Diretrizes

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Orientações 05/2022 sobre a utilização da tecnologia de reconhecimento facial no domínio da aplicação da lei

Versão 2.0

Adotadas em 26 de abril de 2023

Histórico de versões

Versão 1.0	12 de maio de 2022	Adoção das orientações para consulta pública
Versão 2.0	26 de abril de 2023	Adoção das orientações após consulta pública

Índice

SÍNTESE

Cada vez mais autoridades de aplicação da lei aplicam ou tencionam aplicar tecnologias de reconhecimento facial (TRF). Estas podem ser utilizadas para **autenticar** ou **identificar** uma pessoa e podem ser aplicadas a vídeos (por exemplo, imagens de televisão em circuito fechado – CCTV) ou fotografias. Podem ser utilizadas para diversas finalidades, nomeadamente para procurar pessoas que façam parte de listas de observação da polícia ou para seguir os movimentos de uma pessoa no espaço público.

A TRF baseia-se no tratamento de **dados biométricos**, pelo que abrange o tratamento de categorias especiais de dados pessoais. Muitas vezes, a TRF utiliza componentes de **inteligência artificial** (IA) ou de aprendizagem automática o que permite o tratamento de dados em grande escala, embora também implique um risco de discriminação e de resultados falsos. A TRF pode ser utilizada em situações controladas de 1:1, mas também em grandes multidões e em importantes plataformas de transporte.

A TRF é uma **ferramenta sensível para as autoridades de aplicação da lei.** As autoridades de aplicação da lei são autoridades executivas com direitos soberanos. A TRF é propensa a interferir com os direitos fundamentais – nomeadamente além do direito à proteção dos dados pessoais – e é capaz de afetar a nossa estabilidade política social e democrática.

Para garantir a proteção dos dados pessoais no contexto da aplicação da lei, é necessário cumprir os **requisitos da Diretiva Proteção de Dados na Aplicação da Lei**. A Diretiva Proteção de Dados na Aplicação da Lei define um determinado regime relativo à utilização de TRF, nomeadamente o artigo 3.º, ponto 13, da diretiva (definição do termo «dados biométricos»), o artigo 4.º (princípios relativos ao tratamento de dados pessoais), o artigo 8.º (licitude do tratamento), o artigo 10.º (tratamento de categorias especiais de dados pessoais) e o artigo 11.º (decisões individuais automatizadas).

A aplicação de TRF pode afetar também vários outros direitos fundamentais. Por conseguinte, a **Carta dos Direitos Fundamentais da UE** (a seguir designada por «Carta») é essencial para a interpretação da Diretiva Proteção de Dados na Aplicação da Lei, nomeadamente o direito à proteção dos dados pessoais previsto no artigo 8.º da Carta, mas também o direito à privacidade previsto no artigo 7.º da Carta.

As **medidas legislativas** que servem de base jurídica para o tratamento dos dados pessoais são constitutivas de uma ingerência direta nos direitos garantidos pelos artigos 7.º e 8.º da Carta. O tratamento de dados biométricos, seja em que circunstância for, constitui, por si só, uma ingerência grave. Esta não depende do resultado, por exemplo uma correspondência positiva. Qualquer restrição ao exercício dos direitos e liberdades fundamentais deve ser prevista por lei e respeitar o conteúdo essencial desses direitos e liberdades.

Os termos da base jurídica devem ser **suficientemente claros** para dar aos cidadãos uma indicação adequada das condições e das circunstâncias em que as autoridades têm poderes para recorrer a quaisquer medidas de recolha de dados e de vigilância secreta. Uma mera transposição para o direito nacional da cláusula geral do artigo 10.º da Diretiva Proteção de Dados na Aplicação da Lei careceria de rigor e previsibilidade.

Antes de criar uma base jurídica para qualquer forma de tratamento de dados biométricos que utilize reconhecimento facial, o legislador nacional deve **consultar** a autoridade de controlo competente em matéria de proteção de dados.

As medidas legislativas têm de ser **adequadas** para alcançar os objetivos legítimos da legislação em causa. Um **objetivo de interesse geral**, por muito fundamental que seja, não pode, por si só, justificar uma restrição a um direito fundamental. As medidas legislativas devem **diferenciar** e visar as pessoas abrangidas pelo seu âmbito de aplicação em função do respetivo objetivo, por exemplo de combater um tipo específico de criminalidade grave. Se a medida abranger todas as pessoas de um modo geral, sem essa diferenciação, limitação ou exceção, a ingerência é intensificada. A ingerência é igualmente intensificada se o tratamento de dados abranger uma parte significativa da população.

Os dados têm de ser tratados de uma forma que garanta a aplicabilidade e a eficácia das regras e princípios da UE em matéria de proteção de dados. Dependendo da situação específica, a **avaliação da necessidade e da proporcionalidade** tem também de identificar e ponderar todas as repercussões possíveis noutros direitos fundamentais. Se os dados forem sistematicamente tratados sem o conhecimento dos respetivos titulares, é provável que se gere uma **sensação geral de vigilância constante**. Este sentimento pode produzir efeitos dissuasores em relação à totalidade ou a parte dos direitos fundamentais em causa, tais como a dignidade humana nos termos do artigo 1.º da Carta, a liberdade de pensamento, de consciência e de religião nos termos do artigo 10.º da Carta, a liberdade de expressão nos termos do artigo 11.º da Carta, bem como a liberdade de reunião e de associação nos termos do artigo 12.º da Carta.

O tratamento de categorias especiais de dados, como os dados biométricos, só pode ser considerado como «**estritamente necessário**» (artigo 10.º da Diretiva Proteção de Dados na Aplicação da Lei) se a ingerência na proteção dos dados pessoais e nas suas limitações se circunscrever ao absolutamente necessário, isto é, indispensável, e excluindo qualquer tratamento de natureza geral ou sistemática.

O facto de uma fotografia ter sido **manifestamente tornada pública** (artigo 10.º da Diretiva Proteção de Dados na Aplicação da Lei) pelo titular dos dados não implica que se possa considerar que os dados biométricos correspondentes que possam ser extraídos da fotografia por meios técnicos específicos tenham sido manifestamente tornados públicos. Quaisquer dados divulgados na sequência das configurações predefinidas de um serviço, por exemplo a disponibilização de modelos ao público, ou da ausência de escolha, por exemplo o facto de os modelos serem tornados públicos sem que o utilizador possa alterar essa configuração, não devem de forma alguma ser considerados dados manifestamente tornados públicos.

O artigo 11.º da Diretiva Proteção de Dados na Aplicação da Lei estabelece um enquadramento para as **decisões individuais automatizadas**. A utilização de TRF implica a utilização de categorias especiais de dados e pode conduzir à definição de perfis, dependendo da forma como a TRF é utilizada e da sua finalidade. De qualquer das formas, em conformidade com o direito da União e com o artigo 11.º, n.º 3, da Diretiva Proteção de Dados na Aplicação da Lei, são proibidas as definições de perfis que conduzam à discriminação de pessoas singulares com base em categorias especiais de dados pessoais.

O artigo 6.º da Diretiva Proteção de Dados na Aplicação da Lei diz respeito à necessidade de **distinguir entre diferentes categorias de titulares de dados**. No que diz respeito aos titulares de dados em relação aos quais não haja indícios que levem a acreditar que o seu comportamento possa ter um nexo, ainda que indireto ou longínquo, com o objetivo legítimo de acordo com a diretiva, muito provavelmente não há justificação para uma ingerência.

O **princípio da minimização dos dados** (artigo 4.º, n.º 1, alínea e), da Diretiva Proteção de Dados na Aplicação da Lei) também exige que qualquer material de vídeo que não seja pertinente para a finalidade do tratamento seja sempre removido ou anonimizado (por exemplo, através de desfocagem, sem possibilidade de recuperação retroativa dos dados) antes da sua utilização.

O responsável pelo tratamento tem de ponderar cuidadosamente (se ou) de que forma pode cumprir os requisitos relativos aos **direitos do titular dos dados** antes de ser iniciado qualquer tratamento com TRF, uma vez que a TRF implica frequentemente o tratamento de categorias especiais de dados pessoais sem qualquer interação aparente com o titular dos dados.

O exercício efetivo dos direitos do titular dos dados depende do cumprimento, pelo responsável pelo tratamento, das suas **obrigações de informação** (artigo 13.º da Diretiva Proteção de Dados na Aplicação da Lei). Ao avaliar se se trata de um «determinado caso» nos termos do artigo 13.º, n.º 2, da Diretiva Proteção de Dados na Aplicação da Lei, há que ter em conta vários fatores, nomeadamente se os dados pessoais são recolhidos sem o conhecimento do respetivo titular, uma vez que esta seria a única forma de permitir aos titulares dos dados exercerem efetivamente os seus direitos. Se a decisão for tomada exclusivamente com base em TRF, os titulares dos dados têm de ser informados das características da decisão automatizada.

No que diz respeito aos **pedidos de acesso**, quando os dados biométricos estão armazenados e ligados a uma identidade também por dados alfanuméricos, em conformidade com o princípio da minimização dos dados, tal deve permitir à autoridade competente confirmar um pedido de acesso com base numa pesquisa por esses dados alfanuméricos e sem iniciar qualquer outro tratamento de dados biométricos de terceiros (por exemplo, pesquisando com TRF numa base de dados).

Os riscos para os titulares dos dados são particularmente graves se os dados inexatos forem armazenados numa base de dados da polícia e/ou partilhados com outras entidades. O responsável pelo tratamento deve **corrigir** os dados armazenados e os sistemas de TRF em conformidade (ver também o considerando 47 da Diretiva Proteção de Dados na Aplicação da Lei).

O direito à **limitação** torna-se especialmente importante quando se trata de tecnologia de reconhecimento facial (baseada em algoritmos e que, por isso, nunca apresente um resultado definitivo) em situações em que sejam recolhidas grandes quantidades de dados e em que a exatidão e a qualidade da identificação possam variar.

Uma **avaliação de impacto sobre a proteção de dados (AIPD)** antes da utilização de TRF é um requisito obrigatório, conforme previsto no artigo 27.º da Diretiva Proteção de Dados na Aplicação da Lei. O Comité Europeu para a Proteção de Dados (CEPD) recomenda a divulgação ao público dos resultados dessas avaliações ou, pelo menos, das principais constatações e conclusões da AIPD, como medida de reforço da confiança e da transparência.

A maioria dos casos de implantação e utilização de TRF comporta um risco intrinsecamente elevado para os direitos e as liberdades dos titulares dos dados. A autoridade que implanta a TRF deve, por isso, **consultar** a autoridade de controlo competente antes da implantação do sistema.

Dada a natureza única dos dados biométricos, a autoridade que aplica e/ou utiliza a TRF deve prestar especial atenção à **segurança do tratamento**, em conformidade com o artigo 29.º da Diretiva Proteção de Dados na Aplicação da Lei. Concretamente, a autoridade de aplicação da lei deve assegurar que o sistema cumpre as normas pertinentes e aplica medidas de proteção de modelos biométricos. Os princípios e as garantias de proteção de dados devem ser incorporados na tecnologia antes do início do tratamento dos dados pessoais. Por conseguinte, mesmo quando tencionam aplicar e utilizar TRF de fornecedores externos, as autoridades de aplicação da lei têm de garantir, por exemplo através do procedimento de adjudicação de contratos, que apenas são utilizadas TRF baseadas nos princípios da **proteção de dados desde a conceção e por defeito**.

O **registo cronológico** (ver artigo 25.º da Diretiva Proteção de Dados na Aplicação da Lei) é uma garantia importante para a verificação da licitude do tratamento, tanto a nível interno (ou seja, autocontrolo pelo responsável pelo tratamento/subcontratante em causa) como por autoridades de controlo externas. No contexto dos sistemas de reconhecimento facial, recomenda-se o registo cronológico também das alterações da base de dados de referência e das tentativas de identificação ou verificação, incluindo o utilizador, o resultado e a pontuação de confiança. No entanto, o registo cronológico é apenas um elemento essencial do **princípio da responsabilização** geral (ver artigo 4.º, n.º 4, da Diretiva Proteção de Dados na Aplicação da Lei). O responsável pelo tratamento tem de ser capaz de demonstrar a conformidade do tratamento com os princípios básicos de proteção de dados previstos no artigo 4.º, n.ºs 1 a 3, da Diretiva Proteção de Dados na Aplicação da Lei.

O CEPD recorda o seu **apelo** conjunto com a Autoridade Europeia para a Proteção de Dados (AEPD) **à proibição** de certos tipos de tratamento em relação a (1) identificação biométrica de indivíduos, à distância, em zonas acessíveis ao público, (2) sistemas de reconhecimento facial apoiados por IA que agrupem indivíduos com base nos seus dados biométricos de acordo com a etnia, o género, a orientação política ou sexual ou outros motivos de discriminação, (3) utilização do reconhecimento facial ou de tecnologias semelhantes para inferir as emoções de uma pessoa singular e (4) tratamento de dados pessoais num contexto de aplicação da lei que se baseie numa base de dados preenchida através da recolha de dados pessoais em massa e de forma indiscriminada, por exemplo através da «raspagem» de fotografias e imagens faciais acessíveis em linha.

Uma salvaguarda central dos direitos fundamentais em causa é a **supervisão eficaz** por parte das autoridades de controlo competentes em matéria de proteção de dados. Por conseguinte, os Estados-Membros têm de assegurar que os recursos das autoridades de controlo são adequados e suficientes para lhes permitir cumprir o seu mandato.

As presentes **orientações dirigem-se** aos legisladores a nível nacional e da UE, bem como às autoridades de aplicação da lei e aos seus agentes que aplicam e utilizam sistemas de TRF. As pessoas são abordadas na qualidade de partes interessadas ou de titulares de dados, nomeadamente no que diz respeito aos direitos dos titulares dos dados.

As **orientações visam** transmitir informações sobre certas propriedades das TRF e sobre o quadro jurídico aplicável no contexto da aplicação da lei (em particular a Diretiva Proteção de Dados na Aplicação da Lei).

- Além disso, constituem uma **ferramenta de apoio a uma primeira classificação da natureza sensível de um determinado caso de utilização** (anexo I).
- Contêm igualmente **orientações práticas para as autoridades de aplicação da lei que pretendam adquirir e utilizar um sistema de TRF** (anexo II).
- As orientações descrevem ainda vários **casos de utilização típicos e enumeram várias considerações pertinentes**, especialmente no que diz respeito ao teste da necessidade e da proporcionalidade (anexo III).

1 INTRODUÇÃO

1. A tecnologia de reconhecimento facial (TRF) pode ser utilizada para reconhecer automaticamente as pessoas com base no seu rosto. A TRF baseia-se frequentemente na inteligência artificial, nomeadamente em tecnologias de aprendizagem automática. As aplicações de TRF são cada vez mais testadas e utilizadas em vários domínios, desde o uso particular até à utilização em organizações

privadas e na administração pública. As autoridades de aplicação da lei esperam retirar vantagens da utilização da TRF. Esta promete soluções para desafios relativamente novos, como as investigações que envolvem uma grande quantidade de elementos de provas, mas também para problemas conhecidos, nomeadamente no que diz respeito à falta de pessoal para as tarefas de observação e de busca.

2. Grande parte do interesse crescente na TRF está relacionado com a sua eficiência e potencial de expansão. A estas juntam-se as desvantagens inerentes à tecnologia e à sua aplicação – inclusive em grande escala. Embora esta tecnologia permita analisar milhares de conjuntos de dados pessoais premindo apenas um botão, os efeitos ligeiros da discriminação algorítmica ou da identificação incorreta podem afetar gravemente grandes números de indivíduos no seu comportamento e na sua vida quotidiana. A grande dimensão do tratamento de dados pessoais e, em especial, de dados biométricos, é outro elemento-chave da TRF, uma vez que o tratamento de dados pessoais constitui uma ingerência no direito fundamental à proteção dos dados pessoais consagrado no artigo 8.º da Carta dos Direitos Fundamentais da União Europeia (a seguir designada por «Carta»).

3. A aplicação da TRF pelas autoridades de aplicação da lei terá – e, em certa medida, já tem – repercussões significativas nos indivíduos e em certos grupos de pessoas, incluindo as minorias. Estas repercussões terão também efeitos consideráveis na forma como vivemos em conjunto e na nossa estabilidade política social e democrática, valorizando a elevada importância do pluralismo e da oposição política. O direito à proteção dos dados pessoais é muitas vezes uma condição prévia indispensável para garantir outros direitos fundamentais. A aplicação da TRF é bastante suscetível de interferir com direitos fundamentais para além do direito à proteção dos dados pessoais.

4. Por conseguinte, o CEPD considera importante contribuir para a integração contínua da TRF no domínio da aplicação da lei abrangido pela Diretiva Proteção de Dados na Aplicação da Lei[1], respetivamente as legislações nacionais que a transpõem, e disponibilizar as presentes orientações. As orientações têm por objetivo disponibilizar informações pertinentes aos legisladores a nível nacional e da UE, bem como às autoridades de aplicação da lei e aos seus agentes sempre que apliquem e utilizem sistemas de TRF. O âmbito de aplicação das orientações limita-se à TRF. No entanto, outras formas de tratamento de dados pessoais com base em dados biométricos utilizadas pelas autoridades de aplicação da lei, sobretudo se utilizadas à distância, podem implicar riscos semelhantes ou adicionais para os indivíduos, para certos grupos e para a sociedade. Dependendo das respetivas circunstâncias, alguns aspetos das presentes orientações podem também servir como uma fonte útil nestes casos. Por último, as partes interessadas em geral ou os titulares dos dados podem também encontrar aqui informações importantes, nomeadamente no que diz respeito aos direitos dos titulares dos dados.

5. As orientações são constituídas pelo documento principal e por três anexos. O documento principal apresenta a tecnologia e o quadro jurídico aplicável. No anexo I, é apresentado um modelo que visa ajudar a identificar alguns dos principais aspetos necessários para classificar a gravidade da ingerência nos direitos fundamentais num determinado domínio de aplicação. As autoridades de aplicação da lei que pretendam adquirir e aplicar um sistema de TRF podem encontrar orientações práticas no anexo II. Dependendo do âmbito de aplicação da TRF, podem ser relevantes diferentes considerações. O anexo III contém um conjunto de cenários hipotéticos e considerações relevantes.

[1]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.

2 TECNOLOGIA

2.1 Uma tecnologia biométrica, duas funções distintas

6. O reconhecimento facial é uma tecnologia probabilística que pode reconhecer automaticamente indivíduos com base no seu rosto, a fim de os autenticar ou identificar.

7. A TRF insere-se na categoria mais vasta da tecnologia biométrica. Os dados biométricos englobam todos os processos automatizados utilizados para reconhecer uma pessoa através da quantificação de características físicas, fisiológicas ou comportamentais (impressões digitais, estrutura da íris, voz, marcha, padrões dos vasos sanguíneos, etc.). Estas características são definidas como «dados biométricos», porque permitem ou confirmam a identificação única dessa pessoa.

8. É o caso do rosto das pessoas ou, mais especificamente, do respetivo processamento técnico utilizando dispositivos de reconhecimento facial: ao recolher a imagem de um rosto (uma fotografia ou vídeo) – a chamada «amostra biométrica» –, é possível extrair uma representação digital de características distintas desse rosto (o chamado «modelo»).

9. Um modelo biométrico é uma representação digital das características únicas que foram extraídas de uma amostra biométrica e que podem ser armazenadas numa base de dados biométrica[2]. Este modelo deverá ser único e específico para cada pessoa e é, em princípio, constante ao longo do tempo[3]. Na fase de reconhecimento, o dispositivo compara este modelo com outros modelos previamente produzidos ou calculados diretamente a partir de amostras biométricas, tais como rostos encontrados numa imagem, fotografia ou vídeo. O «reconhecimento facial» é, portanto, um processo em duas etapas: a recolha da imagem facial e a sua transformação num modelo, seguida do reconhecimento desse rosto através da comparação do modelo correspondente com um ou mais outros modelos.

10. Tal como qualquer processo biométrico, o reconhecimento facial pode desempenhar duas funções distintas:

- a **autenticação** da pessoa, com o objetivo de verificar se a pessoa é quem afirma ser. Neste caso, o sistema comparará uma amostra ou um modelo biométrico previamente gravado (por exemplo, armazenado num cartão inteligente ou num passaporte eletrónico) com um único rosto, por exemplo o de uma pessoa que se apresente num ponto de controlo, para verificar se se trata da mesma pessoa. Esta funcionalidade baseia-se, portanto, na comparação de dois modelos. É também chamada «**verificação** de um para um».

- a **identificação** de uma pessoa, com o objetivo de encontrar uma pessoa num grupo de indivíduos, dentro de uma área específica, numa imagem ou numa base de dados. Neste caso, o sistema tem de processar cada rosto captado para gerar um modelo biométrico e, em seguida, verificar se este corresponde a uma pessoa conhecida pelo sistema. Esta funcionalidade baseia-se, portanto, na comparação de um modelo com uma base de dados de modelos ou amostras (base de referência). Este processo é também designado por «identificação de um para muitos». Por exemplo, pode associar um registo de nome pessoal (apelido, nome próprio) a um rosto, se a comparação for feita com uma base de dados de fotografias associadas a apelidos e nomes próprios. Pode

[2] *Guidelines on facial recognition* [Diretrizes sobre o reconhecimento facial], Comité Consultivo da Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, Conselho da Europa, junho de 2021.

[3] Pode depender do tipo de biometria e da idade do titular dos dados.

também envolver o seguimento de uma pessoa numa multidão, sem estabelecer necessariamente a ligação à identidade civil da pessoa.

11. Em ambos os casos, as técnicas de reconhecimento facial utilizadas baseiam-se numa correspondência estimada entre modelos: o que está a ser comparado e a(s) base(s) de referência. Deste ponto de vista, são probabilísticas: a comparação deduz uma maior ou menor probabilidade de a pessoa em questão ser efetivamente a pessoa a autenticar ou a identificar. Se esta probabilidade exceder um determinado limiar no sistema, definido pelo utilizador ou pelo programador do sistema, este assumirá que existe uma correspondência.

