



Valter Dione Faria Freitas

**Da posição do imigrante face à dimensão tecnológica dos sistemas  
de controlo das fronteiras da UE: O caso do iBorderCtrl**

Dissertação com vista à obtenção de grau de Mestre  
em Direito na especialidade de Direito e Segurança

Orientador/a:

Doutora Sofia Santos, Professora da Faculdade de Direito da Universidade Nova de  
Lisboa

Novembro, 2020

## **Declaração de Compromisso Anti-Plágio**

Declaro por minha honra que o trabalho que apresento é original e que todas as minhas citações estão corretamente identificadas. Tenho consciência de que a utilização de elementos alheios não identificados constitui uma grave falta de ética e disciplinar.

Lisboa, 2020

Valter Freitas  
  
24/11/2020

## **Declaração de conformidade**

A presente dissertação comporta um total de 199.668 caracteres (corpo e notas de rodapé), ou um total de 170.335 caracteres completa, cumprindo o estipulado no n.º 4 do artigo 7º do Regulamento do Segundo Ciclo de Estudos conducente ao Grau de Mestre em Direito e Segurança (Regulamento nº 402/2016, publicado no Diário da República, 2ª série - nº 80 - 26 de abril de 2016)

## Dedicatória

*À minha acompanhante  
pela compreensão e amor,  
aos meus tios, aos meus avós, meus sogros  
pela motivação e apoio nos momentos difíceis.*

## **Agradecimentos**

Ao longo deste percurso trilhado, importa refletir sobre o mesmo e agradecer a todos/as que me ajudaram a chegar até aqui, começando por dirigir à Professora Doutora Sofia Santos a minha palavra de agradecimento por ter aceite orientar esta dissertação e apoiar-me no rumo dado a este trabalho.

Este trabalho é o culminar deste percurso trilhado, após a aprendizagem obtida na parte curricular com especialistas nas áreas da segurança, no despertar do interesse a temáticas com muita pertinência na área da Segurança. Os interesses destas temáticas fizeram querer aprofundar mais na Segurança, investindo no estudo da cibersegurança como área inevitável nos estudos da Segurança.

Um agradecimento geral a todos os professores do curso, aos colegas do curso pela disponibilidade constante de apoiar sempre quando necessário, à minha família, aos meus amigos pelo apoio, aos meus irmãos e à minha acompanhante pela compreensão neste isolamento reflexivo e a motivação contínua.

## Lista de siglas, abreviaturas e acrónimos

ABC	-	Controlo Automatizado de Fronteiras
AEPD	-	Autoridade Europeia de Proteção de Dados
CEDH	-	Convenção Europeia dos Direitos Humanos
CDFUE	-	Carta dos Direitos Fundamentais da UE
CFS	-	Código das Fronteiras Schengen
FRA	-	Agência dos Direitos Fundamentais da União Europeia
cfr.	-	confira, confronte
DUDH	-	Declaração Universal dos Direitos Humanos
EES	-	Sistema de Entrada/Saída
EMSA	-	Agência Europeia de Segurança Marítima
ETIAS	-	Sistema Europeu de Informação e Autorização de Viagem
ed., eds.	-	edição, edições; editora, editoras
<i>e. g.</i>	-	exempli gratia (por exemplo)
<i>[et al.]</i>	-	[et al.]ii (e outros)
FRONTEX	-	Agência Europeia da Guarda de Fronteiras e Costeira
<i>i. e.</i>	-	id est (isto é)
n.	-	nota
n.º, n.ºs	-	número, números
n. m., ns. ms.	-	número marginal, números marginais
org.	-	organizador, organização
p., pp.	-	página, páginas
reimp.	-	reimpressão
rev.	-	revisão, revista
RGPD	-	Regulamento Geral de Proteção de Dados
s., ss.	-	seguinte, seguintes
séc.	-	século
SIS	-	Sistemas de Informação Schengen
t., ts.	-	tomo, tomos
trad.	-	tradução (de), traduzido (por)
TFUE	-	Tratado sobre o Funcionamento da União Europeia
TIC	-	Tecnologias da Informação e Comunicação
TUE	-	Tratado da União Europeia
<i>v. g.</i>	-	verbi gratia (por exemplo)
vol., vols.	-	volume, volumes
UE	-	União Europeia
VIS	-	Sistema de Informação sobre Vistos

## **Resumo**

Neste mundo digital, estamos dependentes das tecnologias da informação e comunicação, estas presentes nos diversos equipamentos móveis do nosso quotidiano. A sua presença, por um lado, auxilia o Estado na prossecução dos demais direitos tutelados previamente por este, por outro lado, estende para uma nova geração de direitos a serem salvaguardados deste indivíduo digital. Por conseguinte, as tecnologias são relevantes para o Estado contemporâneo, em particular no caso das imigrações, face à reconhecida vulnerabilidade da posição do imigrante, bem como o uso das tecnologias para o controlo dos fluxos migratórios na tutela dos direitos fundamentais deste sujeito de direito internacional.

Desta feita, as tecnologias adotadas no espaço da União para o controlo fronteiriço devem cumprir o respeito pelos direitos fundamentais no desenho dos sistemas de informação para o controlo fronteiriço, sob prejuízo de prejudicar a posição do imigrante. Em contraste, esta proliferação dos sistemas de informação assumem o intuito do controlo fronteiriço dos fluxos migratórios nas dimensões da securitização, privatização e externalização com a recolha de dados do migrante para tomada de decisões para a gestão dos fluxos migratórios.

Concomitantemente, verificamos o uso de sistemas de controlo fronteiriço automatizado, os quais contemplem vários módulos que permitem recolher vários dados no auxílio da tomada de decisão automatizada, colocando certas indagações em termos dos direitos fundamentais estritamente tecnológicos do imigrante. Por fim, ao considerarmos os módulos do sistema iBorderCtrl, compreende-se a recolha de dados de saúde (e.g. biométricos), dados relativos à definição de perfis (i.e. interoperabilidade com as restantes bases de dados), dados não visuais (i.e. através do detetor de mentiras) entre outros módulos, assentes em modelos de inteligência artificial.

## **Palavras-chave:**

Imigrante, Sistemas de informação da UE, iBorderCtrl, Direitos Fundamentais

## **Abstract**

In this digital world, with our mobile devices within our daily lives. These technologies, on the one hand, assist the State to pursue rights previously protected by him. On the other hand, it disseminates other rights needed to be safeguarded from this new generation the digital individual. In fact, technologies must be considered within the scope of the State's tutelage, particularly in the case of migration.

Simultaneously, the individual's fundamental rights are increasingly recognized, which must be considered into the design of EU information systems for border control, without prejudice or damage the migrant's position. Therefore, we have seen an increase on the use of technological tools for processing data for border control of migratory flows, based on the dimensions of securitization, privatization, and externalization. We will try to understand the immigrant's position in relation to these technologies, particularly in the case of the iBorderCtrl project.

