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/biometricsbrochure-en.pdf> [visualizado em 2026-04-27]

Resumo: «[...] Este relatório explora as implicações em matéria de direitos humanos decorrentes da utilização de ferramentas e dados biométricos, com especial destaque para os desafios que se colocam à sua implementação em conformidade com os direitos humanos no contexto da prevenção e do combate ao terrorismo e ao extremismo violento. O relatório apresenta um resumo das formas como os dados e as ferramentas biométricas são utilizados, nomeadamente no contexto da luta contra o terrorismo. Em seguida, expõe as implicações em matéria de direitos humanos decorrentes da utilização da biometria, incluindo, entre outros, os direitos à privacidade e à proteção de dados, e delinea tanto as obrigações do Estado como as responsabilidades das empresas a este respeito. Por fim, apresenta um conjunto de recomendações sobre medidas destinadas a promover uma abordagem baseada nos direitos humanos relativamente à utilização de ferramentas e dados biométricos.» [Da introdução]

JACOBSEN, Katja Lindskov. Biometric data flows and unintended consequences of counterterrorism. Em Linha. *International Review of the Red Cross*, vol. 103, n.º 916-917 (2021), pp.619–652. Counterterrorism, sanctions and war. Disponível em: <https://international-review.icrc.org/sites/default/files/reviews-pdf/2022-02/biometric-data-flows-and-unintended-consequences-of-counterterrorism-916.pdf> [visualizado em 2026-04-27]

Resumo: «Ao examinar as consequências indesejadas da produção e do tratamento de dados biométricos em contextos de combate ao terrorismo e humanitários, este artigo apresenta um quadro duplo através do qual analisa a produção e os fluxos de dados biométricos no Afeganistão e na Somália. Combina a noção de “laboratório vivo” de Tilley e a noção de infraestrutura de Larkin numa estrutura que aborda as condições sob as quais os dados biométricos são produzidos e os fluxos subsequentes desses dados através de acordos de partilha de dados ou acesso não planeado. Ao explorar essas consequências indesejadas, é necessário prestar atenção à variedade de atores que utilizam a biometria para diferentes fins, mas com fluxos de dados que atravessam essas diferenças. Assim, o artigo introduz a noção de infraestruturas de intervenção digital, tendo as bases de dados biométricos como uma das suas dimensões.» [Do resumo]

SIMMLER, Monika; CANOVA, Giulia. Facial recognition technology in law enforcement: regulating data analysis of another kind. Em Linha. *Computer Law & Security Review*:

The International Journal of Technology Law and Practice, nº 56 (2025), pp. 1-10.

Disponível

em:

<https://www.sciencedirect.com/science/article/pii/S0267364924001572/pdf?md5=a6dd31fb942a730a357b78b9a8dca8f&pid=1-s2.0-S0267364924001572-main.pdf>

[visualizado em 2026-04-27]

Resumo: «A tecnologia de reconhecimento facial (FRT) surgiu como uma ferramenta poderosa para as forças policiais, permitindo a identificação automatizada de indivíduos com base nas suas características faciais únicas. As autoridades têm recorrido cada vez mais a esta tecnologia para melhorar as investigações criminais através da análise de imagens e gravações de vídeo. Tendo em conta a sua utilização crescente na Europa, este artigo explora as implicações jurídicas da FRT no âmbito da aplicação da lei ao abrigo do direito da UE e avalia as abordagens regulamentares. A utilização da FRT constitui um tratamento de dados biométricos e implica uma análise particularmente sensível dos dados. A sua natureza específica assenta na criação de uma nova qualidade (biométrica) dos dados, a fim de posteriormente comparar e identificar correspondências. Devido ao seu impacto nos direitos fundamentais, esta abordagem difere das análises forenses convencionais e deve ser devidamente regulamentada. Tal regulamentação deve ter em conta as múltiplas etapas do tratamento de dados e refletir o impacto de cada etapa nos direitos fundamentais. A partir desta perspetiva processual, as lacunas da Lei da Inteligência Artificial da UE (Lei da IA) tornam-se evidentes. A Lei da IA contém regras específicas para sistemas de IA biométricos, mas não fornece as bases jurídicas necessárias para justificar a utilização da FRT pelas autoridades policiais. Sem um quadro jurídico abrangente, tal utilização não é permitida. Este artigo fornece orientações concretas para abordar essa regulamentação.» [Do resumo]