12. Embora sejam distintas, ambas as funções – autenticação e identificação – dizem respeito ao tratamento de dados biométricos relacionados com uma pessoa singular identificada ou identificável, pelo que constituem tratamento de dados pessoais e, mais especificamente, tratamento de categorias especiais de dados pessoais.

13. O reconhecimento facial faz parte de um espetro mais alargado de técnicas de processamento de imagens de vídeo. Algumas câmaras de vídeo podem filmar pessoas dentro de uma área definida, nomeadamente os seus rostos, mas não podem ser utilizadas para o reconhecimento automático desses indivíduos. O mesmo se aplica à fotografia simples: uma câmara não é um sistema de reconhecimento facial porque as fotografias de pessoas têm de ser processadas de uma forma específica para permitirem a extração de dados biométricos.

14. A mera deteção de rostos pelas chamadas câmaras «inteligentes» também não constitui necessariamente um sistema de reconhecimento facial. Embora também levantem questões importantes em termos de ética e de eficácia, as técnicas digitais de deteção de comportamentos anormais ou de acontecimentos violentos, ou de reconhecimento de emoções faciais ou até mesmo de silhuetas, não podem ser consideradas como sistemas biométricos de tratamento de categorias especiais de dados pessoais, desde que não tenham por objetivo a identificação de pessoas de forma exclusiva e que o tratamento de dados pessoais em causa não inclua outras categorias especiais de dados pessoais. Estes exemplos não estão totalmente dissociados do reconhecimento facial e continuam sujeitos às regras de proteção de dados pessoais[4]. Além disso, este tipo de sistema de deteção pode ser utilizado em conjunto com outros sistemas destinados a identificar pessoas, sendo, nesse caso, considerado como uma tecnologia de reconhecimento facial.

15. Ao contrário dos sistemas de captura e processamento de vídeo, por exemplo, que requerem a instalação de dispositivos físicos, o reconhecimento facial é uma funcionalidade de *software* que pode ser implementada em sistemas existentes (câmaras, bases de dados de imagens, etc.). Esta funcionalidade pode, por conseguinte, ser ligada ou ter interface com uma multiplicidade de sistemas e ser combinada com outras funcionalidades. Esta integração numa infraestrutura já existente exige uma atenção especial, uma vez que acarreta riscos inerentes ao facto de a tecnologia de reconhecimento facial poder ser fluida e fácil de ocultar[5].

2.2 Uma vasta variedade de finalidades e aplicações

16. Para além do âmbito de aplicação das presentes orientações e fora do âmbito de aplicação da Diretiva Proteção de Dados na Aplicação da Lei, o reconhecimento facial pode ser utilizado para uma vasta variedade de objetivos, tanto de natureza comercial como para dar resposta a preocupações de

[4] O artigo 10.º da Diretiva Proteção de Dados na Aplicação da Lei (ou o artigo 9.º do RGPD) é, no entanto, aplicável a sistemas utilizados para agrupar indivíduos com base nos seus dados biométricos de acordo com a sua etnia, orientação política ou sexual ou outras categorias especiais de dados pessoais.

[5] Por exemplo, nas câmaras corporais, que são cada vez mais utilizadas por certos profissionais.

segurança pública ou de aplicação da lei. Pode ser aplicado em muitos contextos diferentes: na relação pessoal entre um utilizador e um serviço (acesso a uma aplicação), para acesso a um local específico (filtragem física) ou sem qualquer limitação específica no espaço público (reconhecimento facial em tempo real). Pode ser aplicado a qualquer tipo de titular de dados: um cliente de um serviço, um trabalhador, um simples espetador, uma pessoa procurada ou uma pessoa envolvida num processo judicial ou administrativo, etc. Algumas utilizações já são comuns e generalizadas; outras encontram-se, neste momento, em fase experimental ou especulativa. Embora as presentes orientações não abordem todas essas utilizações e aplicações, o CEPD recorda que só podem ser implementadas se estiverem em conformidade com o quadro jurídico aplicável, designadamente com o Regulamento Geral sobre a Proteção de Dados (RGPD) e com as leis nacionais aplicáveis[6]. Mesmo no contexto da Diretiva Proteção de Dados na Aplicação da Lei, além das funções de autenticação ou identificação, os dados tratados com recurso a tecnologias de reconhecimento facial também podem ser objeto de tratamento ulterior para outros fins, nomeadamente de classificação.

17. Mais concretamente, poderá ponderar-se uma escala de utilizações potenciais em função do grau de controlo que as pessoas têm sobre os seus dados pessoais, dos meios efetivos de que dispõem para exercer esse controlo e do seu direito de iniciativa para acionar e utilizar esta tecnologia, bem como das consequências para elas (em caso de reconhecimento ou não reconhecimento) e da escala do tratamento efetuado. O reconhecimento facial com base num modelo armazenado num dispositivo pessoal (cartão inteligente, telemóvel inteligente, etc.) pertencente a essa pessoa, utilizado para fins de autenticação e de uso estritamente pessoal através de uma interface dedicada, não apresenta os mesmos riscos que, por exemplo, a utilização para fins de identificação num ambiente não controlado, sem a participação ativa dos titulares dos dados e em que o modelo de cada rosto que entra na área de monitorização é comparado com modelos provenientes de uma secção transversal ampla da população armazenada numa base de dados. Entre estes dois extremos reside um espetro muito variado de utilizações e questões associadas relacionadas com a proteção de dados pessoais.

18. Para melhor ilustrar o contexto em que as tecnologias de reconhecimento facial estão atualmente a ser debatidas ou aplicadas, quer para autenticação, quer para identificação, o CEPD considera pertinente mencionar uma série de exemplos. Os exemplos que se seguem são meramente descritivos e não devem ser considerados como qualquer tipo de avaliação preliminar da sua conformidade com o acervo da UE no domínio da proteção de dados.

Exemplos de autenticação por reconhecimento facial

19. A autenticação pode ser concebida de modo que os utilizadores tenham total controlo sobre ela, por exemplo para permitir o acesso a serviços ou aplicações exclusivamente no contexto doméstico. Como tal, é amplamente utilizada pelos proprietários de telemóveis inteligentes para desbloquear o dispositivo, em vez da autenticação por palavra-passe.

20. A autenticação com base no reconhecimento facial também pode ser utilizada para verificar a identidade de uma pessoa que pretenda obter serviços públicos ou privados prestados por terceiros. Estes processos oferecem, assim, uma forma de criar uma identidade digital utilizando uma aplicação móvel (telemóvel inteligente, táblete, etc.) que pode depois ser utilizada para aceder a serviços administrativos em linha.

21. Além disso, a autenticação por reconhecimento facial pode ter como objetivo controlar o acesso físico a um ou mais locais predefinidos, tais como entradas em edifícios ou pontos de passagem específicos.

[6] Para mais orientações, ver também as Diretrizes 3/2019 sobre tratamento de dados pessoais através de dispositivos de vídeo, do CEPD, adotadas em 29 de janeiro de 2020.

Esta funcionalidade é, por exemplo, utilizada em certos tratamentos para efeitos de passagem de fronteiras, em que o rosto da pessoa no dispositivo do ponto de controlo é comparado com o que está armazenado no seu documento de identidade (passaporte ou autorização de residência segura).

Exemplos de identificação por reconhecimento facial

22. A identificação pode ser aplicada de muitas formas, ainda mais diversas. Estas incluem, entre outras, as utilizações enumeradas abaixo, atualmente em fase de observação, experimentação ou planeamento na UE:

- pesquisa, numa base de dados de fotografias, da identidade de uma pessoa não identificada (vítima, suspeita, etc.),
- monitorização dos movimentos de uma pessoa no espaço público. O rosto da pessoa é comparado com os modelos biométricos das pessoas que viajam ou viajaram na área monitorizada, por exemplo quando um volume de bagagem é deixado para trás ou após a ocorrência de um crime,
- reconstrução do percurso de uma pessoa e das suas interações subsequentes com outras pessoas, através de uma comparação diferida dos mesmos elementos, por exemplo numa tentativa de identificar os seus contactos,
- identificação biométrica à distância de pessoas procuradas em espaços públicos. Todos os rostos captados em tempo real por câmaras de videovigilância são comparados, em tempo real, com uma base de dados mantida pelas forças de segurança,
- reconhecimento automático de pessoas numa imagem para identificar, por exemplo, as suas relações numa rede social que o utilize. A imagem é comparada com os modelos de todas as pessoas na rede que tenham consentido esta funcionalidade, a fim de sugerir a identificação nominativa destas relações,
- acesso a serviços, existindo caixas automáticas que reconhecem os seus clientes comparando um rosto captado por uma câmara com a base de dados de imagens faciais detida pelo banco,
- rastreamento do percurso de um passageiro numa determinada fase da viagem. O modelo, calculado em tempo real, de qualquer pessoa que passe por portas localizadas em determinadas fases da viagem (pontos de entrega de bagagem, portas de embarque, etc.) é comparado com os modelos de pessoas previamente registadas no sistema.

23. Para além da utilização da TRF no domínio da aplicação da lei, o vasto leque de aplicações observadas exige certamente um debate e uma abordagem política abrangentes, a fim de assegurar a coerência e a conformidade com o acervo da UE no domínio da proteção de dados.

2.3 Fiabilidade, exatidão e riscos para os titulares dos dados

24. Como qualquer tecnologia, também a aplicação do reconhecimento facial pode estar sujeita a desafios, nomeadamente no que diz respeito à sua fiabilidade e eficiência em termos de autenticação ou identificação, bem como à questão geral da qualidade e da exatidão dos «dados-fonte» e do resultado do processamento da tecnologia de reconhecimento facial.

25. Estes desafios tecnológicos implicam riscos específicos para os titulares dos dados em causa, que são ainda mais significativos ou graves no domínio da aplicação da lei se tivermos em conta os possíveis efeitos, de natureza jurídica ou outra, para os titulares dos dados que os afetem de forma significativa. Neste contexto, afigura-se igualmente útil sublinhar que a utilização *a posteriori* da TRF não é, por si

só, mais segura, uma vez que permite rastrear os indivíduos ao longo do tempo e em vários locais. A utilização *a posteriori* também apresenta riscos específicos que têm de ser avaliados caso a caso[7].

26. Tal como salientado pela Agência dos Direitos Fundamentais da UE no seu relatório de 2019, «a determinação do nível necessário de exatidão do *software* de reconhecimento facial é um desafio: existem muitas formas diferentes de avaliar e aferir a exatidão, dependendo nomeadamente da tarefa, do objetivo e do contexto da sua utilização. Ao aplicar a tecnologia em locais visitados por milhões de pessoas – como estações ferroviárias ou aeroportos – uma percentagem relativamente pequena de erros (por exemplo, 0,01 %)[8] implica a sinalização incorreta de centenas de pessoas. Além disso, certas categorias de pessoas podem ter mais probabilidades de serem objeto de correspondências erradas do que outras, como descrito na secção 3. Existem diferentes formas de calcular e interpretar as taxas de erro, pelo que é necessária prudência. Além do mais, no que diz respeito à exatidão e aos erros, as questões relacionadas com a facilidade com que um sistema pode ser enganado, por exemplo, por imagens faciais falsas (o chamado *spoofing*, ou mistificação da identidade) são importantes, especialmente para efeitos de aplicação da lei»[9].

27. Neste contexto, o CEPD considera importante recordar que a TRF, quer seja utilizada para efeitos de autenticação ou de identificação, não produz um resultado definitivo, mas baseia-se na probabilidade de que dois rostos, ou imagens de rostos, correspondam à mesma pessoa[10]. Este resultado é ainda menos fiável quando a qualidade da amostra biométrica introduzida no sistema de reconhecimento facial é baixa. Imagens de entrada desfocadas, a baixa resolução da câmara, movimento e iluminação fraca podem contribuir para a baixa qualidade dos resultados. Outros aspetos com impacto significativo nos resultados são a prevalência e a mistificação da identidade, por exemplo quando os criminosos tentam evitar passar por câmaras ou enganar a TRF. Numerosos estudos salientaram igualmente que estes resultados estatísticos do tratamento algorítmico podem também estar sujeitos a enviesamentos, nomeadamente resultantes da qualidade dos dados-fonte e das bases de dados de treino, ou de outros fatores, como a escolha da localização da implantação. Além disso, há que salientar também o impacto da tecnologia de reconhecimento facial noutros direitos fundamentais, como o respeito pela vida privada e familiar, a liberdade de expressão e de informação, a liberdade de reunião e de associação, etc.

28. É, pois, essencial que a fiabilidade e a exatidão da tecnologia de reconhecimento facial sejam tidas em conta como critérios para avaliar a conformidade com os princípios fundamentais da proteção de dados, nos termos do artigo 4.º da Diretiva Proteção de Dados na Aplicação da Lei, nomeadamente no que se refere à equidade e à exatidão.

29. Embora salientando que algoritmos de alta qualidade requerem dados de alta qualidade, o CEPD sublinha também a necessidade de os responsáveis pelo tratamento de dados, no âmbito da sua obrigação de responsabilidade, procederem a uma avaliação regular e sistemática do tratamento algorítmico, a fim de garantir, concretamente, a exatidão, a equidade e a fiabilidade do resultado desse tratamento de dados pessoais. Os dados pessoais utilizados para efeitos de avaliação, treino e ulterior

[7] Ver os exemplos apresentados no anexo III.

[8] Esta taxa de exatidão resulta do relatório citado e reflete uma taxa muito superior ao desempenho atual dos algoritmos em aplicações de TRF.

[9] *Facial recognition technology: fundamental rights considerations in the context of law enforcement* [Tecnologia de reconhecimento facial: considerações relativas aos direitos fundamentais no contexto da aplicação da lei], Agência dos Direitos Fundamentais da UE, 21 de novembro de 2019.

[10] Esta probabilidade é referida como «pontuação de confiança».

desenvolvimento dos sistemas de TRF só podem ser tratados com fundamento numa base jurídica suficiente e em conformidade com os princípios comuns em matéria de proteção de dados.

3 QUADRO JURÍDICO APLICÁVEL

30. A utilização de tecnologias de reconhecimento facial está intrinsecamente ligada ao tratamento de dados pessoais, incluindo de categorias especiais de dados. Além disso, tem um impacto direto ou indireto numa série de direitos fundamentais, consagrados na Carta dos Direitos Fundamentais da UE. Este aspeto é de particular importância no domínio da aplicação da lei e da justiça penal. Qualquer utilização de tecnologias de reconhecimento facial deve, pois, ser efetuada em estrita conformidade com o quadro jurídico aplicável.

31. As informações que se seguem destinam-se a ser utilizadas para consideração aquando da avaliação de futuras medidas legislativas e administrativas, bem como de forma individualizada na aplicação da legislação em vigor em casos que envolvam TRF. A relevância dos respetivos requisitos varia em função das circunstâncias específicas em apreço. Dada a impossibilidade de prever todas as circunstâncias futuras, estas informações servem apenas de apoio e não devem ser interpretadas como uma enumeração exaustiva.

3.1 Quadro jurídico geral – A Carta dos Direitos Fundamentais da UE e a Convenção Europeia dos Direitos Humanos (CEDH)

3.1.1 Aplicabilidade da Carta

32. A Carta dos Direitos Fundamentais da UE (a seguir designada por «Carta») tem por destinatários as instituições, os órgãos e os organismos da União, bem como os Estados-Membros, quando apliquem o direito da União.

33. A regulamentação do tratamento de dados biométricos para fins de aplicação da lei nos termos do artigo 1.º, n.º 1, da Diretiva Proteção de Dados na Aplicação da Lei levanta inevitavelmente a questão do respeito dos direitos fundamentais, em especial do respeito pela vida privada e pelas comunicações privadas nos termos do artigo 7.º da Carta e do direito à proteção dos dados pessoais nos termos do artigo 8.º da Carta.

34. A recolha e a análise de imagens de vídeo de pessoas singulares, incluindo os seus rostos, implica o tratamento de dados pessoais. O tratamento técnico da imagem abrange também os dados biométricos. O tratamento técnico dos dados relacionados com o rosto de uma pessoa singular em relação ao tempo e ao local permite tirar conclusões sobre a vida privada da pessoa em causa. Essas conclusões podem dizer respeito à origem racial ou étnica, à saúde, à religião, aos hábitos diários, aos locais de residência permanentes ou temporários, às deslocações diárias ou outras, às atividades realizadas e às relações sociais dessas pessoas, bem como aos ambientes sociais que elas frequentam. O grande leque de informações que podem ser reveladas pela aplicação de TRF mostra claramente o possível impacto no direito à proteção dos dados pessoais consagrado no artigo 8.º da Carta, mas também no direito à privacidade consagrado no artigo 7.º da Carta.

35. Nestas circunstâncias, também não é inconcebível que a recolha, a análise e o posterior tratamento dos dados biométricos (faciais) em questão possam repercutir-se na forma como as pessoas se sentem livres para agir, mesmo que os atos em questão se inscrevam plenamente nos limites de uma sociedade livre e aberta. Pode também ter implicações graves no exercício dos seus direitos

fundamentais, como o seu direito à liberdade de pensamento, de consciência e de religião, à liberdade de expressão e à liberdade de reunião pacífica e de associação nos termos dos artigos 1.º, 10.º, 11.º e 12.º da Carta. Esse tratamento envolve também outros riscos, tais como o risco de utilização abusiva das informações pessoais recolhidas pelas autoridades competentes em resultado do acesso e da utilização ilícitos dos dados pessoais, o risco de violações de segurança, etc. Os riscos dependem frequentemente do tratamento e das suas circunstâncias, tais como o risco de acesso e utilização ilícitos por agentes da polícia ou por outras partes não autorizadas. No entanto, alguns riscos são simplesmente intrínsecos à natureza única dos dados biométricos. Ao contrário de uma morada ou de um número de telefone, é impossível ao titular dos dados alterar as suas características únicas, como o seu rosto ou a sua íris. Em caso de acesso não autorizado ou de publicação acidental de dados biométricos, os dados passam a estar comprometidos para utilização como palavras-passe ou chaves criptográficas ou podem ser utilizados para outras atividades de vigilância não autorizadas lesivas do titular dos dados.

3.1.2 Ingerência nos direitos consagrados na Carta

36. O tratamento de dados biométricos, seja em que circunstância for, constitui, por si só, uma ingerência grave. Esta não depende do resultado, por exemplo uma correspondência positiva. O tratamento constitui uma ingerência mesmo que o modelo biométrico seja imediatamente apagado depois de a verificação numa base de dados da polícia resultar numa resposta negativa.

37. A ingerência nos direitos fundamentais dos titulares dos dados pode resultar de um ato jurídico que tenha por objetivo ou por efeito restringir o respetivo direito fundamental[11]. Por outro lado, pode resultar de um ato de uma autoridade pública com o mesmo objetivo ou efeito ou até de uma entidade privada encarregada por lei de exercer a autoridade e os poderes públicos.

38. Uma medida legislativa que serve de base jurídica para o tratamento de dados pessoais é constitutiva de uma ingerência direta nos direitos garantidos pelos artigos 7.º e 8.º da Carta[12].

39. A utilização de dados biométricos e, em especial, de TRF, em muitos casos, afeta também o direito à dignidade humana, garantido pelo artigo 1.º da Carta. A dignidade humana requer que os indivíduos não sejam tratados como meros objetos. A TRF calcula características existenciais e altamente pessoais, os traços faciais, num formato de leitura automática, com o objetivo de os utilizar como matrícula ou cartão de identificação humano, objetificando assim o rosto da pessoa.

40. Este tratamento pode também constituir uma ingerência noutros direitos fundamentais, tais como os direitos garantidos pelos artigos 10.º, 11.º e 12.º da Carta, na medida em que a videovigilância em causa realizada pelos serviços de aplicação da lei resulte, intencional ou inadvertidamente, em efeitos dissuasores.

41. Além disso, importa ter também cuidadosamente em conta os potenciais riscos gerados pela utilização de tecnologias de reconhecimento facial pelas autoridades de aplicação da lei no que diz respeito aos direitos a um tribunal imparcial e à presunção de inocência, consagrados nos artigos 47.º e 48.º da Carta. O resultado da aplicação da TRF, por exemplo uma correspondência, pode não só levar a que uma pessoa seja sujeita a policiamento mais intensivo, mas também constituir uma prova decisiva num processo judicial. As insuficiências da TRF, nomeadamente possíveis enviesamentos, discriminação ou erros de identificação («falsos positivos») podem, por conseguinte, ter graves consequências também

[11] Acórdão de 28 de outubro de 1992, Ter Voort, C-219/91, EU:C:1992:414, n.º 36; Acórdão de 28 de abril de 1998, Metronome Musik/Music Point Hokamp, C-200/96, EU:C:1998:172, n.º 28.
[12] Acórdão de 8 de abril de 2014, Digital Rights Ireland, C-594/12, EU:C:2014:238, n.º 36; Acórdão de 17 de outubro de 2013, Schwarz, C-291/12, EU:C:2013:670, n.º 23 e seguintes.

em processos penais. Além disso, na apreciação dos elementos de prova, o resultado da aplicação da TRF pode ser favorecido, mesmo perante provas contraditórias («enviesamento da automatização»).

3.1.3 Justificação da ingerência

42. Nos termos do artigo 52.º, n.º 1, da Carta, qualquer restrição ao exercício dos direitos e liberdades fundamentais deve ser prevista por lei e respeitar o conteúdo essencial desses direitos e liberdades. Na observância do princípio da proporcionalidade, essas restrições só podem ser introduzidas se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros.

3.1.3.1 Prevista por lei

43. O artigo 52.º, n.º 1, da Carta estabelece o requisito de uma base jurídica específica. Os termos dessa base jurídica devem ser suficientemente claros para dar aos cidadãos uma indicação adequada das condições e das circunstâncias em que as autoridades têm poderes para recorrer a medidas de recolha de dados e de vigilância secreta[13]. A base jurídica deve indicar, com uma nitidez razoável, a amplitude e as modalidades do exercício do poder discricionário conferido às autoridades públicas, de modo a garantir aos indivíduos o grau mínimo de proteção a que têm direito ao abrigo do Estado de direito numa sociedade democrática[14]. Além disso, a licitude requer salvaguardas adequadas para garantir, concretamente, que o direito de um indivíduo ao abrigo do artigo 8.º da Carta seja respeitado. Estes princípios aplicam-se igualmente ao tratamento de dados pessoais para efeitos de avaliação, treino e desenvolvimento dos sistemas de TRF.