Finally, this project is relevant to consider in the light of the migrant's strictly technological fundamental rights, as it contains components that may threaten migrant's fundamental rights. In particular, considering the use of modules for obtaining health data (e.g. biometric), data related to the definition of profiles (i.e. interoperability with the other databases), lie detection, among other modules, through advanced technologies of neural networks (i.e. deep learning).

## **Keywords:**

Migrant, EU Information System, iBorderCtrl, Fundamental Rights

## Índice

Declaração de Compromisso Anti-Plágio.....	i
Declaração de conformidade .....	ii
Dedicatória.....	iii
Agradecimentos .....	iv
Lista de siglas, abreviaturas e acrónimos.....	v
Resumo .....	vi
Abstract .....	vii
Introdução .....	1
Capítulo I   Breve enquadramento do controlo dos fluxos migratórios na sociedade tecnológica da UE.....	4
1. O fenómeno migratório e a sociedade tecnológica.....	4
1.1. Dados .....	9
1.2. Algoritmos .....	12
1.3. Machine learning e deep learning.....	15
2. Direitos fundamentais dos imigrantes na UE .....	18
2.1. Direitos face às tecnologias .....	19
2.2. Direitos de cariz tecnológico. ....	21
2.3. Direitos face a decisões automatizadas e definição de perfis .....	25
Capítulo II   Sistemas de Informação no controlo dos fluxos migratórios na UE .....	27
1. Enquadramento jurídico do controlo dos fluxos migratórios na UE .....	27
2. As tipologias do controlo dos fluxos migratórios na UE.....	31
2.1. Securitização .....	35
2.2. Privatização.....	37
2.3. Externalização.....	38
3. Sistemas de informação da UE .....	43

Capítulo III   O caso do iBorderCtrl .....	53
1. O Controlo Fronteiriço Automático: o projeto iBorderCtrl.....	53
1.1. Reconhecimento biométrico .....	61
1.2. Ferramenta de reconhecimento facial .....	63
1.3. Ferramenta de avaliação da autenticidade do documento .....	64
1.4. Ferramenta de deteção de humanos ocultos.....	65
1.5. Sistema externo de legado e interface social .....	66
1.6. Ferramenta de análise integrada de controlo fronteiriço .....	66
1.7. Ferramenta baseada na avaliação de risco .....	67
1.8. Sistema de deteção automática de mentiras.....	68
2. Proteção dos direitos dos imigrantes?.....	71
Considerações finais .....	76
Bibliografia .....	80

## **Introdução**

A presente dissertação surge como requisito para a obtenção do grau de mestre em Direito e Segurança pela FDUNL – Faculdade de Direito da Universidade Nova de Lisboa, focando na dimensão securitária do controlo dos fluxos migratórios pela União Europeia via ferramentas tecnológicas presentes nos sistemas informação da UE.

Esta é uma área com interesse desenvolvido na área académica dos Estudos Europeus, com a abordagem sociológica sobre o fenómeno das imigrações, levando a remontar esse conhecimento e, por sua vez, observá-lo com a aprendizagem neste mestrado de Direito e Segurança, a dimensão da securitização das migrações. Neste caso particular, através do uso dos sistemas de informação da União Europeia para o controlo dos fluxos migratórios.

Por outro lado, a fusão com a área da cibersegurança prende-se com o rumo profissional tido nos últimos tempos, bem como o investimento académico nesta área tão relevante das relações internacionais. A relevância desta análise parte da conjugação dos elementos técnicos e jurídicos dos sistemas de informação da União, em particular do projeto do iBorderCtrl, assumindo a abordagem do direito à proteção de dados como meta-direito para a prossecução dos demais direitos do imigrante. Ainda, cumpre referir que outro dos aspetos inovadores parte da teórica dos sistemas de controlo fronteiriço automatizado, detalhando algumas vulnerabilidades que poderão prejudicar o interesse deste sujeito de direito internacional.

Paralelamente, estes assuntos estão cada vez mais prementes, principalmente quando falamos na nova geração de direitos fundamentais ligados com a tecnologia, onde esta assume um papel preponderante na sociedade tecnológica com a melhoria do bem-estar, contudo, também acarreta certos desafios que devem ser considerados. Por conseguinte, esses desafios são colocados aos indivíduos principalmente com a constante complexificação da tecnologia, bem como o uso destas na ação operacional nos serviços de fronteira.

Para o presente estudo, o tema escolhido, *Da posição do imigrante face à dimensão tecnológica dos sistemas de controlo das fronteiras da UE: Caso do*

*iBorderCtrl*, delimita o foco neste sistema de informação, reconhecendo a sua integração nos sistemas interoperáveis da União. Isso não prejudica a análise do enquadramento dos sistemas de informação da UE, conjuntamente com a posição do imigrante nesta articulação complexa.

Neste sentido, a tónica deverá recair sobre as tecnologias usadas neste sistema de informação, analisá-la à luz dos direitos subjacentes aos imigrantes, quando tipicamente a tónica recai sobre as formas como as tecnologias podem melhorar o controlo dos fluxos migratórios. Após delineado o foco, será relevante considerar um conjunto de questões que pretendemos responder para alcançar os objetivos desta investigação. Desta feita, impõe-se a indagar:

*(P1) Será que a posição dos imigrantes face às tecnologias de controlo dos fluxos migratórios tem vindo a ser acompanhada por medidas adequadas de segurança e privacidade, em particular nos sistemas de informação da UE, nomeadamente no projeto iBorderCtrl?*

Para entendermos a dimensão desta questão, devemos compreender se, a posição dos migrantes deve ser considerada no âmbito das migrações, em particular os direitos fundamentais, compreender se a sociedade tecnológica tem impacto nas migrações, nomeadamente nas deslocações convencionais, na tomada de decisões automatizadas e, se esse impacto das novas tecnologias tem sido considerado para minimizar o potencial intrusivo das mesmas.

Estas medidas de segurança, partiram da análise dos componentes do sistema de informação no sentido amplo, enquadrá-lo no enquadramento dos controlos fronteiriços automatizados e, conjuntamente, analisar a dimensão técnica para retirar as implicações relativos à privacidade e cibersegurança.

A metodologia optada será a investigação qualitativa, recorrendo ao método indutivo. Para o propósito a que o trabalho se propõe, acompanhar-se-á de recolha de dados provenientes da análise documental de diplomas europeus e jurisprudência europeia, juntamente com uma reflexão da dimensão tecnológica dos sistemas de

informação da UE no controlo dos fluxos migratórios, face à posição do imigrante a essas tecnologias.