44. Constituindo os dados biométricos, quando tratados para efeitos de identificação inequívoca de uma pessoa singular, categorias especiais de dados na aceção do artigo 10.º da Diretiva Proteção de Dados na Aplicação da Lei, as diferentes aplicações da TRF exigiriam, na maioria dos casos, uma lei específica que descreva com precisão a aplicação e as condições da sua utilização. Esta descrição engloba, nomeadamente, os tipos de crimes e, se for caso disso, o limiar adequado de gravidade dos mesmos, a fim de, entre outras coisas, excluir efetivamente a pequena criminalidade[15].

3.1.3.2 O conteúdo essencial do direito fundamental à privacidade e à proteção dos dados pessoais consagrado nos artigos 7.º e 8.º da Carta

45. As limitações dos direitos fundamentais inerentes a cada situação têm, não obstante, de garantir o conteúdo essencial do direito concreto a respeitar. O conteúdo essencial refere-se à própria essência do direito fundamental em causa[16]. A dignidade humana também tem de ser respeitada, mesmo quando um direito é restringido[17].

46. Os indícios de uma eventual infração da essência inviolável são os seguintes:

- Uma disposição que imponha limitações independentemente do comportamento individual de uma pessoa ou de circunstâncias excecionais[18].
- Impossibilidade ou dificuldade no recurso aos tribunais[19].

[13] TEDH, Shimovolos c. Rússia, § 68; Vukota-Bojić c. Suíça.
[14] TEDH, Piechowicz c. Polónia, § 212.
[15] Ver, por exemplo, o Acórdão de 21 de junho de 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, n.º 151, e o Acórdão de 2 de outubro de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, n.º 56.
[16] Acórdão de 22 de dezembro de 2010, DEB, C-279/09, EU:C:2010:811, n.º 60.
[17] Anotações relativas à Carta dos Direitos Fundamentais, Título I, Anotação *ad* artigo 1.º (JO C 303 de 14.12.2007, p. 17).
[18] Acórdão de 15 de fevereiro de 2016, N., C-601/15, EU:C:2016:84, n.º 52.
[19] Acórdão de 5 de outubro de 2010, McB., C-400/10, EU:C:2010:582, n.º 55.

- Antes de uma limitação grave, as circunstâncias do indivíduo em causa não são tidas em conta[20].
- Tendo em vista os direitos previstos nos artigos 7.º e 8.º da Carta: para além de uma ampla recolha de metadados de comunicação, a aquisição do conhecimento do conteúdo da comunicação eletrónica poderia violar o conteúdo essencial desses direitos[21].
- Tendo em vista os direitos previstos nos artigos 7.º, 8.º e 11.º da Carta: legislação que exige que os prestadores de acesso a serviços de comunicação pública em linha e os prestadores de serviços de alojamento virtual conservem, de forma geral e indiscriminada, entre outros, dados pessoais relacionados com esses serviços[22].
- No que se refere aos direitos previstos no artigo 8º da Carta: a falta de princípios básicos de proteção e segurança dos dados poderia também infringir o conteúdo essencial do direito[23].

3.1.3.3 Objetivo legítimo

47. Tal como já se explicou no ponto 3.1.3., as restrições aos direitos fundamentais têm de corresponder efetivamente a objetivos de interesse geral reconhecidos pela União Europeia ou satisfazer a necessidade de proteger os direitos e liberdades de terceiros.

48. A União reconhece tanto os objetivos mencionados no artigo 3.º do Tratado da União Europeia como outros interesses protegidos por disposições específicas dos Tratados[24], isto é, nomeadamente, um espaço de liberdade, segurança e justiça e a prevenção e o combate à criminalidade. Nas suas relações com o resto do mundo, a União deve contribuir para a paz e para a segurança, bem como para a proteção dos direitos humanos.

49. A necessidade de proteger os direitos e as liberdades de terceiros refere-se aos direitos das pessoas protegidas pelo direito da União Europeia ou dos seus Estados-Membros. A avaliação deve ser efetuada com o objetivo de conciliar as exigências da proteção dos respetivos direitos e de encontrar um justo equilíbrio entre eles[25].

3.1.3.4 Teste da necessidade e da proporcionalidade

50. Quando estão em causa ingerências nos direitos fundamentais, o poder discricionário do legislador nacional e da União pode revelar-se limitado. Tal depende de uma série de fatores, incluindo a zona em causa, a natureza do direito em questão garantido pela Carta, a natureza e a gravidade da ingerência e o objetivo da ingerência[26]. As medidas legislativas têm de ser adequadas para alcançar os objetivos legítimos da legislação em causa. Além disso, a medida não deve exceder os limites do que é adequado e necessário à realização desses objetivos[27]. Um objetivo de interesse geral, por muito fundamental que seja, não pode, por si só, justificar uma restrição a um direito fundamental[28].

---

[20] Acórdão de 23 de março de 2006, Comissão/Bélgica, C-408/03, EU:C:2006:192, n.º 68.

[21] Acórdão de 21 de dezembro de 2016, Tele2 Sverige, C-203/15, EU:C:2016:970, n.º 101, com referência ao Acórdão de 8 de abril de 2014, Digital Rights Ireland, C-293/12 e C-594/12, n.º 39.

[22] Acórdão de 6 de outubro de 2020, La Quadrature du Net e o., C-512/18, EU:C:2020:791, n.º 209 e seguintes.

[23] Acórdão de 8 de abril de 2014, Digital Rights Ireland, C-594/12, EU:C:2014:238, n.º 40.

[24] Anotações relativas à Carta dos Direitos Fundamentais, Título I, Anotação *ad* artigo 52.º (JO C 303 de 14.12.2007, p. 17).

[25] Jarass GrCh, 3. Aufl. 2016, EU-Grundrechte-Charta Art. 52 Rn. 31-32.

[26] Acórdão de 8 de abril de 2014, Digital Rights Ireland, C-594/12, EU:C:2014:238, n.º 47, com as seguintes fontes: v., por analogia, no que respeita ao artigo 8.º da CEDH, acórdão TEDH, S. e Marper c. Reino Unido [GC], n.os 30562/04 e 30566/04, § 102, CEDH 2008-V.

[27] Acórdão de 8 de abril de 2014, Digital Rights Ireland, C-594/12, EU:C:2014:238, n.º 46, com as seguintes fontes: acórdãos Afton Chemical, C-343/09, EU:C:2010:419, n.º 45; Volker und Markus Schecke e Eifert, EU:C:2010:662, n.º 74; Nelson e o., C-581/10 e C-629/10, EU:C:2012:657, n.º 71; Sky Österreich, C-283/11, EU:C:2013:28, n.º 50; e Schaible, C-101/12, EU:C:2013:661, n.º 29.

[28] Acórdão de 8 de abril de 2014, Digital Rights Ireland, C-594/12, EU:C:2014:238, n.º 51.

51. Segundo a jurisprudência constante do TJUE, as derrogações e limitações à proteção dos dados pessoais devem ocorrer na estrita medida do necessário[29]. Tal implica também a inexistência de meios menos intrusivos para alcançar a finalidade em questão. Importa identificar e avaliar cuidadosamente alternativas possíveis, como – dependendo da finalidade em causa – reforço dos recursos humanos, policiamento mais frequente ou mais iluminação pública. As medidas legislativas devem diferenciar e visar as pessoas abrangidas pelo seu âmbito de aplicação em função do respetivo objetivo, por exemplo de combater a criminalidade grave. Se a medida abranger todas as pessoas de um modo geral, sem essa diferenciação, limitação ou exceção, a ingerência é intensificada[30]. A ingerência é igualmente intensificada se o tratamento de dados abranger uma parte significativa da população[31].

52. A proteção dos dados pessoais que resulta da obrigação expressa prevista no artigo 8.º, n.º 1, da Carta assume particular importância para o direito ao respeito da vida privada consagrado no artigo 7.º desta[32]. A legislação deve estabelecer regras claras e precisas que regulem o âmbito e a aplicação da medida em causa e imponham exigências, de modo que as pessoas cujos dados foram tratados disponham de garantias suficientes que permitam proteger eficazmente os seus dados pessoais contra os riscos de abuso e contra qualquer acesso ou utilização ilícita dos mesmos[33]. A necessidade de dispor de tais garantias é ainda mais importante quando os dados pessoais são sujeitos a tratamento automático e existe um risco significativo de acesso ilícito aos mesmos[34]. Além disso, a autorização interna ou externa, por exemplo judicial, da utilização de TRF também pode contribuir como exigência e pode revelar-se necessária em certos casos de ingerência grave[35].

53. As regras estabelecidas devem ser adaptadas à situação específica, por exemplo, a quantidade de dados tratados, o caráter dos dados[36]e o risco de acesso ilícito aos mesmos. Tal requer regras que se destinariam, designadamente, a regular de maneira clara e estrita a proteção e a segurança dos dados em causa, a fim de garantir a sua plena integridade e confidencialidade[37].

54. No que diz respeito à relação entre o responsável pelo tratamento e o subcontratante, este último não deve poder ter em conta apenas considerações económicas na determinação do nível de segurança que aplica aos dados pessoais, já que, dessa forma, pode não conseguir garantir um nível de proteção suficientemente elevado[38].

55. Um ato legislativo tem de estabelecer condições substantivas e processuais e critérios objetivos que permitam delimitar o acesso das autoridades competentes aos dados e a sua utilização posterior. Para fins de prevenção, deteção ou ação penal, as infrações em causa teriam de ser consideradas

[29] Acórdão de 8 de abril de 2014, Digital Rights Ireland, C-594/12, EU:C:2014:238, n.º 52, com as seguintes fontes: acórdão IPI, C-473/12, EU:C:2013:715, n.º 39 e jurisprudência referida).
[30] Acórdão de 8 de abril de 2014, Digital Rights Ireland, C-594/12, EU:C:2014:238, n.º 57.
[31] Acórdão de 8 de abril de 2014, Digital Rights Ireland, C-594/12, EU:C:2014:238, n.º 56.
[32] Acórdão de 8 de abril de 2014, Digital Rights Ireland, C-594/12, EU:C:2014:238, n.º 53.
[33] Acórdão de 8 de abril de 2014, Digital Rights Ireland, C-594/12, EU:C:2014:238, n.º 54, com as seguintes fontes: v., por analogia, no que respeita ao artigo 8.º da CEDH, acórdãos TEDH, Liberty e outros c. Reino Unido de 1 de julho de 2008, n.º 58243/00, §§ 62 e 63; Rotaru c. Roménia, já referido, §§ 57 a 59; e S e Marper c. Reino Unido, já referido, § 99.
[34] Acórdão de 8 de abril de 2014, Digital Rights Ireland, C-594/12, EU:C:2014:238, n.º 55, com as seguintes fontes: v., por analogia, no que respeita ao artigo 8.º da CEDH, acórdãos TEDH, S e Marper c. Reino Unido, já referido, § 103, e M. K. c. França de 18 de abril de 2013, n.º 19522/09, § 35.
[35]TEDH, Szabó e Vissy c. Hungria, §§ 73-77.
[36] Ver também os requisitos reforçados de medidas técnicas e organizativas para o tratamento de categorias especiais de dados, artigo 29.º, n.º 1, da Diretiva Proteção de Dados na Aplicação da Lei.
[37] Acórdão de 8 de abril de 2014, Digital Rights Ireland, C-594/12, EU:C:2014:238, n.º 66.
[38] Acórdão de 8 de abril de 2014, Digital Rights Ireland, C-594/12, EU:C:2014:238, n.º 67.

suficientemente graves para justificar a amplitude e a gravidade dessas ingerências nos direitos fundamentais consagrados, por exemplo, nos artigos 7.º e 8.º da Carta[39].

56. Os dados têm de ser tratados de forma a garantir a aplicabilidade e o efeito das regras de proteção de dados da UE, em especial das previstas no artigo 8.º da Carta, que estabelece que o respeito das exigências de proteção e de segurança está sujeito a fiscalização por parte de uma autoridade independente. O local geográfico onde o tratamento é efetuado pode, nessa situação, ser relevante[40].

57. No que diz respeito às diferentes etapas do tratamento de dados pessoais, importa distinguir entre as categorias de dados em função da sua eventual utilidade relativamente ao objetivo prosseguido ou em função das pessoas em causa[41]. A determinação das condições do tratamento, por exemplo a determinação do período de conservação, deve basear-se em critérios objetivos, a fim de garantir que a ingerência se limita ao estritamente necessário[42].

58. Em função da situação em apreço, a avaliação da necessidade e da proporcionalidade tem de identificar e ponderar todas as repercussões abrangidas pelo âmbito de aplicação dos direitos fundamentais, tais como a dignidade humana nos termos do artigo 1.º da Carta, a liberdade de pensamento, de consciência e de religião nos termos do artigo 10.º da Carta, a liberdade de expressão nos termos do artigo 11.º da Carta, bem como a liberdade de reunião e de associação nos termos do artigo 12.º da Carta.

59. Importa, além disso, considerar como uma questão de gravidade que, se os dados forem sistematicamente tratados sem o conhecimento dos respetivos titulares, é provável que se gere uma sensação geral de vigilância constante[43]. Esta sensação pode provocar efeitos dissuasores em relação à totalidade ou a parte dos direitos fundamentais em causa.

60. Para facilitar e operacionalizar a avaliação da necessidade e da proporcionalidade no que diz respeito a medidas legislativas relacionadas com o reconhecimento facial no domínio da aplicação da lei, os legisladores nacionais e da União poderiam tirar partido dos instrumentos práticos disponíveis especialmente concebidos para esta tarefa. Em especial, poderá ser utilizado o conjunto de ferramentas para a avaliação da necessidade e da proporcionalidade[44] disponibilizado pela Autoridade Europeia para a Proteção de Dados.

3.1.3.5 Artigo 52.º, n.º 3, e artigo 53.º da Carta (nível de proteção, nomeadamente em relação ao da CEDH)

61. Nos termos do artigo 52.º, n.º 3, e do artigo 53.º da Carta, o sentido e o âmbito dos direitos da Carta que correspondam aos direitos garantidos pela CEDH devem ser iguais aos conferidos pela CEDH. Embora, nomeadamente no que se refere ao artigo 7.º da Carta, possa existir um equivalente na CEDH, o mesmo não se verifica relativamente ao artigo 8.º da Carta[45]. O artigo 52.º, n.º 3, da Carta não obsta

[39] Acórdão de 8 de abril de 2014, Digital Rights Ireland, C-594/12, EU:C:2014:238, n.os 60 e 61.
[40] Acórdão de 8 de abril de 2014, Digital Rights Ireland, C-594/12, EU:C:2014:238, n.º 68.
[41] Acórdão de 8 de abril de 2014, Digital Rights Ireland, C-594/12, EU:C:2014:238, n.º 63.
[42] Acórdão de 8 de abril de 2014, Digital Rights Ireland, C-594/12, EU:C:2014:238, n.º 64.
[43] Acórdão de 8 de abril de 2014, Digital Rights Ireland, C-594/12, EU:C:2014:238, n.º 37.
[44] Autoridade Europeia para a Proteção de Dados: «Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit» [Avaliar a necessidades das medidas que limitam o direito fundamental à proteção dos dados pessoais: um conjunto de ferramentas] (11.4.2017); Autoridade Europeia para a Proteção de Dados: «EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data» [Orientações da AEPD sobre a avaliação da proporcionalidade de medidas que limitem os direitos fundamentais à privacidade e à proteção de dados pessoais] (19.12.2019).
[45] Acórdão de 21 de dezembro de 2016, Tele2 Sverige, C-203/15, EU:C:2016:970, n.º 129.

a que o direito da União conceda uma proteção mais alargada. Uma vez que a CEDH não constitui um instrumento jurídico formalmente integrado na ordem jurídica da UE, a interpretação da legislação da UE deve ser realizada à luz dos direitos fundamentais garantidos pela Carta[46].

62. Nos termos do artigo 8.º da CEDH, não pode haver ingerência da autoridade pública no exercício do direito ao respeito pela vida privada e familiar, senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros.

63. A CEDH estabelece igualmente normas no que diz respeito à forma como as limitações podem ser aplicadas. Um requisito básico, para além do Estado de direito, é a previsibilidade. Para cumprir o requisito da previsibilidade, os termos da lei devem ser suficientemente claros para proporcionar aos indivíduos uma indicação adequada das circunstâncias em que as autoridades têm o direito de recorrer a tais medidas[47]. Esta exigência é reconhecida pelo TJUE e pela legislação da UE em matéria de proteção de dados (ver secção 3.2.1.1).

64. Especificando ainda mais os direitos previstos no artigo 8.º da CEDH, as disposições da Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal[48]também têm de ser plenamente respeitadas. Ainda assim, deve considerar-se que estas disposições representam apenas uma norma mínima, tendo em conta a legislação prevalecente na União.

3.2 Quadro jurídico específico – a Diretiva Proteção de Dados na Aplicação da Lei

65. A Diretiva Proteção de Dados na Aplicação da Lei prevê um determinado quadro relativo à utilização de TRF. Em primeiro lugar, o artigo 3.º, ponto 13, da diretiva define o termo «dados biométricos»[49]. Para mais informações, ver secção 2.1 *supra*. Em segundo lugar, o artigo 8.º, n.º 2, esclarece que, para ser lícito, o tratamento tem de – para além de ser necessário para os fins indicados no artigo 1.º, n.º 1, da diretiva – ser regulado por legislação nacional que especifique pelo menos os objetivos do tratamento, os dados pessoais a tratar e as finalidades do tratamento. Outras disposições de especial relevância no que diz respeito aos dados biométricos são os artigos 10.º e 11.º da diretiva. O artigo 10.º deve ser lido em conjugação com o artigo 8.º da diretiva[50]. Os princípios relativos ao tratamento de dados pessoais estabelecidos no artigo 4.º da diretiva devem ser sempre respeitados e devem reger qualquer avaliação do eventual tratamento biométrico por TRF.

3.2.1 Tratamento de categorias especiais de dados para efeitos de aplicação da lei

66. Nos termos do artigo 10.º da Diretiva Proteção de Dados na Aplicação da Lei, o tratamento de categorias especiais de dados, como dados biométricos, só é autorizado se for estritamente necessário

[46] Acórdão de 16 de julho de 2020, Facebook Ireland e Schrems, C-311/18, EU:C:2020:559, n.º 99.
[47] Tribunal Europeu dos Direitos Humanos, acórdão Copland c. Reino Unido, 3.4.2007, petição n.º 62617/00, n.º 46.
[48] STE n.º 108.
[49] Artigo 3.º, ponto 13, da Diretiva Proteção de Dados na Aplicação da Lei: «"Dados biométricos", dados pessoais resultantes de um tratamento técnico específico, relativos às características físicas, fisiológicas ou comportamentais de uma pessoa singular, que permitem ou confirmam a sua identificação única, tais como imagens faciais ou dados dactiloscópicos».
[50]WP258, *Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)* [Parecer sobre algumas questões importantes da Diretiva relativa à proteção de dados na aplicação da lei (UE 2016/680)], p. 7.

e se estiver sujeito a garantias adequadas dos direitos e liberdades do titular dos dados. Além disso, só é autorizado se for autorizado pelo direito da União ou de um Estado-Membro, se se destinar a proteger os interesses vitais do titular dos dados ou de outra pessoa singular ou se estiver relacionado com dados manifestamente tornados públicos pelo titular dos dados. Esta cláusula geral sublinha o caráter sensível do tratamento de categorias especiais de dados.

3.2.1.1 Autorizado pelo direito da União ou de um Estado-Membro

67. No que diz respeito ao tipo de medida legislativa necessária, o considerando 33 da Diretiva Proteção de Dados na Aplicação da Lei prevê que «[s]empre que a presente diretiva se refira ao direito de um Estado-Membro, a um fundamento jurídico ou a uma medida legislativa, não se trata necessariamente de um ato legislativo adotado por um parlamento, sem prejuízo dos requisitos que decorram da ordem constitucional do Estado-Membro em causa»[51].

68. De acordo com o artigo 52.º, n.º 1, da Carta, qualquer restrição ao exercício dos direitos e liberdades reconhecidos pela Carta deve ser «prevista por lei». Esta locução reflete a expressão «prevista na lei» presente no artigo 8.º, n.º 2, da CEDH, o que significa, não só a conformidade com o direito aplicável, mas também a relação com a qualidade dessa legislação, sem prejuízo da natureza do ato em causa, devendo ser compatível com o Estado de direito.

69. O considerando 33 da Diretiva Proteção de Dados na Aplicação da Lei estabelece ainda que «[n]o entanto, esse direito de um Estado-Membro, esse fundamento jurídico ou essa medida legislativa deverão ser claros e precisos, e a sua aplicação deverá ser previsível para os particulares, como exigido pela jurisprudência do Tribunal de Justiça e pelo Tribunal Europeu dos Direitos do Homem. O direito dos Estados-Membros que rege o tratamento de dados pessoais no âmbito da presente diretiva deverá especificar, pelo menos, os objetivos, os dados pessoais a tratar, as finalidades do tratamento e os procedimentos destinados a preservar a integridade e a confidencialidade dos dados pessoais, bem como os procedimentos para a destruição dos mesmos».

70. Os termos da legislação nacional devem ser suficientemente claros para proporcionar aos titulares dos dados uma indicação adequada das circunstâncias e das condições em que os responsáveis pelo tratamento têm o direito de recorrer a essas medidas. Estas incluem eventuais condições prévias para o tratamento, nomeadamente tipos específicos de elementos de prova, bem como a necessidade de uma autorização judicial ou interna. A respetiva legislação pode ser tecnologicamente neutra, na medida em que os riscos e as características específicos do tratamento de dados pessoais pelos sistemas de TRF sejam suficientemente tidos em conta. Em conformidade com a Diretiva Proteção de Dados na Aplicação da Lei e com a jurisprudência do Tribunal de Justiça da União Europeia (TJUE) e do Tribunal Europeu dos Direitos Humanos (TEDH), é efetivamente essencial que as medidas legislativas, que visam proporcionar uma base jurídica para uma medida de reconhecimento facial, sejam previsíveis para os titulares dos dados.

71. Uma medida legislativa não pode ser invocada como uma lei que autoriza o tratamento de dados biométricos através de TRF para efeitos de aplicação da lei se se tratar de uma mera transposição da cláusula geral do artigo 10.º da diretiva.

72. Para além dos dados biométricos, o artigo 10.º da Diretiva Proteção de Dados na Aplicação da Lei regula o tratamento de outras categorias especiais de dados, nomeadamente dados relativos à orientação sexual, às opiniões políticas e às crenças religiosas, abrangendo assim um leque

[51] O tipo de medidas legislativas em causa tem de estar em conformidade com o direito da UE ou com a legislação nacional. Dependendo do grau de ingerência da restrição, poderá ser necessária a nível nacional uma medida legislativa específica, tendo em conta o nível de norma.

diversificado de formas de tratamento dos dados. Além disso, tal disposição careceria de requisitos específicos que indicassem as circunstâncias e as condições em que as autoridades de aplicação da lei teriam poderes para recorrer à tecnologia de reconhecimento facial. Devido à referência a outros tipos de dados e à necessidade explícita de garantias especiais sem especificações adicionais, a disposição que transpõe o artigo 10.º da Diretiva Proteção de Dados na Aplicação da Lei para o direito nacional – com uma redação igualmente geral e abstrata – não pode ser invocada como base jurídica para o tratamento de dados biométricos que envolvam o reconhecimento facial, uma vez que careceria de precisão e previsibilidade. Em conformidade com o artigo 28.º, n.º 2, ou com o artigo 46.º, n.º 1, alínea c), da Diretiva Proteção de Dados na Aplicação da Lei, antes de o legislador criar uma base jurídica para qualquer forma de tratamento de dados biométricos utilizando reconhecimento facial, a autoridade nacional de controlo em matéria de proteção de dados deve ser consultada.

3.2.1.2 Estritamente necessário

73. O tratamento só pode ser considerado «estritamente necessário» se a ingerência na proteção de dados pessoais e nas suas restrições ocorrer na estrita medida do necessário[52]. O aditamento do termo «estritamente» significa que o legislador pretendia que o tratamento de categorias especiais de dados apenas ocorresse em condições ainda mais estritas do que as condições relativas à necessidade (ver ponto 3.1.3.4 *supra*). Este requisito deve ser interpretado como indispensável. Restringe ao mínimo absoluto a margem de apreciação concedida à autoridade de aplicação da lei no teste da necessidade. Em conformidade com a jurisprudência constante do TJUE, a condição de «necessidade estrita» está também intimamente ligada à exigência de critérios objetivos para definir as circunstâncias e as condições nas quais o tratamento pode ser efetuado, excluindo assim qualquer tratamento de natureza geral ou sistemática[53].

3.2.1.3 Manifestamente tornados públicos

74. Ao apurar se o tratamento diz respeito a dados manifestamente tornados públicos pelo titular dos dados, importa recordar que uma fotografia, enquanto tal, não é sistematicamente considerada um dado biométrico[54]. Por conseguinte, o facto de uma fotografia ter sido manifestamente tornada pública pelo titular dos dados não implica que se possa considerar que os dados biométricos correspondentes, que podem ser extraídos da fotografia recorrendo a meios técnicos específicos, foram manifestamente tornados públicos.

75. Quanto aos dados pessoais em geral, para que se considere que os dados biométricos foram manifestamente tornados públicos pelo titular dos dados, este deve ter deliberadamente tornado o modelo biométrico (e não apenas uma imagem facial) livremente acessível e público através de uma fonte aberta. Se um terceiro divulgar os dados biométricos, não se pode considerar que os dados tenham sido manifestamente tornados públicos pelo seu titular.

76. Além disso, não basta interpretar o comportamento de um titular de dados para considerar que os dados biométricos foram manifestamente tornados públicos. Por exemplo, no caso das redes sociais

[52] Jurisprudência constante relativa ao direito fundamental ao respeito pela vida privada, ver Acórdão de 16 de dezembro de 2008, Satakunnan Markkinapörssi e Satamedia, C-73/07, EU:C:2008:727, n.º 56; Acórdão de 9 de novembro de 2010, Volker und Markus Schecke, C-92/09 e C-93/09, EU:C:2010:662, n.º 77; Acórdão de 8 de abril de 2014, Digital Rights Ireland, C-594/12, EU:C:2014:238, n.º 52 e Acórdão de 6 de outubro de 2015, Schrems, C-362/14, EU:C:2015:650, n.º 92.

[53] Acórdão de 6 de outubro de 2020, Privacy International, C-623/17, EU:C:2020:790, n.º 78.

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

ou das plataformas em linha, o CEPD considera que o facto de o titular dos dados não ter ativado ou definido configurações específicas de privacidade não basta para considerar que tornou manifestamente públicos os seus dados pessoais e que esses dados (por exemplo, fotografias) podem ser transformados em modelos biométricos e utilizados para fins de identificação sem o seu consentimento. De um modo mais geral, quaisquer dados divulgados na sequência das configurações predefinidas de um serviço, por exemplo a disponibilização de modelos ao público, ou da ausência de escolha, por exemplo o facto de os modelos serem tornados públicos sem que o utilizador possa alterar essa configuração, não devem de forma alguma ser considerados dados manifestamente tornados públicos.

3.2.2 Decisões individuais automatizadas, incluindo a definição de perfis

77. O artigo 11.º, n.º 1, da Diretiva Proteção de Dados na Aplicação da Lei prevê a obrigação de os Estados-Membros proibirem, de um modo geral, decisões tomadas exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produzam efeitos adversos na esfera jurídica do titular dos dados ou que o afetem de forma significativa. Como exceção a esta proibição geral, esse tratamento só é possível se for autorizado pelo direito da União ou do Estado-Membro ao qual o responsável pelo tratamento está sujeito, e que preveja garantias adequadas dos direitos e liberdades do titular dos dados, pelo menos o direito de obter a intervenção humana do responsável pelo tratamento. Só pode ser utilizado de forma restritiva. Este limiar aplica-se a categorias normais (ou seja, não especiais) de dados pessoais. Aplica-se um limiar ainda mais elevado e uma utilização mais restritiva à isenção prevista no artigo 11.º, n.º 2, da Diretiva Proteção de Dados na Aplicação da Lei. Este sublinha novamente que as decisões tomadas ao abrigo do n.º 1 não se devem basear em categorias especiais de dados, nomeadamente dados biométricos para efeitos de identificação inequívoca de uma pessoa singular. Uma isenção só pode ser prevista se estiverem em vigor medidas adequadas para salvaguardar os direitos e liberdades do titular dos dados e os interesses legítimos da pessoa singular em causa. Esta isenção deve ser lida em complemento e à luz das disposições do artigo 10.º da mesma diretiva.

78. Dependendo do sistema de TRF, mesmo a intervenção humana para avaliar os resultados da TRF pode não constituir necessariamente uma garantia suficiente, por si só, de respeito pelos direitos individuais, nomeadamente do direito à proteção dos dados pessoais, tendo em conta o possível enviesamento e erro que podem resultar do próprio tratamento. Além disso, a intervenção humana só pode ser considerada uma salvaguarda se a pessoa que intervém puder contestar de forma crítica os resultados da TRF durante a intervenção humana. É fundamental capacitar a pessoa para compreender o sistema de TRF e os seus limites, bem como para interpretar corretamente os seus resultados. É igualmente necessário definir um local de trabalho e uma organização que contrariem os efeitos do enviesamento da automatização e evitem promover a aceitação acrítica dos resultados, por exemplo, através de pressão temporal, procedimentos onerosos, potenciais consequências negativas para a carreira, etc.

79. Nos termos do artigo 11.º, n.º 3, da Diretiva Proteção de Dados na Aplicação da Lei, em conformidade com o direito da União, são proibidas as definições de perfis que conduzam à discriminação de pessoas singulares com base nas categorias especiais de dados pessoais, como os dados biométricos. Nos termos do artigo 3.º, ponto 4, da Diretiva Proteção de Dados na Aplicação da Lei, entende-se por «definição de perfis» qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento,

localização ou deslocações. Ao considerar se estão previstas medidas adequadas para salvaguardar os direitos e liberdades do titular dos dados e os interesses legítimos da pessoa singular em causa, há que ter em conta que a utilização da TRF pode conduzir à definição de perfis, dependendo da forma como a TRF é aplicada e da sua finalidade. De qualquer das formas, em conformidade com o direito da União e com o artigo 11.º, n.º 3, da Diretiva Proteção de Dados na Aplicação da Lei, são proibidas as definições de perfis que conduzam à discriminação de pessoas singulares com base em categorias especiais de dados pessoais.

3.2.3 Categorias de titulares de dados

80. O artigo 6.º da Diretiva Proteção de Dados na Aplicação da Lei diz respeito à necessidade de distinguir entre diferentes categorias de titulares de dados. Esta distinção tem de ser feita se aplicável e na medida do possível. Tem de produzir efeitos na forma como os dados são tratados. A partir dos exemplos apresentados no artigo 6.º da Diretiva Proteção de Dados na Aplicação da Lei, pode deduzir-se que, regra geral, o tratamento de dados pessoais tem de satisfazer os critérios da necessidade e da proporcionalidade também no que respeita à categoria dos titulares dos dados[55]. Além disso, pode deduzir-se que, no que diz respeito aos titulares de dados em relação aos quais não haja indícios que levem a acreditar que o seu comportamento possa ter um nexo, ainda que indireto ou longínquo, com o objetivo legítimo de acordo com a diretiva, muito provavelmente não há justificação para uma ingerência[56]. Se não for aplicável ou possível qualquer distinção em conformidade com o artigo 6.º da Diretiva Proteção de Dados na Aplicação da Lei, a exceção à regra desse artigo tem de ser rigorosamente analisada no contexto da avaliação da necessidade e da proporcionalidade da ingerência. A distinção entre as diferentes categorias de titulares de dados afigura-se um requisito essencial no que diz respeito ao tratamento de dados pessoais que envolva reconhecimento facial, tendo igualmente em conta os eventuais falsos positivos ou falsos negativos, que podem ter impactos significativos para os titulares dos dados, bem como no decurso de uma investigação.

81. Como foi dito, ao aplicar o direito da União, importa respeitar as disposições da Carta dos Direitos Fundamentais da União Europeia, ver artigo 52.º da Carta. O quadro e os critérios previstos na Diretiva Proteção de Dados na Aplicação da Lei devem, por conseguinte, ser lidos à luz da Carta. Os atos legislativos da UE e dos seus Estados-Membros não podem ficar aquém desta medida e têm de garantir o pleno efeito da Carta.

3.2.4 Direitos do titular dos dados

82. O CEPD já disponibilizou orientações sobre os direitos dos titulares dos dados ao abrigo do RGPD em diferentes aspetos[57]. A Diretiva Proteção de Dados na Aplicação da Lei prevê direitos semelhantes para os titulares de dados, tendo sido apresentadas orientações gerais sobre esta matéria num parecer do Grupo do Artigo 29.º, que foi aprovado pelo CEPD[58]. Em determinadas circunstâncias, a Diretiva Proteção de Dados na Aplicação da Lei permite algumas limitações a estes direitos. Os parâmetros dessas limitações serão descritos de forma mais pormenorizada na secção 3.2.4.6. «Limitações legítimas aos direitos dos titulares dos dados».

83. Embora todos os direitos do titular dos dados enumerados no capítulo III da Diretiva Proteção de Dados na Aplicação da Lei também se apliquem, naturalmente, ao tratamento de dados pessoais

[55] Ver também Acórdão de 8 de abril de 2014, Digital Rights Ireland, C-594/12, EU:C:2014:238, n.os 56 a 59.
[56] Ver também Acórdão de 8 de abril de 2014, Digital Rights Ireland, C-594/12, EU:C:2014:238, n.º 58.
[57] Ver, por exemplo, as Orientações 1/2022 sobre os direitos dos titulares dos dados – direito de acesso e as Diretrizes 3/2019 sobre tratamento de dados pessoais através de dispositivos de vídeo, ambas do CEPD.
[58] WP258, *Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)* [Parecer sobre algumas questões importantes da Diretiva relativa à proteção de dados na aplicação da lei (UE 2016/680)].

através de tecnologias de reconhecimento facial (TRF), o capítulo seguinte centrar-se-á em alguns dos direitos e em aspetos que poderão ser especialmente merecedores de orientações. Além disso, este capítulo e a sua análise dependem do facto de o tratamento de TRF em questão ter passado pelos requisitos legais descritos no capítulo anterior.

84. Dada a natureza do tratamento de dados pessoais através de TRF (tratamento de categorias especiais de dados pessoais, muitas vezes sem qualquer interação aparente com o titular dos dados), o responsável pelo tratamento deve ponderar cuidadosamente (se ou) de que forma pode cumprir os requisitos da Diretiva Proteção de Dados na Aplicação da Lei antes de iniciar qualquer tratamento de TRF. Pode fazê-lo, nomeadamente, através de uma análise cuidadosa:

- de quem são os titulares dos dados (muitas vezes, mais do que o(s) que é/são o principal alvo do tratamento),
- da forma como os titulares dos dados são informados do tratamento de TRF (ver secção 3.2.4.1);
- da forma como os titulares dos dados podem exercer os seus direitos (neste caso, tanto os direitos de informação e de acesso, como os direitos de retificação ou de limitação podem ser particularmente difíceis de defender no caso de todas as utilizações da TRF, com exceção da verificação de um para um, em contacto direto com o titular dos dados).

3.2.4.1 Dar a conhecer os direitos e as informações aos titulares dos dados de uma forma concisa, inteligível e de fácil acesso

85. As TRF suscitam desafios quando se trata de assegurar que os titulares dos dados são informados do tratamento dos seus dados biométricos. Esta garantia é particularmente difícil se uma autoridade de aplicação da lei estiver a analisar, através de material de vídeo de TRF proveniente ou fornecido por um terceiro, uma vez que é pouco provável e, na maior parte das vezes, impossível a autoridade de aplicação da lei notificar o titular dos dados no momento da recolha (por exemplo, através de um sinal no local). Qualquer material de vídeo que não seja relevante para a investigação (ou para a finalidade do tratamento) deve ser sempre eliminado ou anonimizado (por exemplo, através de desfocagem sem possibilidade de recuperação retroativa dos dados) antes de efetuar qualquer tratamento de dados biométricos, a fim de evitar o risco de incumprimento do princípio da minimização previsto no artigo 4.º, n.º 1, alínea e), da Diretiva Proteção de Dados na Aplicação da Lei e das obrigações de informação previstas no artigo 13.º, n.º 2, da mesma diretiva. Cabe ao responsável pelo tratamento avaliar quais as informações que seriam importantes para o titular dos dados no exercício dos seus direitos e assegurar que sejam fornecidas as informações necessárias. O exercício efetivo dos direitos do titular dos dados depende do cumprimento, pelo responsável pelo tratamento, das suas obrigações de informação.

86. O artigo 13.º, n.º 1, da Diretiva Proteção de Dados na Aplicação da Lei estipula quais as informações mínimas que, em geral, devem ser facultadas ao titular dos dados. Estas informações podem ser transmitidas através do sítio Web do responsável pelo tratamento, em formato impresso (por exemplo, um folheto disponível mediante pedido) ou através de outras fontes de fácil acesso para o titular dos dados. O responsável pelo tratamento de dados deve, em qualquer caso, assegurar a transmissão efetiva de informações, no mínimo em relação aos seguintes elementos:

- a identidade e os contactos do responsável pelo tratamento, incluindo o encarregado da proteção de dados,
- a finalidade do tratamento e o facto de se tratar de um tratamento através da TRF,

- o direito de apresentar uma reclamação junto de uma autoridade de controlo e os contactos dessa autoridade,
- o direito de solicitar o acesso, a retificação ou o apagamento dos dados pessoais e a limitação do tratamento dos dados pessoais.

87. Além disso, em casos específicos definidos na legislação nacional, que devem estar em conformidade com o artigo 13.º, n.º 2, da Diretiva Proteção de Dados na Aplicação da Lei[59], como, por exemplo, o tratamento através de TRF, as seguintes informações devem ser fornecidas diretamente ao titular dos dados:
    - a base jurídica aplicável ao tratamento,
    - informações sobre onde os dados pessoais foram recolhidos sem o conhecimento do titular dos dados,
    - o prazo de conservação dos dados pessoais ou, se tal não for possível, os critérios aplicados para definir esse prazo,
    - se aplicável, as categorias de destinatários dos dados pessoais (inclusive países terceiros ou organizações internacionais).

88. Enquanto o artigo 13.º, n.º 1, da Diretiva Proteção de Dados na Aplicação da Lei diz respeito às informações gerais disponibilizadas ao público, o n.º 2 do mesmo artigo diz respeito às informações adicionais a facultar a um titular de dados específico em determinados casos, por exemplo quando os dados são recolhidos diretamente junto do titular dos dados ou indiretamente sem o seu conhecimento[60]. Não existe uma definição clara do que se entende por «determinados casos» no artigo 13.º, n.º 2, da Diretiva Proteção de Dados na Aplicação da Lei. No entanto, a expressão refere-se a situações em que os titulares dos dados têm de ser informados de um tratamento que lhes diz especificamente respeito e de receber informações suficientes que lhes permitam exercer efetivamente os seus direitos. O CEPD considera que, ao avaliar se se trata de um «determinado caso», há que ter em conta vários fatores, nomeadamente se os dados pessoais são recolhidos sem o conhecimento do respetivo titular, uma vez que esta seria a única forma de permitir aos titulares dos dados exercerem efetivamente os seus direitos. Outros exemplos de «determinados casos» podem ser quando os dados pessoais são objeto de tratamento posterior no âmbito de um processo de cooperação penal internacional ou caso os dados pessoais sejam tratados no âmbito de operações com agentes infiltrados, tal como especificado na legislação nacional. Além disso, decorre do considerando 38 da Diretiva Proteção de Dados na Aplicação da Lei que, se a decisão for tomada exclusivamente com base em TRF, os titulares dos dados têm de ser informados das características da decisão automatizada. Tal indicaria também que se trata de um caso em que devem ser fornecidas informações adicionais ao titular dos dados, em conformidade com o artigo 13.º, n.º 2, da Diretiva Proteção de Dados na Aplicação da Lei[61].

---

[59] Por exemplo, o artigo 56.º, n.º 1, da Lei Federal de Proteção de Dados alemã, que estabelece, entre outros aspetos, quais as informações que têm de ser facultadas aos titulares dos dados em operações com agentes infiltrados.

[60] WP258, *Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)* [Parecer sobre algumas questões importantes da Diretiva relativa à proteção de dados na aplicação da lei (UE 2016/680)], p. 17.

[61] Note-se bem a diferença entre a expressão «faculte ao titular dos dados» no artigo 13.º, n.º 1, da Diretiva Proteção de Dados na Aplicação da Lei e a expressão «forneça ao titular dos dados» no n.º 2 do mesmo artigo. N.T.: A expressão no n.º 1 em inglês é «make available», que se pode traduzir de forma mais literal como «pôr à

89. Por último, importa salientar que, nos termos do artigo 13.º, n.º 3, da Diretiva Proteção de Dados na Aplicação da Lei, os Estados-Membros podem adotar medidas legislativas que restrinjam a obrigação de prestar informações em casos específicos e para determinados objetivos. Esta disposição aplica-se se e enquanto tais medidas constituírem medidas necessárias e proporcionadas numa sociedade democrática, tendo devidamente em conta os direitos fundamentais e os interesses legítimos do titular dos dados.

3.2.4.2 Direito de acesso

90. Em geral, o titular dos dados tem o direito de receber uma confirmação positiva ou negativa de qualquer tratamento dos seus dados pessoais e, em caso afirmativo, de aceder aos dados pessoais enquanto tal, acrescido de informações adicionais, tal como previsto no artigo 14.º da Diretiva Proteção de Dados na Aplicação da Lei. No caso da TRF, quando os dados biométricos estão armazenados e ligados a uma identidade também por dados alfanuméricos, tal deve permitir à autoridade competente confirmar um pedido de acesso com base numa pesquisa por esses dados alfanuméricos e sem iniciar qualquer outro tratamento de dados biométricos de terceiros (por exemplo, pesquisando com TRF numa base de dados). O princípio da minimização dos dados deve ser respeitado, não devendo ser conservados mais dados do que os necessários para a finalidade do tratamento.

3.2.4.3 Direito de retificação dos dados pessoais

91. Uma vez que a TRF não garante exatidão absoluta, é particularmente importante que os responsáveis pelo tratamento estejam atentos a eventuais pedidos de retificação de dados pessoais. Estes pedidos podem também surgir se um titular de dados baseados em TRF for colocado numa categoria errada, por exemplo inserido indevidamente na categoria de suspeitos com base no pressuposto inicial de um curso de ação depreendido de imagens de vídeo. Os riscos para os titulares dos dados são particularmente graves se esses dados inexatos forem armazenados numa base de dados da polícia e/ou partilhados com outras entidades. O responsável pelo tratamento deve corrigir os dados armazenados e os sistemas de TRF em conformidade, ver o considerando 47 da Diretiva Proteção de Dados na Aplicação da Lei.

3.2.4.4 Direito ao apagamento dos dados

92. A TRF equivalerá, na maioria das circunstâncias – no caso de não ser utilizada para verificação/autenticação de um para um – ao tratamento de um grande número de dados biométricos dos titulares dos dados. Por conseguinte, é importante que o responsável pelo tratamento pondere previamente quais são os limites da sua finalidade e necessidade, para que um pedido de apagamento nos termos do artigo 16.º da Diretiva Proteção de Dados na Aplicação da Lei possa ser tratado sem demora injustificada (uma vez que o responsável pelo tratamento precisa, nomeadamente, de apagar os dados pessoais que são tratados para além do permitido pela legislação aplicável nos termos dos artigos 4.º, 8.º e 10.º da Diretiva Proteção de Dados na Aplicação da Lei).