Para analisarmos a proporcionalidade das medidas com carácter restritivo dos direitos fundamentais relativos à privacidade e à proteção de dados pessoais, seguiremos a metodologia de análise recomendada pela Agência Europeia para a Proteção de Dados (2019) no teste da proporcionalidade das medidas, seguindo as fases de análise delineadas por esta mesma agência da União, avaliando a legitimidade, a essência, o interesse público e a proporcionalidade e, por fim, analisar as conclusões.

Pelas particularidades em estudo, repartimos em três capítulos. No primeiro capítulo, intitulado por *Breve enquadramento do controlo dos fluxos migratórios na sociedade tecnológica da UE*, procuraremos compreender os fluxos migratórios enquadrados na sociedade tecnológica, as tendências desta, em particular os dados, os algoritmos e a inteligência artificial. O efeito destas tendências no controlo dos fluxos migratórios, reconhecendo os direitos a serem salvaguardados pelos Estados-Membros da União.

No segundo capítulo, intitulado por *Sistemas de Informação no controlo dos fluxos migratórios na UE*, abordaremos a literatura relativa às migrações, enquadrando-as no espaço da União Europeia, os obstáculos que os imigrantes enfrentam no enquadramento europeu, demarcando as tipologias de controlo que persistem neste controlo (i.e. Securitização, Privatização e Externalização), sendo a dimensão tecnológica transversal às tipologias. Em adição, procederemos à análise dos sistemas de informação da União Europeia no controlo fronteiriço (e.g. aéreo e terreno), bem como no controlo marítimo, atendendo à recolha de dados considerável pelos variados sistemas de informação.

No terceiro capítulo, intitulado por *Posição do imigrante face aos sistemas de informação da UE: Caso do iBorderCtrl*, compreenderemos os tipos de controlo fronteiriços automáticos, as tendências dos mesmos controlos conjugado com iniciativas à escala da União de projetos deste tipo, a infraestrutura do sistema iBorderCtrl e os diversos módulos e, por fim, ponderar com a análise dos direitos fundamentais do

imigrante seguindo a metodologia de análise recomendada pela Agência Europeia para a Proteção de Dados (2019) no teste da proporcionalidade.

# Capítulo I | Breve enquadramento do controlo dos fluxos migratórios<sup>1</sup> na sociedade tecnológica da UE

## 1. O fenómeno migratório e a sociedade tecnológica

As imigrações<sup>2</sup> são um velho fenómeno que acompanham a evolução histórica humana, desde os primeiros nómadas onde procuravam outros espaços geográficos para sobreviver, até às migrações contemporâneas em que o indivíduo migra para outros territórios, não somente com intuito de sobrevivência, bem como na procura de melhorar a sua qualidade de vida.

Nesta fase contemporânea das migrações, assistimos à progressiva mutação da posição do migrante, principalmente após a 2<sup>a</sup> metade do século XX, onde o foco nos direitos da pessoa humana tem sido constante, reconhecendo-a como sujeito de direito internacional<sup>3</sup>. Nesta potencial ordem cosmopolita de cariz kantiana<sup>4</sup>, o reconhecimento

---

<sup>1</sup> Para a compreensão deste controlo, o mesmo deve ser repartido na dimensão do controlo das fronteiras internas, na aceção do n.º 1 do artigo 2.º do Código das Fronteiras Schengen (Regulamento (UE) 2016/399, com posteriores alterações), bem como as fronteiras externas, na aceção do n.º 2 do artigo 2.º do CFS

<sup>2</sup> Não existe uma definição vinculativa de imigrantes internacional, mas podemos definir, seguindo a IOM (2020): “...international migrant is someone who changes his or her country of usual residence, irrespective of the reason for migration or legal status. Generally, a distinction is made between short-term or temporary migration, covering movements with a duration between three and 12 months, and long-term or permanent migration, referring to a change of country of residence for a duration of one year or more.” Cfr. a hiperligação <https://www.iom.int/key-migration-terms>, consultado em outubro de 2020. Por outro lado, podemos recorrer a Gil, (2017, p. 218) que define como “a pessoa que deixa o país da nacionalidade ou a residência habitual (no caso dos apátridas) e que procura entrar ou permanecer num país terceiro como fim de aí residir”.

<sup>3</sup> É relativamente a esta posição que a Declaração Universal dos Direitos Humanos no seu artigo 1.º apela a que todos os seres humanos nascem livres e iguais em dignidade e em direitos, sendo esta posição reforçada pelo artigo 2.º, no qual refere que “*Todos os seres humanos podem invocar os direitos e as liberdades proclamados na presente Declaração, sem distinção alguma, nomeadamente de raça, de cor, de sexo, de língua, de religião, de opinião política ou outra, de origem nacional ou social, de fortuna, de nascimento ou de qualquer outra situação. Além disso, não será feita nenhuma distinção fundada no estatuto político, jurídico ou internacional do país ou do território da naturalidade da pessoa, seja esse país ou território independente, sob tutela, autónomo ou sujeito a alguma limitação de soberania.*”. Conjuntamente, existem outros instrumentos de Direito Internacional que consagraram essa tutela dos direitos da pessoa humana, tomando como exemplificativo o Pacto Internacional sobre Direitos Civis e Políticos (PIDCP) no seu artigo 2.º, no Pacto Internacional sobre Direitos Económicos, Sociais e Culturais, na Convenção Internacional sobre Eliminação de Todas as Formas de Discriminação Racial, a Convenção sobre a Eliminação de Todas as Formas de Discriminação contra as Mulheres, a Convenção sobre os Direitos da Criança, entre outros instrumentos.

<sup>4</sup> É indiscutivelmente uma mutação tremenda nas relações internacionais, onde a pessoa humana é colocada gradualmente no centro das preocupações do Estado, principalmente após a Segunda Guerra Mundial, assente na emergência do instituto internacional dos Direitos Humanos vincular os Estados nas ações destes perante os indivíduos. Cfr. Coutinho, 2017, pp. 109 e ss.; Cfr. Gouveia, 2015a, pp. 16 e ss.; para a compreensão da dimensão filosófica do *ius cosmopolitanum*, no âmbito do projeto contratualista da Paz Perpétua, Cfr. Kant, 1995, p. 20 e ss.; no que concerne a dimensão da Segurança Humana, recomendamos Cfr. Gouveia, 2015b, pp. 418 e ss.

culmina com a existência de mecanismos de proteção diplomática, de proteção humanitária e da proteção específica dos refugiados e asilados<sup>5</sup>.

Estes mecanismos, em parte, dependem da prossecução dos Estados, tomando o mecanismo da proteção diplomática na ótica de uma intervenção mediata do Estado, contudo os mecanismos relativos à proteção humanitária e a proteção dos refugiados e asilados devem ser garantidos na ótica da intervenção imediata assente na proteção humana, principalmente com a emergência dos direitos humanos.