3.2.4.5 Direito à restrição

93. Caso a exatidão dos dados seja contestada pelo titular dos dados e não possa ser determinada (ou se os dados pessoais tiverem de ser conservados para efeitos de provas futuras), o responsável pelo tratamento tem a obrigação de limitar os dados pessoais desse titular de dados em conformidade com o artigo 16.º da Diretiva Proteção de Dados na Aplicação da Lei. Esta obrigação torna-se especialmente importante quando se trata de tecnologia de reconhecimento facial (baseada em algoritmos e que,

---

disposição», por oposição ao verbo «give», isto é, fornecer, utilizado no n.º 2. No artigo 13.º, n.º 2, da diretiva, o responsável pelo tratamento deve assegurar que as informações chegam ao titular dos dados, caso as informações publicadas num sítio Web não sejam suficientes.

por isso, nunca apresenta um resultado definitivo) em situações em que sejam recolhidas grandes quantidades de dados e em que a exatidão e a qualidade da identificação possam variar. Com materiais de vídeo de má qualidade (por exemplo, provenientes de uma cena de crime), o risco de falsos positivos aumenta. Além disso, se as imagens faciais de uma lista de observação não forem atualizadas regularmente, isso também aumentará o risco de falsos positivos ou falsos negativos. Em casos específicos, sempre que os dados não possam ser apagados devido ao facto de existirem motivos razoáveis para crer que o seu apagamento poderia afetar os interesses legítimos do respetivo titular, os dados devem, em vez disso, ser limitados e tratados apenas para a finalidade que impediu o seu apagamento (ver considerando 47 da Diretiva Proteção de Dados na Aplicação da Lei).

3.2.4.6 Limitações legítimas aos direitos dos titulares dos dados

94. No que diz respeito às obrigações de informação do responsável pelo tratamento e ao direito de acesso dos titulares dos dados, as limitações são permitidas apenas desde que estejam previstas na lei, que, por sua vez, tem de constituir uma medida necessária e proporcionada numa sociedade democrática, tendo devidamente em conta os direitos fundamentais e os interesses legítimos da pessoa singular em causa (ver artigo 13.º, n.^{os} 3 e 4, artigo 15.º e artigo 16.º, n.º 4, da Diretiva Proteção de Dados na Aplicação da Lei). Quando a TRF é utilizada para fins de aplicação da lei, pode esperar-se que seja utilizada em circunstâncias em que seria prejudicial à finalidade de informar o titular dos dados ou de permitir o acesso aos dados. Tal aplicar-se-ia, por exemplo, a uma investigação criminal ou para proteger a segurança nacional ou a segurança pública.

95. O direito de acesso não significa automaticamente o acesso a todas as informações, por exemplo num processo penal em que estejam em causa os dados pessoais de um indivíduo. Um exemplo viável de quando podem ser permitidas limitações a este direito pode ser no decurso de uma investigação criminal.

3.2.4.7 Exercício dos direitos através da autoridade de controlo

96. Nos casos em que existam limitações legítimas ao exercício dos direitos, de acordo com o capítulo III da Diretiva Proteção de Dados na Aplicação da Lei, o titular dos dados pode solicitar à autoridade de proteção de dados que exerça os seus direitos em seu nome, verificando a licitude do tratamento efetuado pelo responsável pelo tratamento. Compete ao responsável pelo tratamento informar o titular dos dados da possibilidade de exercer os seus direitos dessa forma (ver artigo 17.º e artigo 46.º, n.º 1, alínea g), da Diretiva Proteção de Dados na Aplicação da Lei). No caso da TRF, isto significa que o responsável pelo tratamento tem de assegurar a existência de medidas adequadas para que esse pedido possa ser tratado, por exemplo permitindo a pesquisa de material gravado, desde que o titular dos dados forneça informações suficientes para localizar os seus dados pessoais.

3.2.5 Outros requisitos legais e garantias

3.2.5.1 Artigo 27.º – Avaliação de impacto sobre a proteção de dados

97. A realização de uma avaliação de impacto sobre a proteção de dados (AIPD) antes da utilização de TRF é obrigatória, uma vez que o tipo de tratamento, em especial a utilização de novas tecnologias, e tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento, é suscetível de resultar num elevado risco para os direitos e liberdades das pessoas singulares. Uma vez que a utilização de TRF implica o tratamento automático sistemático de categorias especiais de dados, poderia presumir-se que, em tais casos, o responsável pelo tratamento seria, em regra, obrigado a realizar uma AIPD. A AIPD deve conter, no mínimo, uma descrição geral das operações de tratamento previstas, uma avaliação da necessidade e da proporcionalidade das operações de tratamento em relação às respetivas finalidades, uma avaliação dos riscos para os direitos e liberdades dos titulares dos dados, as medidas previstas para fazer face a esses riscos e as garantias, medidas de segurança e mecanismos

para assegurar a proteção dos dados pessoais e demonstrar a conformidade. O CEPD recomenda a divulgação ao público dos resultados dessas avaliações ou, pelo menos, das principais constatações e conclusões da AIPD, como medida de reforço da confiança e da transparência[62].

3.2.5.2 Artigo 28.º – Consulta prévia da autoridade de controlo

98. Nos termos do artigo 28.º da Diretiva Proteção de Dados na Aplicação da Lei, o responsável pelo tratamento ou subcontratante tem de consultar a autoridade de controlo antes de proceder ao tratamento, caso: a) a avaliação de impacto sobre a proteção de dados indique que o tratamento resultaria num elevado risco na ausência das medidas a tomar pelo responsável pelo tratamento para atenuar o risco; ou b) o tipo de tratamento envolva, especialmente no caso de se utilizarem novas tecnologias, mecanismos ou procedimentos, um elevado risco para os direitos e liberdades dos titulares dos dados. Tal como já se explicou na secção 2.3 das presentes orientações, o CEPD considera que a maioria dos casos de implantação e utilização de TRF implicam um risco intrinsecamente elevado para os direitos e liberdades dos titulares dos dados. Por conseguinte, para além da AIPD, a autoridade que implanta a TRF deve consultar a autoridade de controlo competente antes da implantação do sistema.

3.2.5.3 Artigo 29.º – Segurança do tratamento

99. A natureza única dos dados biométricos impossibilita que o titular dos dados os altere caso sejam comprometidos, por exemplo na sequência de uma violação de dados. Por conseguinte, a autoridade competente que aplica e/ou utiliza a TRF deve prestar especial atenção à segurança do tratamento, em conformidade com o artigo 29.º da Diretiva Proteção de Dados na Aplicação da Lei. Concretamente, a autoridade de aplicação da lei deve assegurar que o sistema cumpre as normas pertinentes e aplica medidas de proteção de modelos biométricos[63]. Esta obrigação é ainda mais relevante se a autoridade de aplicação da lei estiver a utilizar um prestador de serviços terceiro (subcontratante).

3.2.5.4 Artigo 20.º – Proteção de dados desde a conceção e por defeito

100. A proteção de dados desde a conceção e por defeito, em conformidade com o artigo 20.º da Diretiva Proteção de Dados na Aplicação da Lei, visa assegurar que os princípios e garantias da proteção de dados, como a minimização dos dados e a limitação da conservação, sejam incorporados na tecnologia através de medidas técnicas e organizativas adequadas, como a pseudonimização, mesmo antes do início do tratamento de dados pessoais, e sejam aplicados durante todo o seu ciclo de vida. Dado o elevado risco inerente para os direitos e liberdades das pessoas singulares, a escolha destas medidas não deve depender exclusivamente de considerações económicas[64], devendo antes procurar aplicar as tecnologias de proteção de dados de ponta. Na mesma ordem de ideias, uma autoridade de aplicação da lei que tencione aplicar e utilizar TRF de fornecedores externos tem de garantir, por exemplo através do procedimento de adjudicação de contratos, que apenas são utilizadas TRF baseadas nos princípios da proteção de dados desde a conceção e por defeito[65]. Isto implica também

[62] Para mais informações, ver WP248 rev.01 – Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679.

[63] Ver, por exemplo: ISO/IEC 24745 Segurança da informação, cibersegurança e proteção da privacidade – Proteção de informações biométricas.

[64] Ver o considerando 53 da Diretiva Proteção de Dados na Aplicação da Lei.

[65] Para mais informações, ver as Orientações 4/2019 relativas ao artigo 25.º – Proteção de Dados desde a Conceção e por Defeito, do CEPD, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf .

que a transparência do funcionamento das TRF não seja limitada pela reivindicação de segredos comerciais ou de direitos de propriedade intelectual.

3.2.5.5 Artigo 25.º – Registo cronológico

101. A Diretiva Proteção de Dados na Aplicação da Lei prevê diferentes métodos de demonstração, pelo responsável pelo tratamento ou pelo subcontratante, da licitude do tratamento e da garantia da integridade e segurança dos dados. Neste contexto, os registos do sistema são uma ferramenta muito útil e uma garantia importante para a verificação da licitude do tratamento, tanto a nível interno (ou seja, autocontrolo) como pelas autoridades de controlo externas, como as autoridades de proteção de dados. Nos termos do artigo 25.º da Diretiva Proteção de Dados na Aplicação da Lei, devem ser conservados em sistemas de tratamento automatizado registos pelo menos das seguintes operações de tratamento: recolha, alteração, consulta, divulgação (incluindo transferências), interconexão e apagamento. Além disso, os registos cronológicos das operações de consulta e divulgação devem permitir determinar o motivo, a data e a hora dessas operações e, na medida do possível, a identificação da pessoa que consultou ou divulgou dados pessoais, e a identidade dos destinatários desses dados pessoais. No contexto dos sistemas de reconhecimento facial, recomenda-se ainda o registo das seguintes operações de tratamento adicionais (parcialmente além do âmbito do artigo 25.º da Diretiva Proteção de Dados na Aplicação da Lei):

- Alterações da base de dados de referência (adição, supressão ou atualização). O registo deve conservar uma cópia da imagem relevante (adicionada, suprimida ou atualizada), sempre que não seja possível verificar de outro modo a licitude ou o resultado das operações de tratamento.

- Tentativas de identificação ou de verificação, incluindo o resultado e a pontuação de confiança. Deve aplicar-se o princípio da minimização estrita, de modo que apenas seja conservado nos registos o identificador da imagem da base de dados de referência, em vez da própria imagem de referência. Deve evitar-se o registo dos dados biométricos de entrada, a menos que seja necessário (por exemplo, apenas em casos de correspondência).

- A identificação do utilizador que solicitou a identificação ou a tentativa de verificação.

- Quaisquer dados pessoais armazenados nos registos dos sistemas estão sujeitos a limitações estritas de finalidade (por exemplo, auditorias) e não devem ser utilizados para outros fins (por exemplo, para poder continuar a efetuar o reconhecimento/verificação, incluindo uma imagem que tenha sido apagada das bases de dados de referência). Devem ser aplicadas medidas de segurança para garantir a integridade dos registos, ao passo que os sistemas automáticos de monitorização para detetar abusos de registos são altamente recomendados. Para os registos da base de dados de referência, as medidas de segurança devem ser equivalentes à base de dados de referência, em caso de conservação de imagens faciais. Além disso, devem ser instituídos processos automáticos para controlar o cumprimento do período de conservação dos dados dos registos.

3.2.5.6 Artigo 4.º, n.º 4 – Responsabilização

102. O responsável pelo tratamento tem de ser capaz de demonstrar a conformidade do tratamento com os princípios previstos no artigo 4.º, n.^{os} 1 a 3, da Diretiva Proteção de Dados na Aplicação da Lei – ver artigo 4.º, n.º 4, da diretiva. Para o efeito, é crucial uma documentação sistemática e atualizada do sistema (incluindo atualizações, novas versões e treino de algoritmos), das medidas técnicas e organizativas (incluindo o controlo do desempenho do sistema e a potencial intervenção humana) e do tratamento dos dados pessoais. Para demonstrar a licitude do tratamento, um elemento particularmente importante é o registo em conformidade com o artigo 25.º da Diretiva Proteção de Dados na Aplicação da Lei (ver secção 3.2.5.5). O princípio da responsabilização não se refere apenas

ao sistema e ao tratamento, mas também à documentação das garantias processuais, como as avaliações da necessidade e da proporcionalidade, as AIPD e as consultas internas (por exemplo, a aprovação do projeto pela direção ou as decisões internas sobre os valores da pontuação de confiança), bem como as consultas externas (por exemplo, a APD). O anexo II inclui uma série de elementos a este respeito.

3.2.5.7 Artigo 47.º – Supervisão eficaz

103. A supervisão eficaz por parte das autoridades competentes em matéria de proteção de dados é uma das garantias mais importantes dos direitos e liberdades fundamentais das pessoas afetadas pela utilização de TRF. Ao mesmo tempo, para o exercício eficaz das suas atribuições e dos seus poderes, é indispensável que cada autoridade de proteção de dados disponha dos recursos humanos, técnicos e financeiros, instalações e infraestruturas necessários[66]. Ainda mais importantes do que o número de pessoal disponível são as competências dos peritos, que devem abranger um vasto leque de temas, desde investigações criminais e cooperação policial até análise de megadados e IA. Por conseguinte, os Estados-Membros devem assegurar que os recursos das autoridades de controlo são adequados e suficientes para lhes permitir cumprir o seu mandato de proteção dos direitos dos titulares dos dados e acompanhar de perto quaisquer evoluções a este respeito[67].

4 CONCLUSÃO

104. A utilização de tecnologias de reconhecimento facial está intrinsecamente ligada ao tratamento de quantidades significativas de dados pessoais, incluindo categorias especiais de dados. O rosto e, de um modo mais geral, os dados biométricos estão permanente e irrevogavelmente ligados à identidade de uma pessoa. Por conseguinte, a utilização do reconhecimento facial tem um impacto direto ou indireto numa série de direitos e liberdades fundamentais consagrados na Carta dos Direitos Fundamentais da UE, que podem ir além da privacidade e da proteção de dados, tais como a dignidade humana, a liberdade de circulação, a liberdade de reunião, entre outros. Este aspeto é de particular importância no domínio da aplicação da lei e da justiça penal.

105. O CEPD compreende a necessidade das autoridades de aplicação da lei de beneficiarem das melhores ferramentas possíveis para poderem identificar rapidamente os autores de atos terroristas ou de outros crimes graves. No entanto, estas ferramentas devem ser utilizadas em estrita conformidade com o quadro jurídico aplicável e apenas nos casos em que satisfaçam os requisitos em matéria de necessidade e proporcionalidade previstos no artigo 52.º, n.º 1, da Carta. Além disso, embora possam fazer parte da solução, as tecnologias modernas não são de modo algum uma «bala de prata».

106. Existem certos casos de utilização de tecnologias de reconhecimento facial que representam riscos inaceitavelmente elevados para os indivíduos e para a sociedade («linhas vermelhas»). Por estes motivos, o CEPD e a AEPD apelaram à sua proibição geral[68].

---

[66] Ver Comunicação da Comissão ao Parlamento Europeu e ao Conselho – Primeiro relatório sobre a aplicação e o funcionamento da Diretiva (UE) 2016/680 relativa à proteção de dados na aplicação da lei («Diretiva Proteção de Dados na Aplicação da Lei»), COM(2022) 364 final, ponto 3.4.1.

[67] Ver *Contribution of the EDPB to the European Commission's evaluation of the Data Protection Law Enforcement Directive (LED) under Article 62* [Contributo do CEPD para a avaliação, pela Comissão Europeia, da Diretiva Proteção de Dados na Aplicação da Lei ao abrigo do artigo 62.º], n.º 14, https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf

[68] Ver o Parecer conjunto 5/2021 do CEPD e da AEPD sobre a proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento

107. Concretamente, a identificação biométrica à distância de indivíduos em espaços acessíveis ao público representa um elevado risco de intrusão na vida privada dos indivíduos e não tem lugar numa sociedade democrática, uma vez que, pela sua natureza, implica uma vigilância em massa. Na mesma ordem de ideias, o CEPD considera incompatíveis com a Carta os sistemas de reconhecimento facial apoiados pela IA que categorizem, com base na biometria, indivíduos em grupos de acordo com a origem étnica, o género, bem como a orientação sexual ou política. Além disso, o CEPD está convicto de que a utilização do reconhecimento facial ou de tecnologias semelhantes para inferir as emoções de uma pessoa singular é extremamente indesejável e deve ser proibida, possivelmente com poucas exceções devidamente justificadas. Além disso, o CEPD considera que o tratamento de dados pessoais num contexto de aplicação da lei assente numa base de dados preenchida pela recolha de dados pessoais em massa e indiscriminada, por exemplo através da «raspagem» de fotografias e imagens faciais acessíveis em linha, em especial as disponibilizadas através das redes sociais, não respeitaria, como tal, o requisito da necessidade estrita previsto no direito da União.

5 ANEXOS

Anexo I: Padrão de apoio

Anexo II: Orientações práticas para a gestão de projetos de TRF pelas autoridades de aplicação da lei

Anexo III: Exemplos práticos

Inteligência Artificial) https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

ANEXO I – MODELO PARA A DESCRIÇÃO DE CENÁRIOS

(Com caixas informativas para os aspetos abordados pelo cenário)

Descrição do tratamento:

- Descrição do tratamento, Contexto (ligação à criminalidade), Finalidade

Fonte da informação:

- Tipos de titulares dos dados: ☐ todos os cidadãos ☐ reclusos ☐ suspeitos ☐ crianças ☐ outros titulares de dados vulneráveis
- Fonte da imagem: ☐ espaços acessíveis ao público ☐ Internet ☐ entidade privada ☐ outros indivíduos ☐ outra .....
- Ligação à criminalidade: ☐ Temporal direta ☐ Temporal indireta ☐ Geográfica direta ☐ Geográfica indireta ☐ Não necessária
- Modo de recolha das informações: ☐ à distância ☐ numa cabina ou em ambiente controlado
- Contexto – que afete outros direitos fundamentais:
  ☐ Não
  Sim, nomeadamente ☐ liberdade de reunião
  ☐ Liberdade de expressão
  ☐ Diversos:.....
- Possibilidades de fontes adicionais de informação sobre o titular dos dados:
  ☐ Documento de identificação ☐ utilização de telefone público ☐ matrícula de veículo
  ☐ outra .....

Base de dados de referência (com a qual a informação captada é comparada):

- Especificidade: ☐ bases de dados gerais ☐ bases de dados específicas relacionadas com a categoria de crime
- Descrição da forma como estas bases de dados de referência foram preenchidas (e base jurídica)
- Alteração da finalidade da base de dados (por exemplo, a segurança da propriedade privada era o objetivo principal): ☐ SIM ☐ NÃO

Algoritmo:

- Tipo de tratamento: ☐ verificação de um para um (autenticação) ☐ identificação de um para muitos
- Considerações em matéria de exatidão
- Meios técnicos de proteção

Resultado:

- Impacto ☐ Direto (por exemplo, o titular dos dados pode ser detido, interrogado, comportamento discriminatório)

  ☐ Indireto (utilizado para modelos estatísticos, ausência de ação judicial grave contra os titulares dos dados)

- Decisão automatizada: ☐ SIM ☐ NÃO
- Duração da conservação

Análise jurídica:

- Análise da necessidade e da proporcionalidade – finalidade/gravidade do crime/número de pessoas não envolvidas, mas afetadas pelo tratamento
- Tipo de informação prévia ao titular dos dados: ☐ Ao entrar na zona específica

  ☐ No sítio Web da autoridade de aplicação da lei em geral

  ☐ No sítio Web da autoridade de aplicação da lei para o tratamento específico

  ☐ Outro .....
- Quadro jurídico aplicável:

  ☐ Diretiva Proteção de Dados na Aplicação da Lei, maioritariamente transposta para a legislação nacional

  ☐ Legislação nacional genérica relativa à utilização de dados biométricos pelas autoridades de aplicação da lei

  ☐ Legislação nacional específica relativa a este tratamento (reconhecimento facial) aplicável à autoridade competente em questão

  ☐ Legislação nacional específica relativa a este tratamento (decisão automatizada)

Conclusão:

Considerações gerais sobre a probabilidade de o tratamento descrito ser compatível com a legislação da UE (e algumas sugestões sobre pré-requisitos jurídicos).

ANEXO II – ORIENTAÇÕES PRÁTICAS PARA A GESTÃO DE PROJETOS DE TRF PELAS AUTORIDADES DE APLICAÇÃO DA LEI

O presente anexo apresenta algumas orientações práticas adicionais para as autoridades de aplicação da lei que planeiem iniciar um projeto que envolva tecnologias de reconhecimento facial («TRF»). Contém mais informações sobre as medidas organizativas e técnicas a ter em conta durante a implantação do projeto e não deve ser considerado como uma lista exaustiva de etapas/medidas a tomar. Além disso, deve ser lido em conjugação com as Diretrizes 3/2019 sobre tratamento de dados pessoais através de dispositivos de vídeo[69] do CEPD e com qualquer regulamento da UE/EEE e orientações do CEPD relativos à utilização da inteligência artificial.

O presente anexo disponibiliza orientações com base no pressuposto de que as autoridades de aplicação da lei adquirirão TRF (como produtos comerciais). Se a autoridade de aplicação da lei planeia desenvolver (continuar a treinar) a TRF, então aplicam-se requisitos adicionais para selecionar os conjuntos de dados de treino, de validação e de teste necessários para utilizar durante o desenvolvimento e os papéis/medidas para o ambiente de desenvolvimento. Do mesmo modo, um produto comercial pode exigir ajustamentos adicionais para a utilização prevista, caso em que devem ser cumpridos os requisitos acima mencionados relativos à seleção dos conjuntos de dados de teste, validação e treino.

Pertencer à mesma autoridade de aplicação da lei não proporciona, por si só, pleno acesso aos dados biométricos. Tal como acontece com quaisquer outras categorias de dados pessoais, os dados biométricos recolhidos para uma determinada finalidade de aplicação da lei ao abrigo de uma base jurídica específica não podem ser utilizados sem uma base jurídica adequada para uma finalidade de aplicação da lei distinta (artigo 4.º, n.º 2, da Diretiva (UE) 2016/680 – Diretiva Proteção de Dados na Aplicação da Lei). Além disso, o desenvolvimento/treino de uma ferramenta de TRF é considerado uma finalidade distinta, pelo que é necessário avaliar se o tratamento de dados biométricos para avaliar o desempenho/treinar a tecnologia de modo a evitar eventuais impactos nos titulares dos dados resultantes de um baixo desempenho é necessário e proporcional, tendo em conta a finalidade inicial do tratamento.

1. FUNÇÕES E RESPONSABILIDADES

Quando uma autoridade de aplicação da lei utiliza TRF para o desempenho das suas atribuições abrangidas pelo âmbito de aplicação da Diretiva Proteção de Dados na Aplicação da Lei (prevenção, investigação, deteção ou repressão de infrações penais, etc., nos termos do artigo 3.º da Diretiva Proteção de Dados na Aplicação da Lei), esta autoridade pode ser considerada o responsável pelo tratamento para a TRF. No entanto, as autoridades de aplicação da lei são compostas por várias unidades/departamentos que podem estar envolvidos neste tratamento, quer definindo o processo de aplicação da TRF, quer aplicando-a na prática. Devido às especificidades desta tecnologia, pode ser necessário envolver diferentes unidades para apoiar as avaliações do seu desempenho ou para a treinar melhor.

[69] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

Num projeto que envolva TRF, existem várias partes interessadas[70] no seio das autoridades de aplicação da lei que podem ter de estar envolvidas:

- Direção – aprovar o projeto depois de ponderar os riscos e os potenciais benefícios.
- EPD e/ou departamento jurídico da autoridade de aplicação da lei – prestar assistência na avaliação da licitude da execução de um determinado projeto de TRF; prestar assistência na realização da AIPD; assegurar o respeito e o exercício dos direitos dos titulares dos dados.
- Proprietário do processo – atuar como a unidade específica dentro da autoridade de aplicação da lei competente para desenvolver o projeto, decidir sobre os detalhes do projeto de TRF, incluindo os requisitos de desempenho do sistema; decidir sobre a métrica de equidade adequada; definir a pontuação de confiança[71]; fixar limiares aceitáveis de enviesamento; identificar os potenciais riscos que o projeto de TRF representa para os direitos e liberdades das pessoas (consultando também o EPD e o departamento informático de IA e/ou ciência de dados (ver abaixo) e apresentá-los à direção. O proprietário do processo consultará igualmente o gestor da base de dados de referência antes de decidir sobre os detalhes do projeto de TRF, para compreender tanto a finalidade da utilização da base de dados de referência como os seus detalhes técnicos. No caso de um novo treino de uma TRF adquirida, o proprietário do processo será também responsável pela seleção do conjunto de dados de treino. Na qualidade de unidade encarregada de desenvolver e decidir os pormenores do projeto, o proprietário do processo é responsável pela realização da AIPD.
- Departamento informático de IA e/ou ciência de dados – ajudar na realização de uma AIPD; explicar as métricas disponíveis para avaliar o desempenho, a equidade[72] e o potencial enviesamento do sistema; implementar a tecnologia e os meios técnicos de proteção para impedir o acesso não autorizado aos dados recolhidos, ciberataques, etc. Em caso de novo treino de uma TRF adquirida, o departamento informático de IA ou de ciência de dados treinará o sistema com base no conjunto de dados de treino fornecido pelo proprietário do processo. Este departamento também será responsável pela elaboração de medidas para reduzir os riscos identificados conjuntamente pelos proprietários do processo (por exemplo, riscos específicos da IA, tais como ataques de inferência de modelo).
- Utilizadores finais (tais como os agentes da polícia no terreno ou nos laboratórios forenses) – para efetuar uma comparação com a base de dados; para analisar os resultados com espírito crítico tendo em conta elementos de prova anteriores e dar *feedback* ao proprietário do processo sobre os falsos positivos e as indicações de possível discriminação.
- Gestor da base de dados de referência – a unidade específica da autoridade de aplicação da lei competente responsável pela acumulação e gestão da base de dados de referência, ou seja, a base de dados com a qual as imagens serão comparadas, incluindo o apagamento das imagens faciais após o período de conservação definido. Esta base de dados pode ser criada especificamente para o projeto de TRF previsto ou pode ser preexistente, para fins compatíveis.

[70] As seguintes funções são indicativas das diferentes partes interessadas e das suas responsabilidades num projeto de TRF. Embora a linguagem utilizada para descrever as funções no presente anexo não seja assertiva, cada autoridade de aplicação da lei tem de definir e atribuir funções semelhantes de acordo com a sua organização. Uma unidade pode acumular mais do que uma função, por exemplo o proprietário do processo e o gestor da base de dados de referência, ou o proprietário do processo e o departamento informático de IA e/ou ciência de dados (caso a unidade do proprietário do processo tenha todos os conhecimentos técnicos necessários).

[71] A pontuação de confiança é o nível de confiança da previsão (correspondência), sob a forma de uma probabilidade. Por exemplo, comparando dois modelos, existe um grau de confiança de 90 % de que estes pertençam à mesma pessoa. A pontuação de confiança é diferente do desempenho da TRF, mas afeta o desempenho. Quanto mais elevado for o limiar de confiança, menor será o número de falsos positivos e maior será o número de falsos negativos nos resultados da TRF.

[72] A equidade pode ser definida como a ausência de discriminação injusta e ilícita, como o preconceito de género ou racial.

O gestor da base de dados de referência é responsável por definir quando e em que circunstâncias as imagens faciais podem ser armazenadas, bem como por estabelecer os respetivos requisitos de conservação de dados (em função do tempo ou de outros critérios).

Uma vez que, na sua maioria, os casos de implantação e utilização de TRF implicam um risco intrinsecamente elevado para os direitos e liberdades dos titulares dos dados, a autoridade de controlo responsável pela proteção dos dados deve também ser envolvida no contexto da consulta prévia exigida pelo artigo 28.º da Diretiva Proteção de Dados na Aplicação da Lei.

2. INÍCIO/ANTES DA AQUISIÇÃO DO SISTEMA DE TRF

O proprietário do processo numa autoridade de aplicação da lei deve, em primeiro lugar, ter uma compreensão clara do(s) processo(s) que utiliza(m) a TRF (os casos de utilização) e assegurar a existência de uma base jurídica que fundamente o caso de utilização previsto. Neste contexto, precisa de:

- Descrever formalmente o caso de utilização. Importa descrever o problema a resolver e a forma como a TRF apresentará uma solução, bem como a visão geral do processo (tarefa) a que será aplicada. A este respeito, as autoridades de aplicação da lei devem documentar, pelo menos[73]:
  - As categorias dos dados pessoais registados no processo.
  - Os objetivos e as finalidades concretas para os quais a TRF será utilizada, incluindo as possíveis consequências de uma correspondência para o titular dos dados.
  - Quando e como serão recolhidas as imagens faciais (incluindo informações sobre o contexto desta recolha, por exemplo na porta do aeroporto, em vídeos de câmaras de segurança no exterior de uma loja onde foi cometido um crime, etc., bem como as categorias dos titulares de dados cujos dados biométricos serão tratados).
  - A base de dados com a qual as imagens serão comparadas (base de dados de referência), bem como informações sobre a forma como foi criada, a sua dimensão e a qualidade dos dados biométricos que contém.
  - Os agentes da autoridade de aplicação da lei que serão autorizados a utilizar o sistema de TRF e a atuar no contexto da aplicação da lei (os seus perfis e direitos de acesso devem ser definidos pelo proprietário do processo).
  - O período de conservação previsto dos dados de entrada, ou o momento que determinará o final deste período (tal como o encerramento ou a conclusão do processo penal, em conformidade com o direito processual nacional, para o qual os dados foram inicialmente recolhidos), bem como qualquer ação subsequente (apagamento destes dados, anonimização e utilização para fins estatísticos ou de investigação, etc.).
  - Implementação do registo cronológico e acessibilidade dos registos conservados.
  - As métricas de desempenho (por exemplo, exatidão, precisão, recordação, pontuação F1) e os respetivos limiares mínimos aceitáveis[74].

[73] O anexo I apresenta uma lista de elementos que ajudam o responsável pelo tratamento a descrever um caso de utilização de TRF.

[74] Existem diferentes métricas para avaliar o desempenho de um sistema de TRF. Cada parâmetro apresenta uma visão diferente dos resultados do sistema, e o seu êxito na transmissão de uma imagem adequada de se o sistema de TRF está ou não a ter um bom desempenho depende do caso de utilização da TRF. Se a ênfase for colocada na obtenção de percentagens elevadas de correspondências corretas de um rosto, podem ser utilizados parâmetros como a precisão e a recordação. No entanto, estes parâmetros não avaliam a eficácia da TRF no tratamento de exemplos negativos (número de correspondências erradas do sistema). O proprietário do processo, apoiado pelos departamentos informáticos de IA e ciência de dados, deve ser capaz de definir os

- Estimativa do número de pessoas que serão sujeitas a TRF em que período/ocasião.

- Realizar uma avaliação da necessidade e da proporcionalidade[75]. A mera existência desta tecnologia não deve ser o que motiva a sua aplicação. O proprietário do processo deve, em primeiro lugar, avaliar se existe uma base jurídica adequada para o tratamento previsto. Para o efeito, é necessário consultar o EPD e o serviço jurídico. O motivo da implantação da TRF deve ser o facto de esta ser a solução necessária e proporcionada para um problema concretamente definido das autoridades de aplicação da lei. Tal tem de ser avaliado de acordo com a finalidade/gravidade do crime/número de pessoas não envolvidas, mas afetadas pelo sistema de TRF. Para a avaliação da licitude, importa analisar, no mínimo, os seguintes: a Diretiva Proteção de Dados na Aplicação da Lei[76], o RGPD[77] [78], qualquer quadro jurídico em vigor em matéria de IA[79] e todas as orientações de acompanhamento fornecidas pelas autoridades de controlo em matéria de proteção de dados (tais como as Diretrizes 3/2019 sobre tratamento de dados pessoais através de dispositivos de vídeo do CEPD[80]). Estes atos legislativos da UE devem ser sempre corroborados pelos requisitos nacionais aplicáveis, sobretudo no domínio do direito processual penal. A avaliação da proporcionalidade deve identificar os direitos fundamentais dos titulares dos dados que podem ser afetados (para além da privacidade e da proteção de dados). Deve também descrever e analisar os eventuais limites (ou falta de limites) impostos ao sistema de TRF no caso de utilização concreto. Por exemplo, se o sistema funcionará de forma contínua ou temporária e se será circunscrito a uma área geográfica.
- Realizar uma avaliação de impacto sobre a proteção de dados (AIPD)[81]. Deve ser realizada uma AIPD, uma vez que a implantação da TRF no domínio da aplicação da lei é suscetível de resultar num elevado risco para os direitos e liberdades dos indivíduos[82]. A AIPD deve conter,

requisitos de desempenho e expressá-los na métrica mais adequada de acordo com o caso de utilização da TRF em causa.

[75] Podem ser ponderadas medidas adicionais para avaliar a necessidade no que diz respeito à adaptação e utilização do sistema, pelo que a descrição do caso de utilização pode também ser ligeiramente alterada durante a avaliação da necessidade e da proporcionalidade.

[76] 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.

[77] 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.

[78] Nos casos em que um projeto científico destinado a investigar a utilização da TRF tenha de proceder ao tratamento de dados pessoais, mas esse tratamento não seja abrangido pelo artigo 4.º, n.º 3, da Diretiva Proteção de Dados na Aplicação da Lei, regra geral é aplicável o RGPD (artigo 9.º, n.º 2, da Diretiva Proteção de Dados na Aplicação da Lei). No caso de projetos-piloto que seriam seguidos de operações de aplicação da lei, continuaria a ser aplicável a Diretiva Proteção de Dados na Aplicação da Lei.

[79] Por exemplo, existe uma proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União, mas que ainda não foi estabelecida como regulamento.

[80] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

[81] Podem ser consultadas mais orientações sobre a AIPD no seguinte documento: WP248 rev.01 – Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679, disponível em: https://ec.europa.eu/newsroom/article29/items/611236 e no conjunto de ferramentas do CEPD sobre responsabilização no terreno, parte II, disponível em: https://edps.europa.eu/node/4582_en.

[82] A TRF, dependendo do caso de utilização, pode enquadrar-se nos seguintes critérios que desencadeiam um tratamento de alto risco (das Orientações relativas à AIPD, WP248 rev.01): monitorização sistemática, tratamento de dados em grande escala, correspondência ou combinação de conjuntos de dados, utilização inovadora ou aplicação de novas soluções tecnológicas ou organizativas.

nomeadamente: uma descrição geral das operações de tratamento previstas[83], uma avaliação dos riscos para os direitos e liberdades dos titulares dos dados[84], as medidas previstas para fazer face a esses riscos e as garantias, medidas de segurança e mecanismos para assegurar a proteção dos dados pessoais e demonstrar a conformidade. A AIPD é um processo contínuo, pelo que importa acrescentar quaisquer novos elementos do tratamento e atualizar a avaliação dos riscos em todas as fases do projeto.

- Obter a aprovação da direção, explicando os riscos para os direitos e liberdades dos titulares dos dados (decorrentes do caso de utilização e da tecnologia) e os respetivos planos de tratamento dos riscos.

3. DURANTE A AQUISIÇÃO E ANTES DA IMPLANTAÇÃO DA TRF

- Decidir os critérios para selecionar a TRF (algoritmo). O proprietário do processo deve decidir os critérios para selecionar um algoritmo, com a ajuda do departamento informático de IA e/ou ciência de dados. Na prática, estes incluiriam parâmetros de equidade e de desempenho decididos na descrição do caso de utilização. Estes critérios devem também incluir informações relacionadas com os dados com os quais o algoritmo foi treinado. O conjunto de treino, teste e validação tem de incluir amostras suficientes de todas as características dos titulares dos dados a submeter à TRF (por exemplo, idade, sexo e raça) para reduzir os enviesamentos. O fornecedor da TRF deve disponibilizar informações e métricas sobre os conjuntos de dados de treino, teste e validação da TRF e descrever as medidas tomadas para medir e atenuar potenciais discriminações ilícitas e enviesamentos. O proprietário do processo, sempre que possível, tem de verificar a existência de uma base jurídica para o fornecedor utilizar este conjunto de dados para treino dos algoritmos (com base nas informações disponibilizadas pelo fornecedor). Além disso, o proprietário do processo deve assegurar que o fornecedor da TRF aplica normas de segurança relacionadas com os dados biométricos, tais como a norma ISO/IEC 24745, que forneçam orientações para a proteção dos dados biométricos ao abrigo de vários requisitos de confidencialidade, integridade e renovação/revogabilidade durante a conservação e a transmissão e requisitos e orientações para a gestão e o tratamento seguros e compatíveis com a privacidade de informações biométricas.

- Treinar novamente o algoritmo (se necessário). O proprietário do processo deve garantir que o ajuste do sistema de TRF para obter uma maior precisão antes da sua utilização também faz parte dos serviços contratados. Caso seja necessário treino adicional do sistema de TRF adquirido para cumprir as métricas de exatidão, o proprietário do processo, para além de tomar a decisão de treinar novamente o sistema, tem de decidir, com a ajuda do departamento informático de IA e/ou ciência de dados, sobre o conjunto de dados adequado e representativo a utilizar e verificar a licitude desta utilização dos dados.
- Estabelecer as garantias adequadas para tratar os riscos relacionados com a segurança, o enviesamento e o baixo desempenho. Tal inclui a criação de um processo para monitorizar a TRF assim que estiver a ser utilizada (registo e *feedback* sobre a exatidão e a equidade dos resultados).

[83] A descrição do tratamento, bem como a avaliação da necessidade e da proporcionalidade, tal como já foi descrito nas etapas anteriores, também fazem parte da AIPD, para além da avaliação dos riscos. Se necessário, a AIPD conterá uma descrição mais pormenorizada dos fluxos de dados pessoais.

[84] A análise dos riscos para os titulares dos dados deve incluir os riscos relacionados com o local onde se encontram as imagens faciais a comparar (local/remoto), os riscos relacionados com os subcontratantes/subcontratantes ulteriores, bem como os riscos específicos da aprendizagem automática quando esta é aplicada (por exemplo, contaminação de dados, exemplos antagónicos).

Além disso, deve assegurar que os riscos que são específicos de alguns sistemas de aprendizagem automática e TRF (por exemplo, contaminação de dados, exemplos antagónicos, inversão de modelo, inferência de caixa branca) são identificados, avaliados e atenuados. O proprietário do processo deve também estabelecer garantias adequadas para assegurar o respeito dos requisitos de conservação dos dados biométricos incluídos no conjunto de dados a utilizar para o novo treino.

- Documentar o sistema de TRF. Esta documentação deve incluir uma descrição geral do sistema de TRF, uma descrição pormenorizada dos elementos do sistema de TRF e do respetivo processo de estabelecimento, informações pormenorizadas sobre a monitorização, o funcionamento e o controlo do sistema de TRF e uma descrição pormenorizada dos seus riscos e medidas de atenuação. Os elementos incluídos nesta documentação incluirão os principais elementos da descrição do sistema de TRF das fases anteriores (ver *supra*); no entanto, estes serão reforçados com informações relacionadas com a monitorização do desempenho e a aplicação de alterações ao sistema, incluindo quaisquer atualizações de versões e/ou novo treino.
- Criar manuais de utilizador, explicando a tecnologia e os casos de utilização. Estes têm de explicar todos os cenários e pré-requisitos sob os quais a TRF será utilizada de uma forma clara.
- Formar os utilizadores finais sobre a utilização da tecnologia. Estas formações têm de explicar as capacidades e as limitações da tecnologia, para que os utilizadores possam compreender as circunstâncias em que é necessário aplicá-la e os casos em que esta pode ser inexata. Estas formações também ajudarão a reduzir os riscos relacionados com a ausência de verificação/crítica do resultado do algoritmo.
- Consultar a autoridade de controlo em matéria de proteção de dados, nos termos do artigo 28.º, n.º 1, alínea b), da Diretiva Proteção de Dados na Aplicação da Lei. Fornecer informações nos termos do artigo 13.º da Diretiva Proteção de Dados na Aplicação da Lei para informar os titulares dos dados sobre o tratamento e os seus direitos. Estas notificações têm de se dirigir aos titulares dos dados numa linguagem adequada, para que estes possam compreender o tratamento e explicar os elementos básicos da tecnologia, incluindo os índices de exatidão, os conjuntos de dados de treino e as medidas tomadas para evitar a discriminação e a baixa exatidão do algoritmo.

4. RECOMENDAÇÕES APÓS A IMPLANTAÇÃO DA TRF

- Assegure a intervenção humana e a supervisão humana dos resultados. Nunca tome nenhuma medida que diga respeito a uma pessoa exclusivamente com base no resultado da TRF (tal implicaria uma violação do artigo 11.º da Diretiva Proteção de Dados na Aplicação da Lei, sobre as decisões individuais automatizadas que produzam efeitos jurídicos ou outros semelhantes no titular dos dados). Garanta que um agente da autoridade de aplicação da lei analisa os resultados da TRF. Garanta também que os utilizadores da autoridade de aplicação da lei evitam o enviesamento da automatização, investigando informações contraditórias e questionando, com espírito crítico, os resultados da tecnologia. Para o efeito, são importantes a formação e a sensibilização contínuas dos utilizadores finais. Contudo, a direção deve assegurar a existência de recursos humanos suficientes para uma supervisão eficaz. Tal implica dar tempo suficiente a cada agente para questionar de forma crítica os resultados da tecnologia. Registe, meça e avalie em que medida a supervisão humana altera a decisão original da TRF.
- Monitorize e corrija eventuais derivas do modelo de TRF (degradação do desempenho) quando o modelo estiver em produção.
- Defina um processo para reavaliar os riscos e as medidas de segurança regularmente e sempre que a tecnologia ou o caso de utilização sofra quaisquer alterações.
- Documente qualquer alteração do sistema ao longo do seu ciclo de vida (por exemplo, atualizações, novos treinos).

- Defina um processo, bem como as capacidades técnicas correspondentes, para responder a pedidos de acesso por parte dos titulares dos dados. As capacidades técnicas para a extração de dados, caso haja necessidade de os fornecer aos titulares dos dados, têm de estar operacionais antes da apresentação de qualquer pedido.
- Garanta que existem procedimentos para o caso de violações de dados. Caso ocorra uma violação de dados pessoais que envolva dados biométricos, é provável que os riscos sejam elevados. Neste caso, todos os utilizadores envolvidos devem ter conhecimento dos procedimentos pertinentes a seguir, o EPD deve ser imediatamente informado e os titulares dos dados devem ser informados.

ANEXO III – EXEMPLOS PRÁTICOS

Existem muitos contextos e finalidades práticas diferentes para a utilização do reconhecimento facial, nomeadamente em ambientes controlados como as passagens de fronteira, a verificação cruzada com dados de bases de dados policiais ou de dados pessoais manifestamente tornados públicos pelo titular dos dados, transmissões de câmaras em tempo real (reconhecimento facial em tempo real), etc. Consequentemente, os riscos para a proteção de dados pessoais e outros direitos e liberdades fundamentais variam significativamente nos diferentes casos de utilização. A fim de facilitar a avaliação da necessidade e da proporcionalidade, que deve preceder a decisão sobre a possível implantação do reconhecimento facial, as orientações atuais fornecem uma lista não exaustiva de possíveis aplicações da TRF no domínio da aplicação da lei.

Os cenários apresentados e avaliados baseiam-se em situações **hipotéticas** e destinam-se a ilustrar certas utilizações concretas da TRF e a prestar assistência para considerações caso a caso, bem como a estabelecer um quadro global. Não pretendem ser exaustivos e não prejudicam quaisquer procedimentos em curso ou futuros empreendidos por uma autoridade de controlo nacional no que diz respeito à conceção, experimentação ou implementação de tecnologias de reconhecimento facial. A apresentação destes cenários deve servir apenas para ilustrar as orientações destinadas aos decisores políticos, aos legisladores e às autoridades de aplicação da lei, já apresentadas no presente documento, aquando da conceção e do planeamento da implementação de tecnologias de reconhecimento facial, a fim de assegurar a plena conformidade com o acervo da UE no domínio da proteção de dados pessoais. Neste contexto, há que ter em conta que, mesmo em situações semelhantes de utilização da TRF, a presença ou ausência de determinados elementos pode conduzir a um resultado diferente na avaliação da necessidade e da proporcionalidade.