Simultaneamente, a Comunidade Internacional tem gradualmente comprometendo-se com a proteção dos imigrantes através de instrumentos de proteção internacional dos direitos humanos, reforçando a prerrogativa do direito à mobilidade, no princípio da universalidade, no princípio da proibição da discriminação reiterados nos instrumentos jurídicos europeus e internacionais<sup>6</sup>, entre outros. Esta proteção facilitou o aumento dos fluxos migratórios no cenário internacional, desde a experiência da Guerra até os dias de hoje<sup>7</sup>, bem como as tecnologias previamente mencionadas.

Durante várias décadas, a tendência era da abertura das fronteiras dos diversos Estados à entrada de imigrantes necessárias para a reconstrução da Europa após os destroços da Segunda Guerra Mundial (1945). Por um lado, esta entrada resultou da falta de pessoas para apoiar neste processo de reconstrução na qualidade de mão-de-obra<sup>8</sup>,

---

<sup>5</sup> Para um entendimento acrescido do reconhecimento da pessoa humana no espectro internacional, recomendamos a leitura evolutiva, Cfr. Gouveia, 2018, pp. 970 e ss.

<sup>6</sup> Sem prejuízo da crescente judicialização de instâncias internacionais para violações de direitos fundamentais, tomando o Tribunal Europeu dos Direitos Humanos como exemplar, bem como a prática de crimes sancionada internacionalmente, nomeadamente pelo Tribunal Penal Internacional. Para uma visão evolutiva da judicialização, Cfr. Gouveia, 2015a, pp. 97-156; Cfr. Pina Delgado e Tiujo Delgado, 2015, pp. 472-476

<sup>7</sup> No panorama atual, assiste-se a um aumento exponencial das movimentações dos imigrantes, e, por conseguinte, a população imigrantes nos distintos países de residência aumentou, quer no seu número absoluto (102 milhões em 1980 para 258 milhões em 2017), quer no peso (2,3% em 1980 e 3,3% em 2017) que esta assume em relação à população mundial. Não menosprezando a dimensão das migrações internas, sendo que atingem os 763 milhões em 2013. (IOM, 2018, p.20).

<sup>8</sup> Cfr. Gil, 2018, pp. 207-222

optando assim pelo modelo de Guest Worker<sup>9</sup> e, por outro lado, estes fluxos foram facilitados pelo incremento da infraestrutura dedicada ao fenómeno migratório<sup>10</sup>.

Este período de abertura das fronteiras cessa cerca 30 após, face ao período de instabilidade vivenciado na sequência da crise petrolífera de 1973<sup>11</sup>. Por conseguinte, verificou-se o isolamento de determinados Estados, robustecendo a dimensão securitização através de mecanismos de repatriação, e, posteriormente será articulado com a dimensão da privatização e, por fim, a dimensão da externalização da responsabilidade neste controlo<sup>12</sup>, como teremos oportunidade de mencionar posteriormente.

Concomitantemente, estes fluxos migratórios não parecem ter diluído a soberania do Estado, em matéria de *ius includendi*<sup>13</sup>, ou seja, o poder de reger o regime de entradas<sup>14</sup> de imigrantes, ainda, o *ius excluendi*, ou seja, o poder de excluir/expulsar os imigrantes. Estes poderes são amplamente limitados na esfera internacional pela constante tutela internacional da pessoa humana, restringindo a discricionariedade da soberania dos Estados. Como tal, reparamos no direito europeu, em particular no Tratado de Lisboa, a vinculação dos Estados no respeito aos direitos e princípios de direito internacional, em particular<sup>15</sup>, o estipulado na Carta dos Direitos Fundamentais

---

<sup>9</sup> Este modelo instrumentaliza a necessidade sentida com a falta de mão-de-obra, optando por esquemas para atrair imigrantes, com condições de trabalho pouco favoráveis, tendo findando alguns dos esquemas após a crise petrolífera começando alguns dos movimentos securitários face às migrações, tal como a repatriação e restrição de entrada de imigrantes, bem como movimentos defensores com emanação nas diversas Constituições, Cfr. Heckmann, *et al*, 2009, pp. 1-10; Cfr. Gil, 2018, pp. 209-210.

<sup>10</sup> Conforme nos aponta Spijkerboer, (2018, p. 455), as estruturas físicas (e.g. portos, aeroportos, hotéis, restaurantes, entre outros), bem como os diversos serviços (e.g. agências de viagens, intermediários de vistos, entre outros) e, por fim a liberalização dos transportes internacionais, principalmente no mercado de aviação, servem como alicerces para o aumento destes fluxos sentidos no século XX.

<sup>11</sup> Cfr. Nota 6

<sup>12</sup> Cfr. Spijkerboer, T., 2018, p. 453

<sup>13</sup> Para reforçar esta tendência dos Estados na União exercerem o exercício do *ius includendi*, como pode ser observado no Ac. de 27/06/2006, *Parlamento Europeu c., Conselho, proc, n<sup>a</sup> C – 540/03*, Cfr. Gil, 2016, pp. 100 e ss. Tal não prejudica a definição de condições para subsequente admissão e residência, harmonização dos direitos dos nacionais de países terceiros, matérias relativas à migração ilegal, o combate ao tráfico de seres humanos, conforme mencionado no n.º 2 do artigo 79.º do TFUE

<sup>14</sup> Conforme menciona Palm (2020, p. 14): “*Migration control is typically seen as a natural part of legitimate nation states’ exercise of sovereign power. (...) Sovereignty has to do with jurisdiction over territory and boundaries of the nation state and the right to make laws, including the right to decide who is a citizen and who enters the country.*”

<sup>15</sup> Cfr. Valente, *et al*, 2016, pp. 46

da União Europeia (CDFUE)<sup>16</sup>, bem como à Convenção Europeia dos Direitos Humanos (CEDH)<sup>17</sup>, sem prejuízo do respeito dos direitos consagrados na Carta das Nações Unidas<sup>18</sup>, tomando como exemplificativo:

- I. Limitação da discricionariedade da entrada de imigrantes<sup>19</sup>
- II. Limitação das medidas de detenção<sup>20</sup>
- III. Limitação da expulsão de imigrantes<sup>21</sup>
- IV. Limitação da expulsão coletiva<sup>22</sup>

Nesta sociedade contemporânea, marcada pela tecnologia, a doutrina tem vindo a falar de novas dimensões do uso da tecnologia, em particular o *data-driven humanitarianism*, ou seja, o uso de ferramentas de análise de dados para prever movimentos das populações durante e após situações de conflito (Molnar, 2019, pp. 7-9). Por outro lado, também se verifica o uso dos algoritmos na tomada de decisões como a detenção, a deportação ou retorno, bem como o uso de detetores de mentiras para atribuir uma pontuação de risco ao imigrante relativo à possibilidade de tornar-se irregular.

Nesta sociedade hodierna, é evidente a constante informatização na vida dos indivíduos, através da integração do seu uso nas tarefas diárias das tecnologias da informação e comunicação (TIC). Essas tecnologias estão presentes em diversos dispositivos eletrónicos (e.g. telemóvel, tablet, computadores), potenciadores da comunicação, do acesso à informação, da liberdade de expressão e, em certa medida, diluindo as fronteiras da comunicação entre os Estados.

---

<sup>16</sup> Cfr. o n.º 1 do artigo 51.º da Carta dos Direitos Fundamentais da União Europeia (doravante CDFUE) com leitura conjunta do n.º 1 do artigo 6.º do Tratado da União Europeia (TUE)

<sup>17</sup> Cfr. o n.º 2 do artigo 6.º do TUE

<sup>18</sup> Cfr. o n.º 1 e 2 do artigo 21.º do TUE relativo ao respeito dos princípios da Carta na ação externa da União.

<sup>19</sup> Nos termos do n.º 4 do artigo 12.º do PIDCP, o qual se aplica às partes contratantes, há uma proibição da discricionariedade na entrada dos imigrantes no seu país de origem.

<sup>20</sup> Já desenvolvida pela jurisprudência do Tribunal Europeu dos Direitos Humanos (TEDH), só pode ser usada como medida de *ultima ratio*, segundo o artigo 9.º da DUDH e o PIDCP, com garantias de condições condignas, nos termos do artigo 10.º

<sup>21</sup> Esta é limitada pelo princípio do *non-refoulement*, previsto no artigo 33.º da Convenção de Genebra de 1951, ampliando ao elenco do artigo 3.º da Convenção Europeia dos Direitos do Homem (CEDH). Ainda, pelo princípio do interesse superior da criança, previsto no artigo 3.º da Convenção sobre os Direitos da Criança (CDC).

<sup>22</sup> Principalmente o artigo 22.º da Convenção Internacional sobre a Proteção dos Direitos de Todos os Trabalhadores Imigrantes e dos Membros das suas famílias.

Por um lado, estas tecnologias permitem facilitar as deslocações dos indivíduos entre os Estados<sup>23</sup> nesta sociedade tecnológica, através das TIC no quotidiano<sup>24</sup>, com o das tecnologias na fase pré-migração, para estabelecer pontos de contacto dentro dos Estados, onde deslocar-se-ão, encontrando-se conectados desde o país de origem, os países de trânsito, até o país de destino. Esta última na fase pós-migração, usando as tecnologias para estabelecer o contacto com a sociedade originária e integrar na sociedade onde se encontrará<sup>25</sup>.

Por outro lado, essas tecnologias encontram-se disponíveis para a prossecução de interesses dos Estados, marcando a tendência da digitalização dos serviços prestados por este (Freitas, 2020), para possibilitar a promoção da desburocratização deste, da extensão da tutela do Estado na salvaguarda dos direitos digitalizados, bem como um conjunto acrescido de direitos estritamente tecnológicos<sup>26</sup>.

Em particular, a sociedade atual depende intrinsecamente das tecnologias para, numa feição positiva, a prossecução dos demais direitos (e.g. o direito ao acesso da informação, o direito à liberdade de expressão), e, numa feição negativa, considerá-los como partes a serem protegidas pelo Estado face à possibilidade da tecnologia poder comprometer determinados direitos<sup>27</sup> caso não haja a devida proteção (e.g. o direito à segurança, o direito à privacidade)

Face à necessidade sentida da garantia dos interesses da sociedade atual, cada vez mais a regulação do ciberespaço tornar-se-á menos burocrática, mais eficiente, mais

---

<sup>23</sup> Este é um dos padrões verificados dos padrões dos fluxos migratórios, estas ligações permitem reduzir os riscos e custos associados com a migração, aumentando os benefícios aos imigrantes facilitando a obtenção de informação através das redes sociais, estabelecer contactos, obter apoio financeiro para essa deslocação entre outros fatores (Collin, *et al*, 2015, pp. 15 e ss). Por outro lado, existe certos riscos inerente a dimensão das redes sociais como a doutrina menciona, em particular o nexó entre o tráfico de pessoas, entre outro tipo de criminalidade organizada, através dos pontos de contacto existentes para transportar os imigrantes de forma irregular para os países destinados (King, 2012, pp. 22 e ss.).

<sup>24</sup> Em particular, caso seja necessário a recolha e partilha de informação relativas a pontos de contacto dentro dos diversos países para facilitar a integração, bem como a possibilidade de manter os laços familiares e, em grande medida, habilita ao posterior envio de remessas para apoiar os familiares residentes no país de origem.

<sup>25</sup> Cfr. Collin, *et al*, 2015, pp. 15 e ss

<sup>26</sup> Esta destrição de direitos prosseguidos através da tecnologia comparativamente a direitos estritamente tecnológicas será escrutinado no capítulo II

<sup>27</sup> Tomemos dois casos ilustrativos do potencial intrusivo nos direitos fundamentais, tomando como ilustrativo o *Cambridge Analytica*, onde esta empresa recorreu à análise de dados para conformar a ação dos eleitores em votar no Presidente Donald Trump. Noutro lado, temos o caso do *Pizzagate*, cujo impacto subsistiu ao disseminar notícias falsas, em particular, o caso que a equipa da campanha de Hillary Clinton estaria a correr um grupo de pedofilia a partir de uma pizzeria. (Omezi, *et al*, 2020, pp. 232 e ss.)

rápida com capacidade de acompanhar a evolução do cenário dos sistemas de informação regulados, são variadas as tendências para conformar a evolução tecnológica<sup>28</sup>. Em particular, no seio da União, encontramos mecanismos de delegação<sup>29</sup> de competências para a Comissão<sup>30</sup> para adotar atos relativos a medidas técnicas e práticas padrão a serem seguidos, conjuntamente com a subdelegação para eu-LISA para detalhar esses padrões.

### 1.1. Dados

Cada vez mais, a sociedade tecnológica consciencializa-se com a quantidade tremenda de dados, sem prejuízo destes já existirem<sup>31</sup>. Estes são produzidos por diversas fontes colocadas voluntariamente através de dispositivos moveis (e.g. telemóveis, computadores), através dos sensores da *Internet das Coisas* (e.g. *smartwatch*, *smart home*), através dos dados partilhados (e.g. redes sociais, correios eletrónicos, biometria). Ainda, também os dados dispostos involuntariamente, para efeitos de estabelecer sessão (e.g. cookies), para os equipamentos tecnológicos comunicarem entre os endereços IP (e.g. protocolos), transmitindo dados. Nesta esteira, cumpre mencionar os tipos de dados regulados no enquadramento jurídico europeu<sup>32</sup>.