1 CENÁRIO 1

1.1. Descrição

Um sistema automatizado de controlo nas fronteiras que permite a passagem automatizada nas fronteiras através da autenticação da imagem biométrica armazenada no documento de viagem eletrónico de cidadãos da UE e outros viajantes que atravessam a fronteira e que confirma que o viajante é o titular legítimo do documento.

Essa verificação/autenticação envolve apenas reconhecimento facial de um para um e é efetuada num ambiente controlado (por exemplo, nas cancelas eletrónicas de um aeroporto). Os dados biométricos do viajante que atravessa a fronteira são recolhidos quando o viajante recebe instruções explícitas para olhar para a câmara na cancela eletrónica e são comparados com os do documento apresentado (passaporte, bilhete de identidade, etc.), que é emitido de acordo com requisitos técnicos específicos.

Ao mesmo tempo, embora, nesses casos, o tratamento esteja, em princípio, fora do âmbito da Diretiva Proteção de Dados na Aplicação da Lei, o resultado da verificação também pode ser utilizado na correspondência de dados (alfanuméricos) da pessoa com bases de dados das autoridades de aplicação da lei no âmbito do controlo de fronteiras, podendo, por conseguinte, implicar ações com um efeito jurídico significativo para o titular dos dados, por exemplo detenção na sequência de uma indicação no SIS. Em circunstâncias específicas, os dados biométricos também podem ser utilizados para pesquisar correspondências em bases de dados das autoridades de aplicação da lei (neste caso, seria efetuada uma identificação de um para muitos nesta etapa).

O resultado do tratamento da imagem biométrica tem um impacto direto no titular dos dados: este só pode atravessar a fronteira caso a verificação seja bem-sucedida. Caso a identificação não seja bem-sucedida, os guardas de fronteira têm de realizar um segundo controlo para assegurar que o titular dos dados é diferente do descrito no documento de identificação.

Se for identificada uma indicação SIS ou nacional, os guardas de fronteira têm de proceder a uma segunda verificação e aos controlos complementares necessários e, em seguida, tomar as medidas necessárias, por exemplo deter a pessoa ou informar as autoridades competentes.

Fonte da informação:
- Tipos de titulares de dados: ☒ todas as pessoas que atravessam as fronteiras
- Fonte da imagem: ☒ outra (documento de identificação)
- Ligação à criminalidade: ☒ Não é necessária
- Modo de recolha das informações: ☒ numa cabina ou em ambiente controlado
- Contexto – que afete outros direitos fundamentais: Sim, nomeadamente: ☒ direito de livre circulação ☒ direito de asilo

Base de dados de referência (com a qual a informação captada é comparada):
- Especificidade: ☒ bases de dados específicas relacionadas com o controlo das fronteiras

Algoritmo:
- Tipo de verificação: ☒ verificação de um para um (autenticação)

Resultado:
- Impacto ☒ Direto (a entrada ao titular dos dados é permitida ou recusada)
- Decisão automatizada: ☒ Sim

1.2. Quadro jurídico aplicável

Desde 2004, nos termos do Regulamento (CE) n.º 2252/2004 do Conselho[85], os passaportes e outros documentos de viagem emitidos pelos Estados-Membros têm de conter uma imagem facial biométrica armazenada num chip eletrónico incorporado no documento.

O Código das Fronteiras Schengen (CFS)[86] estabelece os requisitos aplicáveis aos controlos de pessoas nas fronteiras externas. Para os cidadãos da UE e outras pessoas que beneficiem do direito de livre circulação ao abrigo do direito da União, os controlos mínimos devem consistir numa verificação dos seus documentos de viagem, se for caso disso utilizando dispositivos técnicos. O CFS foi posteriormente alterado pelo Regulamento (UE) 2017/2225[87], que introduziu, nomeadamente, as definições de «cancelas eletrónicas», «sistema automatizado de controlo nas fronteiras» e «sistema de self-service», bem como a possibilidade de tratamento de dados biométricos para a realização de controlos de fronteira.

Pode, pois, presumir-se a existência de uma base jurídica clara e previsível que autoriza esta forma de tratamento de dados pessoais. Além disso, o quadro jurídico é adotado a nível da União e é diretamente aplicável aos Estados-Membros.

[85] Regulamento (CE) n.º 2252/2004 do Conselho, de 13 de dezembro de 2004, que estabelece normas para os dispositivos de segurança e dados biométricos dos passaportes e documentos de viagem emitidos pelos Estados-Membros.
[86] Regulamento (UE) 2016/399 do Parlamento Europeu e do Conselho, de 9 de março de 2016, que estabelece o código da União relativo ao regime de passagem de pessoas nas fronteiras (Código das Fronteiras Schengen).
[87] Regulamento (UE) 2017/2225 do Parlamento Europeu e do Conselho, de 30 de novembro de 2017, que altera o Regulamento (UE) 2016/399 no que respeita à utilização do Sistema de Entrada/Saída.

1.3. Necessidade e proporcionalidade – finalidade/gravidade do crime

A verificação da identidade dos cidadãos da UE num controlo automatizado nas fronteiras, utilizando a sua imagem biométrica, é um elemento dos controlos fronteiriços nas fronteiras externas da UE. Por conseguinte, está diretamente relacionada com a segurança das fronteiras e serve um objetivo de interesse geral reconhecido pela União. Além disso, as portas com controlo automatizado nas fronteiras ajudam a acelerar o tratamento dos passageiros e reduzem o risco de erros humanos. Além disso, o âmbito, a extensão e a intensidade da ingerência neste cenário são muito mais limitados em comparação com outras formas de reconhecimento facial. No entanto, o tratamento de dados biométricos cria riscos adicionais para os titulares dos dados que têm de ser devidamente abordados e mitigados pela autoridade competente que implementa e opera a TRF.

1.4. Conclusão

A verificação da identidade dos cidadãos da UE no contexto de um controlo automatizado nas fronteiras é uma medida necessária e proporcionada, desde que sejam dadas as garantias adequadas, nomeadamente a aplicação dos princípios da limitação da finalidade, da qualidade dos dados, da transparência e um elevado nível de segurança.

2 CENÁRIO 2

2.1. Descrição

As autoridades de aplicação da lei estabelecem um sistema de identificação das vítimas de rapto de crianças. Um agente de polícia autorizado pode efetuar, em condições estritas, uma comparação dos dados biométricos de uma criança que se suspeite ter sido raptada com uma base de dados de vítimas de rapto de crianças, com o único objetivo de identificar menores que possam corresponder à descrição da criança desaparecida relativamente à qual foi iniciada uma investigação, bem como à indicação emitida.

O tratamento em causa seria a comparação do rosto ou da imagem de um indivíduo, que pode corresponder à descrição de uma criança desaparecida, com as imagens armazenadas na base de dados. Esse tratamento seria efetuado em casos específicos e não de forma sistemática.

A base de dados utilizada para efeitos de comparação está preenchida com imagens de crianças desaparecidas relativamente às quais tenha sido comunicada uma suspeita de rapto ou uma ameaça à vida ou à integridade física da criança e tenha sido iniciada uma investigação criminal sob autoridade judiciária, e em relação às quais tenha sido emitido um alerta de rapto de crianças. Os dados são recolhidos no âmbito dos procedimentos estabelecidos pela autoridade de aplicação da lei competente, ou seja, a polícia judiciária. As categorias de dados pessoais registadas são as seguintes:

- identidade, alcunha, pseudónimo, filiação, nacionalidade, endereços, endereços eletrónicos, números de telefone,
- data e local de nascimento,
- informações de parentesco,
- fotografia com características técnicas que permita a utilização de um dispositivo de reconhecimento facial e outras fotografias.

Os resultados da comparação devem também ser revistos e verificados por um agente autorizado, a fim de corroborar elementos de prova anteriores com o resultado da comparação e excluir eventuais falsos positivos.

As fotografias e os dados pessoais de crianças só podem ser conservados durante a duração da indicação e devem ser apagados imediatamente após o encerramento ou a conclusão do processo penal, em conformidade com os procedimentos nacionais no âmbito dos quais tenham sido inseridos na base de dados.

Embora o período de conservação dos dados biométricos na base de dados possa ser previsto para um período relativamente longo e definido de acordo com a legislação nacional, o exercício dos direitos dos titulares dos dados e, em especial, o direito de retificação e apagamento, prevê uma garantia adicional para limitar a ingerência no direito à proteção dos dados pessoais dos titulares dos dados em causa.

Fonte da informação:

- Tipos de titulares de dados: ☒ Crianças
- Fonte da imagem ☒ outra: não predefinida, suspeita de vítima de rapto de crianças
- Ligação à criminalidade ☒ Temporal indireta ☒ Geográfica indireta
- Modo de recolha das informações: ☒ numa cabina ou em ambiente controlado
- Contexto – que afete outros direitos fundamentais ☒ Sim, nomeadamente: ☒ vários

Base de dados de referência (com a qual a informação captada é comparada):

- Especificidade ☒ base de dados específica

Algoritmo:

- Tipo de verificação: ☒ identificação de um para muitos

Resultado:

- Impacto ☒ Direto
- Decisão automatizada: ☒ NÃO, revisão obrigatória por um agente autorizado

Análise jurídica:

- Quadro jurídico aplicável: ☒ Legislação nacional específica relativa a este tipo de tratamento (reconhecimento facial)

2.2. Quadro jurídico aplicável

A legislação nacional prevê um quadro jurídico específico para a criação da base de dados, a determinação das finalidades do tratamento, bem como os critérios de preenchimento, acesso e utilização da base de dados. As medidas legislativas necessárias à sua aplicação preveem igualmente a determinação de um período de conservação, bem como a referência aos princípios de integridade e de confidencialidade aplicáveis. As medidas legislativas também preveem as modalidades da prestação de informações ao titular dos dados e, neste caso, ao(s) titular(es) da responsabilidade parental, bem como o exercício dos direitos do titular dos dados e a sua eventual limitação, se for caso disso. Durante a redação da proposta da medida legislativa em causa, a autoridade nacional de controlo teve de ser consultada.

2.3. Necessidade e proporcionalidade – finalidade/gravidade do crime/número de pessoas não envolvidas, mas afetadas pelo tratamento

Condições e garantias aplicáveis ao tratamento

A comparação do reconhecimento facial só pode ser efetuada por um agente autorizado como último recurso, a menos que não estejam disponíveis outros meios menos intrusivos e se estritamente

necessário, por exemplo em caso de dúvida sobre a autenticidade do documento de identidade de um menor viajante e/ou após análise de elementos de prova e materiais anteriores recolhidos que indiquem uma possível correspondência com a descrição de uma criança desaparecida relativamente à qual está a ser realizada uma investigação criminal.

É igualmente prevista uma garantia adicional com a revisão e verificação obrigatórias da comparação do reconhecimento facial por um agente autorizado, a fim de corroborar elementos de prova anteriores com o resultado da comparação e excluir eventuais falsos positivos.

Objetivo

A criação da base de dados serve objetivos importantes de interesse público geral, em especial a prevenção, investigação, deteção ou repressão de infrações penais ou a execução de sanções penais e a proteção dos direitos e liberdades de terceiros. A criação da base de dados e o tratamento previsto parecem contribuir para a identificação de crianças vítimas de rapto, pelo que podem ser considerados como uma medida adequada para apoiar o objetivo legítimo de investigar e reprimir este tipo de crime.

Finalidade e preenchimento da base de dados

As finalidades do tratamento estão claramente definidas na lei e a base de dados só deve ser utilizada para identificar crianças desaparecidas relativamente às quais tenha sido comunicada uma suspeita de rapto e tenha sido iniciada uma investigação criminal sob autoridade judiciária, e em relação às quais tenha sido emitido um alerta de rapto de crianças. As condições estabelecidas na lei relativas ao preenchimento da base de dados visam limitar estritamente o número de titulares de dados e de dados pessoais a incluir na base de dados. O titular da responsabilidade parental da criança deve ser informado do tratamento efetuado e das condições de exercício dos direitos da criança em relação ao tratamento biométrico previsto para efeitos de identificação, ou aos dados pessoais da criança armazenados na base de dados.

2.4. Conclusão

Tendo em conta a necessidade e a proporcionalidade do tratamento previsto, bem como o interesse superior da criança na realização desse tratamento de dados pessoais, e desde que existam garantias suficientes para assegurar, nomeadamente, o exercício dos direitos do titular dos dados – nomeadamente tendo em conta o facto de se tratar de dados de crianças, essa aplicação do reconhecimento facial pode provavelmente ser considerada compatível com a legislação da UE.

Além disso, tendo em conta o tipo de tratamento e a tecnologia utilizada, que envolve um elevado risco para os direitos e liberdades do titular dos dados em causa, o CEPD considera que a elaboração de uma proposta de medida legislativa a adotar por um parlamento nacional ou de uma medida regulamentar baseada nessa medida legislativa, que esteja relacionada com o tratamento previsto, deve incluir uma consulta prévia da autoridade de controlo, a fim de assegurar a coerência e o cumprimento do quadro jurídico aplicável (ver artigo 28.º, n.º 2, da Diretiva Proteção de Dados na Aplicação da Lei).

3 CENÁRIO 3

3.1. Descrição

No decurso de intervenções policiais em tumultos e de investigações posteriores, várias pessoas foram identificadas como suspeitas, por exemplo, através de investigações anteriores com recurso a imagens de televisão em circuito fechado (CCTV) ou a testemunhas. As imagens destes suspeitos são

comparadas com imagens de pessoas que foram registadas em CCTV ou em dispositivos móveis num local de crime ou nas áreas circundantes.

A fim de obter provas mais circunstanciadas sobre pessoas suspeitas de terem participado em tumultos no contexto de uma manifestação, a polícia cria uma base de dados constituída por materiais de imagem com uma vaga ligação local e temporal aos tumultos. A base de dados inclui gravações privadas enviadas à polícia pelos cidadãos, material de CCTV dos transportes públicos, material de videovigilância pertencente à polícia e material publicado pelos meios de comunicação social sem qualquer limitação ou proteção específica. A exibição de comportamento criminoso grave não é um pré-requisito para a recolha dos ficheiros na base de dados. Por conseguinte, as pessoas não envolvidas nos tumultos – uma percentagem significativa da população local que passou no local no momento da manifestação, ou que participou na manifestação, mas não nos tumultos – ficam registadas na base de dados. Trata-se de milhares de ficheiros de vídeo e imagens.

Utilizando um *software* de reconhecimento facial, todos os rostos que aparecem nesses ficheiros são atribuídos a identificações faciais únicas. Os rostos de cada suspeito são, em seguida, automaticamente comparados com estas identificações faciais. A base de dados constituída por todos os modelos biométricos nos milhares de ficheiros de vídeo e imagem é armazenada até à conclusão de todas as investigações possíveis. As correspondências positivas são tratadas por agentes responsáveis, que decidem, em seguida, sobre as medidas a tomar. Estas podem incluir a atribuição do ficheiro encontrado na base de dados ao processo penal da pessoa em causa, bem como outras medidas, como o interrogatório ou a detenção dessa pessoa.

Uma lei nacional prevê uma disposição genérica, segundo a qual o tratamento de dados biométricos para efeitos de identificação inequívoca de uma pessoa singular é admissível se for estritamente necessário e sujeito a garantias adequadas relativas aos direitos e liberdades da pessoa em causa.

Fonte da informação:

- Tipos de titulares de dados: ☒ todas as pessoas
- Fonte da imagem: ☒ espaços acessíveis ao público ☒ entidade privada ☒ outros indivíduos ☒ outra: meios de comunicação social
- Ligação à criminalidade: ☒ Ligação geográfica ou temporal não necessariamente direta
- Modo de recolha das informações: ☒ à distância
- Contexto – que afete outros direitos fundamentais: Sim, nomeadamente ☒ liberdade de reunião
- Fontes adicionais de informação disponíveis sobre o titular dos dados: ☒ outras: não excluídas (como a utilização de máquinas ATM ou de lojas visitadas), uma vez que não pode ser exercido qualquer controlo sobre os motivos com base nas imagens

Base de dados de referência (com a qual a informação captada é comparada):

- Especificidade: ☒ bases de dados específicas relacionadas com o local do crime

Algoritmo:

- Tipo de tratamento: ☒ identificação de um para muitos

Resultado:

- Impacto: ☒ Direto (por exemplo, o titular dos dados pode ser detido, interrogado)
- Decisão automatizada: ☒ NÃO
- Duração da conservação: até à conclusão de todas as investigações possíveis

Análise jurídica:

- Tipo de informação prévia ao titular dos dados: ☒ No sítio Web da autoridade de aplicação da lei em geral
- Quadro jurídico aplicável: ☒ Diretiva Proteção de Dados na Aplicação da Lei, maioritariamente transposta para a legislação nacional ☒ Legislação nacional genérica relativa à utilização de dados biométricos pelas autoridades de aplicação da lei

3.2. Quadro jurídico aplicável

Tal como esclarecido acima, os termos das bases jurídicas que se limitam a repetir a cláusula geral do artigo 10.º da Diretiva Proteção de Dados na Aplicação da Lei não são suficientemente claros para proporcionar aos indivíduos uma indicação adequada das condições e das circunstâncias em que as autoridades de aplicação da lei têm o direito de utilizar gravações de CCTV de espaços públicos para criar um modelo biométrico do seu rosto e compará-lo com as bases de dados da polícia, outras gravações CCTV ou privadas disponíveis, etc. O quadro jurídico estabelecido neste cenário não cumpre, por isso, os requisitos mínimos para servir de base jurídica.

3.3. Necessidade e proporcionalidade

Neste exemplo, o tratamento suscita várias preocupações ao abrigo dos princípios da necessidade e da proporcionalidade, por várias razões:

As pessoas não são suspeitas de um crime grave. A exibição de comportamento criminoso grave não é um pré-requisito para a utilização dos ficheiros na base de dados que contenham o material de imagem. Além disso, uma ligação temporal e geográfica direta ao crime não é um pré-requisito para a utilização dos ficheiros na base de dados. Por esta razão, uma percentagem significativa da população local é armazenada numa base de dados biométricos por um período que pode atingir vários anos, até que todas as investigações sejam concluídas.

A base de dados do local do crime não se limita a imagens que satisfaçam os requisitos de proporcionalidade, o que resulta numa quantidade ilimitada de imagens a comparar. Este facto contradiz o princípio da minimização dos dados. Uma quantidade menor de imagens permitiria também colocar a hipótese de utilizar meios não algorítmicos e menos intrusivos, por exemplo, super-reconhecedores[88].

Como o exemplo é retirado das proximidades de uma manifestação, também é provável que as imagens revelem as opiniões políticas dos participantes na manifestação, que seria a segunda categoria de dados especiais possivelmente afetados neste cenário. Neste cenário, não é clara a forma como se poderia evitar a recolha destes dados e com que garantias. Além disso, quando os titulares dos dados tomarem conhecimento de que a sua participação numa manifestação resultou na sua inscrição numa base de dados biométricos da polícia, essa revelação poderá ter sérios efeitos dissuasores no exercício futuro do seu direito de reunião.

Os modelos biométricos na base de dados também podem ser comparados entre si. Esta comparação permite à polícia não só procurar uma pessoa específica em todo o seu material, mas também recriar

[88] Isto é, pessoas com uma capacidade de reconhecimento facial extraordinária. Ver também: *Face Recognition by Metropolitan Police Super-Recognisers* [Reconhecimento facial por super-reconhecedores da polícia metropolitana], 26 de fevereiro de 2016, DOI: 10.1371/journal.pone.0150036, https://pubmed.ncbi.nlm.nih.gov/26918457/.

o padrão de comportamento de uma pessoa ao longo de um período de vários dias. Permite-lhe também recolher informações adicionais sobre as pessoas, nomeadamente os seus contactos sociais e o seu envolvimento político.

A ingerência é ainda mais intensificada pelo facto de os dados serem tratados sem o conhecimento dos respetivos titulares.

Tendo em conta que as pessoas tiram fotografias e gravam vídeos constantemente e que mesmo a cobertura omnipresente da CCTV pode ser analisada biometricamente, tal pode ter graves efeitos dissuasores.

A utilização extensiva de fotografias e vídeos privados, incluindo uma potencial utilização abusiva, como a denúncia, constitui outro motivo de preocupação. Uma vez que uma utilização abusiva, como a denúncia, é um risco também inerente aos processos penais em geral, o risco é consideravelmente maior devido à escalabilidade dos dados tratados e ao número de pessoas envolvidas, uma vez que as pessoas podem também carregar material relativo a uma pessoa específica ou a um grupo de pessoas de quem não gostem. Os pedidos da polícia para que as pessoas carreguem fotografias e vídeos resultam, possivelmente, em limiares muito baixos para as pessoas apresentarem material, especialmente porque têm a possibilidade de o fazer anonimamente ou, pelo menos, sem necessidade de aparecer e identificar-se numa esquadra da polícia.

3.4. Conclusão

Neste exemplo, não existe uma disposição específica que possa servir de base jurídica. No entanto, mesmo que existisse uma base jurídica suficiente, os requisitos de necessidade e proporcionalidade não seriam cumpridos, o que resultaria numa ingerência desproporcionada nos direitos do titular dos dados ao respeito pela vida privada e à proteção dos dados pessoais ao abrigo da Carta.

4 CENÁRIO 4

4.1. Descrição

A polícia implementa uma forma de identificar suspeitos de crimes graves captados em CCTV através de TRF retrospetiva. Um agente seleciona manualmente as imagens dos suspeitos no material de vídeo que foi recolhido no local do crime ou noutro local no âmbito de um inquérito e, em seguida, envia as imagens para o departamento forense. O departamento forense utiliza a TRF para comparar essas imagens com imagens de indivíduos que tenham sido previamente reunidas numa base de dados pela polícia (uma chamada base de dados descritiva composta por suspeitos e ex-reclusos). A base de dados descritiva destina-se a este procedimento – temporariamente e num ambiente isolado – e é analisada com TRF para que seja possível realizar o processo de correspondência. Para minimizar a ingerência nos direitos e interesses das pessoas objeto de correspondência, é concedida autorização a um número muito limitado de trabalhadores do departamento forense para conduzir o procedimento de correspondência efetivo, o acesso aos dados está limitado aos agentes responsáveis pelo dossiê específico em questão e é realizado um controlo manual dos resultados antes de qualquer resultado ser encaminhado ao agente responsável pela investigação. Os dados biométricos não são transmitidos para fora do ambiente isolado e controlado. Apenas o resultado e a imagem (e não o modelo biométrico) voltam a ser utilizados na investigação. Os trabalhadores recebem formação específica sobre as regras e os procedimentos aplicáveis a este tratamento, e todo o tratamento de dados pessoais e biométricos está suficientemente especificado na legislação nacional.