#### I. Dados de assinantes<sup>33</sup>

---

<sup>28</sup> Caso reparemos nos modelos de regulação do ciberespaço, tipicamente encontramos o modelo do *Self-Regulation*, assente na participação de fóruns especializados em domínios tecnológicos, bem como a produção de normas técnicas como orientadoras dos padrões a serem seguidos, o modelo de Co-regulação, assente na colaboração com os agentes privados e agentes públicos. Neste sentido, a tendência que verificamos nestes modelos é a constante passagem de uma ótica de formalidade de *Hard Law* para a ótica de *Soft law* para atender às inovações tecnológicas, através de recomendações, comunicações, entre outros instrumentos. Cfr. Freitas, 2020, *A Regulação Jurídica do Ciberespaço – Mutação do paradigma à luz do Acórdão James Elliot do TJUE*, pp. 1-36

<sup>29</sup> Aliás, conforme menciona Palmerini (2013, p. 19), tipicamente é utilizada a ferramenta da delegação técnica, “often used to handle complex scientific matters, to keep pace with their evolutionary change and to maintain a light quality to traditional legislation in fields characterized by a strong technological dimension. (...) Technology itself has been identified as a crucial factor in the growth of private transnational regulation. Combining formal law and technical standards, as a feasible approach to techno-regulation, requires the private sector to be included in the legal order and raises problems of democratic control and legitimacy.” [sublinhado nosso]

<sup>30</sup> Caso reparemos no Tratado sobre o Funcionamento da União Europeia (TFUE), é previsto a possibilidade de delegação na Comissão poderes de adoção de atos não legislativos, ou que alterem elementos não essenciais do ato legislativo, nos termos do artigo 290.º, bem como os atos de execução nos termos do artigo 291.º

<sup>31</sup> A recolha de dados é uma atividade relativamente antiga, já era utilizada pelos decisores políticos, em particular, o regime Nazi carecia de dados em abundância sobre as populações jesuítas, com a ajuda da IBM; durante o genocídio de Ruanda, os Tutsis foram sistematicamente perseguidos através dos registos étnicos, entre outras formas de uso (Molnar, 2019)

<sup>32</sup> Para tal, recorreremos à proposta do Regulamento do Parlamento Europeu e do Conselho relativo às ordens europeias de entrega ou de conservação de provas eletrónicas em matéria penal (*E-Evidence*), com a comunicação 2018/0108 (COD), onde elenca os tipos de dados

<sup>33</sup> Estes são dados relativos “à identidade de um assinante ou cliente, tais como o nome fornecido, a data de nascimento, o endereço postal ou geográfico, os dados de faturação e pagamento, o número de telefone ou

II. Dados de acesso<sup>34</sup>

III. Dados transacionais<sup>35</sup>

IV. Dados de conteúdo<sup>36</sup>

Por esta quantidade tremenda de dados, tipicamente recolhida, armazenada e tratada em grandes conjuntos de dados como parte da *big data*, também utilizada para o fenómeno migratório (Molnar, 2019). Estes conjuntos de dados tem uma dimensão tremenda de potencial benefício para a sociedade, podendo ser explorados de forma automatizada através do uso de algoritmos para otimizar esse tratamento.

Conjuntamente, através do uso de ferramentas da inteligência artificial<sup>37</sup> para processar dados com aprendizagem automática (*machine learning*<sup>38</sup>), a aprendizagem profunda (*deep learning*<sup>39</sup>), bem como o processamento de linguagem natural (*natural*

---

*endereço telefónico*” bem como “ao tipo de serviço e respetiva duração, incluindo dados técnicos e dados que identifiquem medidas técnicas associadas ou interfaces fornecidas ao assinante ou cliente ou por ele utilizadas, e dados relacionados com a validação da utilização do serviço, com exceção de palavras-passe ou outros meios de identificação utilizados em substituição de uma palavra-passe, que sejam fornecidos por um utilizador ou criados a pedido do mesmo” (n.º 7 do artigo 2.º da proposta da E-Evidence)

<sup>34</sup> Quanto aos dados de acesso, estes devem ser definidos como “dados relacionados com o início e o fim da sessão de acesso de um utilizador a um serviço, os quais são estritamente necessários apenas para identificar o utilizador do serviço, tais como a data e hora da utilização ou do início (log-in) e do fim (log-off) da ligação ao serviço, juntamente com o endereço do protocolo IP atribuído pelo fornecedor do serviço de acesso à Internet ao utilizador de um serviço, dados que identifiquem a interface utilizada e o código de identificação do utilizador. Estes dados incluem os metadados das comunicações eletrónicas, na aceção do artigo 4.º, n.º 3, alínea c), do [Regulamento relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas]” (n.º 8 do artigo 2.º das propostas da E-Evidence)

<sup>35</sup> Estes dados transacionais, os quais incluem os dados de tráfego, podem ser definidos como “dados relacionados com a prestação de um serviço por um prestador de serviços que servem para fornecer contexto ou informações adicionais sobre esse serviço e são gerados ou tratados por um sistema de informação do prestador de serviços, tais como o remetente e o destinatário de uma mensagem ou de outro tipo de interação, dados sobre a localização do dispositivo, a data, a hora, a duração, o tamanho, a via, o formato, o protocolo utilizado e o tipo de compressão, exceto se se tratar de dados de acesso. Estes dados incluem os dados das comunicações eletrónicas, na aceção do artigo 4.º, n.º 3, alínea c), do [Regulamento relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas]” (n.º 9 do artigo 2.º da proposta da E-Evidence)

<sup>36</sup> Já os dados de conteúdo devem ser entendidos como “dados armazenados num formato digital, como texto, voz, vídeos, imagens e som, que não sejam dados de assinantes, dados de acesso ou dados transacionais” (n.º 10 do artigo n.º 2 proposta da E-Evidence)

<sup>37</sup> É compreendida como as técnicas que permitem que as máquinas assumam funções do foro cognitivo, as quais, tipicamente associamos à inteligência humana, para aprenderem autonomamente (Taddeo and Floridi, 2018, p. 751; Calo, 2017, p. 404 (*apud* Beduschi, 2020, pp. 1-21)

<sup>38</sup> Faz parte do subsistema da inteligência artificial, congregando um conjunto de técnicas utilizadas nos computadores para estes aprenderem com os dados autonomamente, em particular, “*learn to recognize complex patterns and make intelligent decisions based on data*”, podendo ser esse de forma supervisionada, não supervisionada, semi-supervisionada e compreensão ativa (Han, *et al*, 2012, pp. 24 e ss.)

<sup>39</sup> Pode ser definida como as técnicas que permitem que as máquinas assumam funções do foro cognitivo, as quais, tipicamente associamos à inteligência humana.