Fonte da informação:

- Tipos de titulares dos dados: ☒ suspeitos identificados a partir das gravações CCTV
- Fonte da imagem: ☒ espaços acessíveis ao público ☒ Internet
- Ligação à criminalidade: ☒ Temporal direta
  ☒ Geográfica direta
- Modo de recolha das informações: ☒ à distância
- Contexto – que afete outros direitos fundamentais: Sim, nomeadamente: ☒ Liberdade de reunião ☒ Liberdade de expressão ☒ vários: __

Base de dados de referência (com a qual a informação captada é comparada):

- Especificidade: ☒ bases de dados específicas relacionadas com o local do crime

Algoritmo:

- Tipo de tratamento: ☒ identificação de um para muitos

Resultado:

- Impacto: ☒ Direto (por exemplo, o titular dos dados é detido, interrogado)
- Decisão automatizada: ☒ NÃO

Análise jurídica:

- Quadro jurídico aplicável: ☒ Legislação nacional específica relativa a este tipo de tratamento (reconhecimento facial) aplicável à autoridade competente em questão

4.2. Quadro jurídico aplicável

Neste cenário, a legislação nacional especifica que os dados biométricos podem ser utilizados na realização de análises forenses quando estritamente necessário para alcançar o objetivo de identificar suspeitos da prática de um crime grave através da correspondência das imagens na base de dados descritiva. A legislação nacional especifica quais os dados que podem ser tratados, bem como os procedimentos para preservar a integridade e a confidencialidade dos dados pessoais e os procedimentos para a sua destruição, concedendo assim garantias suficientes contra o risco de abuso e arbitrariedade.

4.3. Necessidade e proporcionalidade

A utilização do reconhecimento facial é claramente mais eficiente em termos de tempo do que a correspondência manual a nível forense. A seleção manual prévia de imagens limita a ingerência por oposição à comparação de todo o material de vídeo contra uma base de dados e, assim, diferencia e visa apenas as pessoas abrangidas pelo objetivo, ou seja, a luta contra a criminalidade grave. No entanto, continua a ser importante ponderar se a correspondência pode ser efetuada manualmente num período razoável, dependendo do caso em questão. A restrição das pessoas com acesso à tecnologia e aos dados pessoais diminui o impacto sobre os direitos à privacidade e à proteção de dados, bem como o facto de os modelos biométricos não serem conservados ou utilizados posteriormente na investigação. O controlo manual do resultado também significa um risco reduzido de falsos positivos.

4.4. Conclusão

É importante que a legislação nacional proporcione uma base jurídica adequada para o tratamento dos dados biométricos, bem como para a base de dados nacional com base na qual se realiza a correspondência. Neste cenário, foram postas em prática várias medidas para limitar a ingerência nos direitos de proteção de dados, tais como as condições para a utilização da TRF especificadas na base

jurídica, o número de pessoas com acesso à tecnologia e aos dados biométricos, os controlos manuais, etc. A TRF melhora significativamente a eficiência do trabalho de investigação do departamento forense da polícia, baseia-se em legislação que permite à polícia tratar dados biométricos quando absolutamente necessário e, por conseguinte, dentro deste perímetro, pode ser considerada uma ingerência lícita nos direitos do indivíduo.

5 CENÁRIO 5

5.1. Descrição

A identificação biométrica à distância ocorre quando as identidades das pessoas são apuradas com a ajuda de identificadores biométricos (imagem facial, marcha, íris, etc.) à distância, num espaço público e de forma contínua ou permanente, comparando-os com dados (biométricos) conservados numa base de dados[89]. A identificação biométrica à distância é efetuada em tempo real, se a captação do material de imagem, a comparação e a identificação forem efetuadas sem atrasos significativos.

Antes de cada utilização da identificação biométrica à distância em tempo real, a polícia compila uma lista de observação de pessoas de interesse no âmbito de uma investigação. Esta é preenchida com imagens faciais dos indivíduos. Com base em informações que sugerem que os indivíduos estarão numa zona específica, como um centro comercial ou uma praça pública, a polícia decide quando, onde e por quanto tempo deverá utilizar a identificação biométrica à distância.

No dia da ação, é estacionada uma carrinha da polícia no terreno como centro de controlo, com um oficial superior de polícia a bordo. A carrinha contém monitores que exibem imagens de câmaras CCTV localizadas nas proximidades, instaladas quer numa base *ad hoc*, quer através da ligação aos fluxos de vídeo de câmaras já instaladas. Quando os transeuntes passam pelas câmaras, a tecnologia isola as imagens faciais, converte-as num modelo biométrico e compara-as com os modelos biométricos das pessoas que constam da lista de observação.

Se for detetada uma potencial correspondência entre a lista de observação e as pessoas que passam pelas câmaras, é enviado um alerta aos agentes que se encontram na carrinha, que depois avisam os agentes no terreno se o alerta for positivo, por exemplo através de um dispositivo de rádio. O agente no terreno decidirá então se deve intervir, abordar ou, em última análise, deter o indivíduo. As medidas tomadas pelo agente no terreno são registadas. No caso de um controlo discreto, as informações recolhidas (como, por exemplo, com quem está a pessoa, o que traz vestido e para onde se dirige) são armazenadas.

Uma lei nacional prevê uma disposição genérica, segundo a qual o tratamento de dados biométricos para efeitos de identificação inequívoca de uma pessoa singular é admissível se for estritamente necessário e sujeito a garantias adequadas relativas aos direitos e liberdades da pessoa em causa.

Fonte da informação:

- Tipos de titulares de dados: ☒ todas as pessoas
- Fonte da imagem: ☒ espaços acessíveis ao público
- Ligação à criminalidade: ☒ Ligação geográfica ou temporal não necessariamente direta
- Modo de recolha das informações: ☒ à distância
- Contexto – que afete outros direitos fundamentais: Sim, nomeadamente: ☒ Liberdade de reunião ☒ Liberdade de expressão ☒ vários

[89] https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

- Fontes adicionais de informação disponíveis sobre o titular dos dados:
  ☒ outras: não excluídas (como a utilização de máquinas ATM ou as lojas visitadas)

Base de dados de referência (com a qual a informação captada é comparada):

- Especificidade: ☒ bases de dados específicas relacionadas com o local do crime

Algoritmo:

- Tipo de tratamento: ☒ identificação de um para muitos

Resultado:

- Impacto: ☒ Direto (por exemplo, o titular dos dados é detido, interrogado)
- Decisão automatizada: ☒ NÃO
- Duração da conservação: até à conclusão de todas as investigações possíveis

Análise jurídica:

- Tipo de informação prévia ao titular dos dados: ☒ No sítio Web da autoridade de aplicação da lei em geral
- Quadro jurídico aplicável: ☒ Diretiva Proteção de Dados na Aplicação da Lei, maioritariamente transposta para a legislação nacional ☒ Legislação nacional genérica relativa à utilização de dados biométricos pelas autoridades de aplicação da lei

5.2. Quadro jurídico aplicável

Os termos das bases jurídicas que se limitam a repetir a cláusula geral do artigo 10.º da Diretiva Proteção de Dados na Aplicação da Lei não são suficientemente claros para proporcionar aos indivíduos uma indicação adequada das condições e das circunstâncias em que as autoridades de aplicação da lei têm o direito de utilizar gravações de CCTV de espaços públicos para criar um modelo biométrico do seu rosto e compará-lo com as bases de dados da polícia. Por conseguinte, o quadro jurídico estabelecido neste cenário não cumpre os requisitos mínimos para servir de base jurídica[90].

5.3. Necessidade e proporcionalidade

Quanto mais profunda for a ingerência, mais elevada a fasquia em termos de necessidade e proporcionalidade. A identificação biométrica à distância em espaços públicos tem várias implicações em termos de direitos fundamentais:

Os cenários implicam a monitorização de todos os transeuntes no respetivo espaço público. Esta afeta, por isso, gravemente a expectativa razoável das populações de anonimato em espaços públicos[91]. Trata-se de um pré-requisito para muitas facetas do processo democrático, como a decisão de aderir a uma associação cívica, de frequentar reuniões e de encontrar pessoas de todas as origens sociais e culturais, de participar numa manifestação política e de visitar todos os tipos de locais. A noção de anonimato nos espaços públicos é essencial à livre reunião e troca de informações e ideias. Preserva a pluralidade de opiniões, a liberdade de reunião pacífica e a liberdade de associação e a proteção das minorias e apoia os princípios da separação de poderes e do equilíbrio de poderes. O enfraquecimento da noção de anonimato nos espaços públicos pode ter como resultado um grave efeito dissuasor nos

[90] Nos casos em que um projeto científico destinado a investigar a utilização da TRF tenha de proceder ao tratamento de dados pessoais, mas esse tratamento não seja abrangido pelo artigo 4.º, n.º 3, da Diretiva Proteção de Dados na Aplicação da Lei ou pelo direito da União, é aplicável o RGPD. No caso de projetos-piloto que seriam seguidos de operações de aplicação da lei, continuaria a ser aplicável a Diretiva Proteção de Dados na Aplicação da Lei.

[91] Resposta do CEPD a deputados ao Parlamento Europeu a respeito da aplicação de reconhecimento facial desenvolvida pela Clearview AI, 10 de junho de 2020, Ref.: OUT2020-0052.

cidadãos. Pode levá-los a abster-se de certos comportamentos que estão bem dentro dos limites de uma sociedade livre e aberta. Este efeito prejudicaria o interesse público, uma vez que uma sociedade democrática exige a autodeterminação e a participação dos seus cidadãos no processo democrático.

Se este tipo de tecnologia for aplicado, os simples atos de andar na rua, caminhar até ao metro ou ir à padaria na zona afetada levará à recolha de dados pessoais, incluindo dados biométricos, pelas autoridades de aplicação da lei e, no primeiro cenário, também à correspondência com bases de dados da polícia. Uma situação em que o mesmo seria feito através da recolha de impressões digitais seria claramente desproporcionada.

O número de titulares de dados afetados é extremamente elevado, uma vez que todas as pessoas que passam pela zona pública em causa serão afetadas. Além disso, os cenários implicariam um tratamento automatizado em massa de dados biométricos e também uma comparação em massa dos dados biométricos com as bases de dados da polícia.

De acordo com a jurisprudência europeia, a vigilância em massa é proibida (por exemplo, o TEDH, no processo S e Marper c. Reino Unido, considerou a conservação indiscriminada de dados biométricos uma «ingerência desproporcionada» no direito à privacidade, uma vez que não é «necessária numa sociedade democrática»).

A identificação biométrica à distância é tão propensa à vigilância em massa que não existem meios fiáveis de restrição. É essencialmente diferente da videovigilância enquanto tal, uma vez que a possível utilização de imagens de vídeo sem identificação biométrica constitui já uma forte ingerência, mas ao mesmo tempo limitada, ao passo que, se a TRF for aplicada, o sistema de videovigilância, já amplamente difundido como principal fonte de dados, sofrerá uma mudança de qualidade. Além disso, sobretudo no que diz respeito aos efeitos dissuasores implícitos, as eventuais restrições à aplicação das instalações de videovigilância já existentes não serão visíveis e, por conseguinte, não merecerão a confiança do público.

A identificação biométrica à distância pelas autoridades policiais trata toda a gente como um potencial suspeito. No entanto, num Estado de direito, presume-se que os cidadãos são inocentes até prova em contrário. Este princípio está também parcialmente refletido na Diretiva Proteção de Dados na Aplicação da Lei, que sublinha a necessidade de distinguir, na medida do possível, entre o tratamento de pessoas condenadas ou suspeitas de crimes, caso em que as autoridades de aplicação da lei devem ter «motivos fundados para crer que cometeram ou estão prestes a cometer uma infração penal» (artigo 6.º, alínea a)) em comparação com as pessoas que não foram condenadas ou suspeitas de atividades criminosas.

Esta tecnologia, capaz de identificar inequivocamente uma única pessoa e de localizar e analisar o seu paradeiro e movimentos, aplicada pelas autoridades de aplicação da lei a pontos nodais de transporte ou a espaços públicos, revelará até as informações mais sensíveis sobre uma pessoa (inclusive preferências sexuais, religião e problemas de saúde). Implica, pois, o imenso risco de acesso e utilização ilícitos dos dados.

A instalação de um sistema que permita revelar o núcleo essencial do comportamento e das características do indivíduo tem fortes efeitos dissuasores. Faz com que as pessoas questionem se devem aderir a uma determinada manifestação, prejudicando assim o processo democrático. Além disso, o facto de uma pessoa se encontrar e ser vista em público com um determinado amigo conhecido por ter problemas com a polícia ou por ter um comportamento peculiar pode ser considerado crítico, uma vez que atrairia o algoritmo do sistema e, por conseguinte, chamaria a atenção das autoridades.

É impossível proteger titulares de dados vulneráveis como as crianças. Além disso, o sistema afeta pessoas que têm um interesse profissional – e muitas vezes a correspondente obrigação legal – em manter os seus contactos confidenciais, tais como jornalistas, advogados e clérigos. Isto pode, por exemplo, levar à revelação da fonte e do jornalista, ou ao facto de uma pessoa consultar um advogado de defesa penal. O problema não se aplica apenas a locais públicos aleatórios, onde, por exemplo, os jornalistas e as suas fontes se encontram, mas também, naturalmente, a espaços públicos necessários para abordar e aceder a instituições ou profissionais neste domínio.

Além disso, o desconforto das pessoas com a TRF pode levá-las a alterar o seu comportamento, evitando locais onde a TRF está implantada e afastando-se assim da vida social e dos eventos culturais. Dependendo da dimensão da implantação da TRF, o impacto nas pessoas pode ser tão significativo que afete a sua capacidade de viver uma vida digna[92].

Existe, por isso, uma forte probabilidade de afetar o conteúdo essencial – o núcleo intocável – do direito à proteção dos dados pessoais. Os indícios fortes (ver secção 3.1.3.2 das orientações) são, em particular, os seguintes: em grande escala, as características biológicas únicas das pessoas são automaticamente tratadas pelas autoridades de aplicação da lei utilizando algoritmos baseados na plausibilidade com uma capacidade de explicação limitada dos resultados. As limitações aos direitos à privacidade e à proteção de dados são impostas independentemente do comportamento individual da pessoa ou das circunstâncias que lhe dizem respeito. Estatisticamente, quase todos os titulares de dados afetados por esta ingerência são pessoas que cumprem a lei. As possibilidades de prestação de informações ao titular dos dados são limitadas. O recurso judicial, na maioria dos casos, só será possível posteriormente.

A dependência de um sistema baseado na plausibilidade e com uma capacidade de explicação limitada pode conduzir à difusão da responsabilidade e a uma carência em termos de medidas corretivas e pode constituir um incentivo à negligência.

Uma vez aplicado, este sistema, que pode ser aplicado também às câmaras CCTV existentes, com muito pouco esforço e sem ser visível para as pessoas, pode ser utilizado de forma abusiva e permitir a elaboração sistemática e rápida de listas de pessoas de acordo com a sua origem étnica, sexo, religião, etc. O princípio do tratamento de dados pessoais de acordo com critérios pré-estabelecidos, como o paradeiro de uma pessoa e o trajeto percorrido, já é praticado[93] e é suscetível de discriminação.

Em função da sensibilidade, da expressividade e da quantidade de dados tratados, os sistemas de reconhecimento facial à distância em locais acessíveis ao público são propensos a serem utilizados de forma abusiva com efeitos prejudiciais para as pessoas em causa. Esses dados podem também ser facilmente recolhidos e utilizados de forma abusiva para exercer pressão sobre os principais intervenientes no princípio do equilíbrio de poderes, como a oposição política, os agentes da autoridade e os jornalistas.

---

92 https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf, p. 20.

93 Ver o artigo 6.º da Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave e o artigo 33.º do Regulamento (UE) 2018/1240 do Parlamento Europeu e do Conselho, de 12 de setembro de 2018, que cria um Sistema Europeu de Informação e Autorização de Viagem (ETIAS) e altera os Regulamentos (UE) n.º 1077/2011, (UE) n.º 515/2014, (UE) 2016/399, (UE) 2016/1624 e (UE)2017/2226.

Por último, os sistemas TRF tendem a incorporar fortes efeitos de enviesamento em relação à raça e ao género: os falsos positivos afetam desproporcionadamente as pessoas de cor e as mulheres[94], resultando em discriminação. As medidas policiais na sequência de um falso positivo, tais como buscas e detenções, estigmatizam ainda mais estes grupos.

5.4. Conclusão

Os cenários supramencionados relativos ao tratamento à distância de dados biométricos em espaços públicos para fins de identificação não conseguem alcançar um justo equilíbrio entre os interesses privados e públicos concorrentes, constituindo assim uma ingerência desproporcionada nos direitos do titular dos dados nos termos dos artigos 7.º e 8.º da Carta.

6 CENÁRIO 6

6.1. Descrição

Uma entidade privada disponibiliza uma aplicação que efetua «raspagem» de imagens faciais da Internet para criar uma base de dados. O utilizador, por exemplo a polícia, pode depois carregar uma fotografia e, utilizando a identificação biométrica, a aplicação tentará compará-la com as imagens faciais ou modelos biométricos existentes na sua base de dados.

Um departamento de polícia local está a investigar um crime captado em vídeo em que não é possível identificar várias potenciais testemunhas e suspeitos através da correspondência das informações recolhidas com quaisquer bases de dados ou informações internas. Com base nas informações recolhidas, os indivíduos não estão registados em nenhuma base de dados da polícia existente. A polícia decide utilizar uma ferramenta como a descrita acima, que é disponibilizada por uma empresa privada, para identificar as pessoas através de identificação biométrica.

Fonte da informação:

- Tipos de titulares dos dados: ☒ todos os cidadãos (testemunhas) ☒ reclusos ☒ suspeitos
- Fonte da imagem: ☒ Gravação de vídeo de um espaço público ou recolhida noutro local, no âmbito de um inquérito
- Ligação à criminalidade: ☒ Não é necessária
- Modo de recolha das informações: ☒ à distância
- Contexto – que afete outros direitos fundamentais: Sim, nomeadamente: ☒ Liberdade de reunião ☒ Liberdade de expressão ☒ vários: __

Base de dados de referência (com a qual a informação captada é comparada):

- Especificidade: ☒ bases de dados de caráter geral preenchidas a partir da Internet

Algoritmo:

- Tipo de tratamento: ☒ identificação de um para muitos

Resultado:

- Impacto ☒ Direto (por exemplo, o titular dos dados é detido, interrogado, comportamento discriminatório)
- Decisão automatizada: ☒ NÃO

[94] https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

Análise jurídica:

- Tipo de informação prévia ao titular dos dados: ☒ Não

6.2. Quadro jurídico aplicável

Quando uma entidade privada presta um serviço que inclui o tratamento de dados pessoais, para o qual determina a finalidade e os meios (neste caso, a raspagem de imagens da Internet para criar uma base de dados), essa entidade privada tem de ter uma base jurídica para esse tratamento. Além disso, a autoridade de aplicação da lei que decide utilizar esse serviço para os seus fins deve dispor de uma base jurídica para o tratamento, cujas finalidades e meios determina. Para que a autoridade de aplicação da lei possa proceder ao tratamento de dados biométricos, tem de existir um quadro jurídico que especifique o objetivo, os dados pessoais a tratar, as finalidades do tratamento e os procedimentos para preservar a integridade e a confidencialidade dos dados pessoais, bem como os procedimentos para a sua destruição.

Este cenário implica a recolha de dados pessoais em massa de pessoas singulares que não têm conhecimento de que os seus dados estão a ser recolhidos. Esse tratamento só poderia ser lícito em circunstâncias muito excecionais. Dependendo da localização da base de dados, a utilização desse serviço pode implicar a transferência de dados pessoais e/ou de categorias especiais de dados pessoais para fora da União Europeia (pela polícia, por exemplo, «enviando» a imagem facial no vídeo de vigilância ou recolhida de outra forma), exigindo assim condições específicas para essa transferência, ver artigo 39.º da Diretiva Proteção de Dados na Aplicação da Lei.

Não existem regras específicas neste cenário que permitam este tratamento pela autoridade de aplicação da lei.

6.3. Necessidade e proporcionalidade

A utilização do serviço pela autoridade de aplicação da lei implica a partilha dos dados pessoais com uma entidade privada que utiliza uma base de dados em que os dados pessoais são recolhidos de forma ilimitada e em massa. Não existe qualquer relação entre os dados pessoais recolhidos e o objetivo da autoridade de aplicação da lei. A partilha de dados entre a autoridade de aplicação da lei e a entidade privada implica também uma falta de controlo por parte da autoridade sobre os dados que estão a ser tratados pela entidade privada e uma grande dificuldade dos titulares dos dados em exercerem os seus direitos, uma vez que não estarão cientes de que os seus dados estão a ser tratados desta forma. Esta situação estabelece uma fasquia muito elevada para situações em que este tipo de tratamento poderia sequer ter lugar. É questionável se qualquer objetivo cumpriria os requisitos estabelecidos na diretiva, uma vez que quaisquer derrogações e limitações aos direitos à privacidade e à proteção de dados só são aplicáveis quando estritamente necessário. O interesse geral da eficácia na luta contra os crimes graves não pode, por si só, justificar o tratamento de dados quando se trata da recolha indiscriminada de quantidades tão grandes de dados. Por conseguinte, este tratamento não cumpriria os requisitos de necessidade e proporcionalidade.

6.4. Conclusão

A ausência de regras claras, precisas e previsíveis que cumpram os requisitos dos artigos 4.º e 10.º da diretiva, bem como a falta de provas de que este tratamento é estritamente necessário para alcançar os objetivos pretendidos, levam a concluir que a utilização desta aplicação não cumpriria os requisitos de necessidade e proporcionalidade e implicaria uma ingerência desproporcionada nos direitos dos titulares dos dados ao respeito pela vida privada e à proteção dos dados pessoais ao abrigo da Carta.