*language processing*<sup>40</sup>), é possível processar dados em grande escala, e, subsequentemente aprender com esses dados, de forma integrada (Ruggiu, 2018, p. 406). Este tratamento de dados poderá ser benéfico, caso o uso de algoritmos seja transparente, bem o uso dos dados não resulte em discriminação como veremos posteriormente.

Conforme menciona Beduschi (2020, p. 3), as tecnologias da inteligência artificial podem afetar a gestão dos fluxos migratórios à escala internacional, em particular, através do aprofundamento da assimetria entre os Estados no plano internacional, ao modernizar as práticas dos Estados e as organizações internacionais e, por fim, ao intensificar o uso dos dados para orientar a decisão política na gestão destes fluxos e no controlo fronteiriço.

Na dimensão das migrações na União, por um lado, cada vez mais os agentes dedicados ao controlo fronteiriço armazenam os dados recolhidos nos pontos de controlo fronteiriço nas diversas bases de dados da União (e.g. SIS II, VIS, Eurodac), procurando correlacionar e encontrar padrões para classificar os dados face aos dados históricos<sup>41</sup>.

Por outro lado, também o uso das tecnologias de inteligência artificial tem sido comumente utilizada, tomemos como exemplificativo do Gabinete Federal Alemão para as Migrações e Refugiados (*Bundesamt für Migration und Flüchtlinge*, BAMF) que pilotou projetos como a automatização do reconhecimento facial, do dialeto, traduzindo o nome, analisando os dados dos equipamentos móveis para verificação da identidade. Podemos ainda considerar o uso destas tecnologias pelas autoridades Suecas na previsão da próxima crise migratória (Tangermann 2017; Federal Office for Migration and Refugees 2018; Carammia and Dumont 2018 (*apud* Beluschi, 2020, p. 4))

Verificamos a presença da informatização do corpo<sup>42</sup> como meio de autenticação para verificar a identidade do migrante, em particular, através dos leitores biométricos, reconhecendo que as características biométricas são únicas em cada indivíduo, bem como

---

<sup>40</sup> Essas técnicas assentes em modelos de redes neurais visam manipular e compreender a linguagem humana, podendo tecer certos padrões partindo da análise comportamental, sem a intervenção humana (Skelac, *et al*, 2020, p. 42 e ss.)

<sup>41</sup> Estes dados históricos são aqueles armazenados nas bases de dados da União noutras situações distintas ao controlo efetuado.

<sup>42</sup> Cfr. Ploeg, *et al*, 2011, pp. 68-104

a comparação com as características biométricas inerentes no documento de identificação ou passaporte (Pötzsch, 2015, p. 11).

Este uso alargado dos dados recolhidos da União, permite melhorar o controlo dos fluxos migratórios, através das técnicas de definições de perfis<sup>43</sup> pelos serviços de fronteira. Estas técnicas de *profiling*<sup>44</sup> são tipicamente utilizadas pelos serviços de fronteira, com o intuito de, por um lado, identificar os indivíduos através da recolha de dados de um indivíduo em específico, com uma abordagem reativa na ótica de *Intelligence-led policing*. Por outro lado, através do método preditivo, permite identificar os potenciais imigrantes que se encontram em situação irregular ou tornar-se-ão passíveis de tornarem-se em situação irregular, partindo de uma abordagem proativa, consubstanciada na análise do risco, na ótica de *Predictive policing*<sup>45</sup>.

## 1.2. Algoritmos

Para o entendimento do termo algoritmo, definimo-lo como uma sequência de instruções criadas para informar o computador sobre o que este deve de fazer<sup>46</sup>. Estes algoritmos encontram-se em toda a nossa atividade, tratando-se de raciocínio lógicos que permitem estabelecer operações lógicas para uma determinada ação, como os operadores lógicos usados na pesquisa no motor de busca<sup>47</sup>, programando numa determinada linguagem (e.g. Java, Python, SQL) para receber as instruções (i.e. input), processá-las com a sequência de passos específicos (i.e. algoritmo), conferindo um determinado resultado (i.e. output).

---

<sup>43</sup> Para o melhor entendimento das decisões automatizadas e a definição de perfis, torna-se imprescindível recorrer à alusão da tutela destes direitos à luz do Regulamento Geral de Proteção de Dados (RGPD), “*O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.*” (Cfr. o n.º 1 do artigo 22.º do RGPD)

<sup>44</sup> Para uma visão jurídica deste assunto, recomendamos a leitura Cfr. José Ferreira, A., 2018, pp. 35-44

<sup>45</sup> Recorrendo à doutrina nesta matéria, este tipo de policiamento tem diversas aplicações, tomando como exemplificativo, “*most predictive policing applications have drawn on location-based data to define increasingly localised “hot spots” on which the police should focus attention at particular times, while others draw on personal data to identify likely offenders. Other applications aim to predict likely victims of crime in cases such as domestic violence, or those at risk of becoming offenders in the future.*” (Macnish, et al, 2020, pp. 201)

<sup>46</sup> Cfr. Domingues, 2015, pp. 21 e ss; Kalpokas, 2019, p. 27-48

<sup>47</sup> Tomemos como exemplificativo o uso do motor de busca da Google, ao realizar a pesquisa (*queries*) através de aspas o resultado aponta para um termo específico, o uso do operador AND estabelecendo uma relação incluyente entre duas expressões pesquisadas, por defeito, o algoritmo assume este operador nas nossas pesquisas, o operador OR com a relação entre duas expressões isoladas ou conjuntas (i.e. web OR site), limitar os resultados para um sítio web específico (i.e. site:website.com)

A presença destes encontram-se em toda a nossa vida, recorrendo às palavras de Domingues (2015, p. 21): “*Não estão apenas nos celulares ou laptops, mas nos carros, em nossa casa, nos utensílios domésticos e em brinquedos. As instituições bancárias são um imenso quebra-cabeça de algoritmos, com pessoas apertando botões do outro lado. Os algoritmos programam voos e também pilotam aeronaves. Eles gerenciam fábricas, comercializam e entregam mercadorias, calculam os lucros e mantêm registros. Se todos os algoritmos parassem de funcionar inesperadamente, o mundo que conhecemos chegaria ao fim.*” A nossa sociedade é mercada pelos algoritmos.

É compreensível que o uso de algoritmos tornou-se vital para o nosso quotidiano, mesmo que não apercebamo-nos da sua presença, estes encontram-se desde a pesquisa de determinados conteúdos num motor de busca, até mesmo assistir na eficiência da tomada de decisões com base na informação recolhida, tomando como ilustrativo o *Intelligence Led Policing*<sup>48</sup>, onde as ferramentas tecnológicas baseadas em determinados algoritmos, permitem facilitar a intervenção, como também decidir as áreas escolhidas para o policiamento em virtude da conjugação com ferramentas de análise de dados.

Esta sociedade tecnológica é marcada pela presença dos algoritmos no quotidiano, como tínhamos mencionado previamente, principalmente pela constante digitalização dos serviços prestados pelo setor público e privado, bem como pelo uso de soluções tecnológicas assentes em algoritmos, carecendo a tutela dos Estados na governança<sup>49</sup> deste mundo digital. Simultaneamente, os Estados deverão, conforme mencionamos previamente, garantir a prossecução dos direitos fundamentais no desenho dos algoritmos<sup>50</sup>.

Relativamente à dimensão dos direitos fundamentais, o direito ao acesso à informação poderá ser dificultado com uso de algoritmos, os quais, para o entendimento do indivíduo mediano, potencialmente não compreenderá. Por conseguinte, a doutrina

---

<sup>48</sup> Este modelo de policiamento orientado pelas informações tem vindo a ser explorado por diversos Estados, sendo definido pelo “*modelo de atuação e filosofia de gestão, em que a análise de dados e as informações criminais são fulcrais para a prossecução de um objetivo, a saber: um processo de tomada de decisão que facilite a redução, a irradicação e a prevenção da criminalidade, através da conjugação de estratégias eficazes de gestão e de combate a delinquentes perigosos e reincidentes*” (Ratcliffe, 2018, p. 89 (*apud* Moleirinho, 2014, p. 255)

<sup>49</sup> Cfr. Kalpokas, 2019, pp. 1-10

<sup>50</sup> Inclusive, na doutrina há quem fale do código algorítmico como regulador da sociedade, devendo o Estado regulá-lo, na esteira de Lessig (2006, p. 79, *apud*), sendo essenciais para o benefício do Estado usar essas tecnologias na prossecução do interesse público legítimo (Kalpokas, 2020, p. 93 e ss)

tem vindo a apelar a duas dimensões para explicar o funcionamento dos algoritmos, democratizando o seu uso, compreendendo os seus efeitos para tomar uma ação consciente.

Paralelamente, podemos explicar os algoritmos recorrendo à explicação baseada no modelo algorítmico (MCE), ou seja, a forma como funciona, bem como a explicação baseada no conteúdo do algoritmo (SCE), ou seja, as suas consequências (Edwards, [et al.], 2017), e, de facto, no ordenamento jurídico europeu, parece dar-se preferência a esta última<sup>51</sup>. Este tipo de explicações deve ser visto para melhorar a transparência e compreensão do tratamento de dados com base em algoritmos. Aliás, a doutrina dos cientistas da computação aponta para o conceito técnico da *legibilidade*<sup>52</sup>, presente como princípio na redação do código fonte pelos cientistas, na compreensão autónoma da importância e as implicações do processamento desses dados.

A relevância deste conceito é um inibidor do exercício do direito pleno ao acesso à informação e de ser informado, tomemos a dimensão dos controlos fronteiriços, nos quais as indicações previstas no Manual Schengen, devem ser suportadas por este conceito. Por conseguinte, deverá ser explicitado o funcionamento do algoritmo detalhadamente, bem como as consequências do mesmo na esfera do imigrante, recorrendo aos modelos de explicação dos algoritmos previamente mencionados, permitindo tomar uma decisão consciente por parte do imigrante<sup>53</sup>.

Por conseguinte, estes algoritmos aumentam a qualidade do serviço prestado, acarreta inúmeras melhorias no nosso quotidiano, contudo é necessário compreender que ao empregar os algoritmos na implementação de medidas, certos elementos devem ser conjugados para controlar os impactos possíveis nos direitos fundamentais do

---

<sup>51</sup> A relevância destes conceitos prende-se com particularidade do RGPD prever a necessidade de explicar-se a lógica envolvida, mas o mesmo, não detalha a forma como deve ser prosseguido, além de mencionar que deve incluir informação específica (considerando 71.º), a lógica subjacente ao eventual tratamento automático, com base nas suas consequências (considerando 63.º com leitura conjunta da alínea f) do n.º 2 do artigo 13.º do RGPD)

<sup>52</sup> O entendimento deste conceito traduz-se no entendimento humano relativa à facilidade da compreensão do mesmo, tipicamente críticos para o desenvolvimento de *software*, uma vez que ao entender previamente, facilita a perda de tempo para compreender o significado das linhas de código mencionadas Cfr. Buse e Weimer, 2008, pp. 1-14; Quanto à sua aplicação no contexto das decisões automatizadas, Cfr. Malgieri, 2019, pp. 4 e ss.

<sup>53</sup> Na secção 1.2 do manual Schengen, verificamos que todos os cidadãos tem o direito a serem informados da natureza do controlo e serem tratados respeitosamente, conjuntamente o processamento desses dados nas diversas bases de dados da UE. Cfr. FRA, 2018c, pp. 58 e ss; Recomendação da Comissão, (2019) 7131 final

terceiro afetado por esse algoritmo, reconhecendo que os mesmos tem estas particularidades<sup>54</sup>:

- Instrumentos criados pelo Homem;
- Discricionariedade no desenho e aplicação de algoritmos;
- Opacidade nas características de determinados algoritmos

Concomitantemente, é necessário compreender que pela circunstância natural destes instrumentos serem criados pelo Homem, reconhecendo que este é um ser imperfeito e, como tal, o desenho destes algoritmos podem conter imperfeições típicas da natureza humana, caso estes não sejam previamente testados quando aos seus impactos numa dimensão holística. O seu funcionamento poderá ser dimensionado para determinados objetivos e, devido à circunstância inicial, os mesmos podem ser desvirtuados do propósito inicial.

Por um lado, também é notório a discricionariedade da mão humana na discricionariedade do desenho destes algoritmos, pois visam solucionar determinados problemas na sociedade, podendo esses problemas serem a eficiência de uma determinada atividade, a melhoria da prestação de um serviço, assegurar propriedades de segurança numa comunicação através de encriptação, entre outros. No entanto, tipicamente os algoritmos visam um propósito concretos como a tomada de decisão relativa à concessão de empréstimos, na contratação de recursos humanos, na autorização da entrada na fronteira de um estado, ou até decisões do Tribunal<sup>55</sup>.

### *1.3. Machine learning e deep learning*

Estas ferramentas de inteligência artificial podem assumir diversos intuitos como a análise de risco nos tribunais para prever a possibilidade de reincidência (COMPAS)<sup>56</sup>, programas de policiamento preditivo para identificar pontos onde

---

<sup>54</sup> Seguindo a esteira, Cfr. Gerards, 2019, pp. 205-209

<sup>55</sup> Para compreender estas dimensões da aplicação de algoritmos com impacto na tomada de decisões, recomendamos esta leitura, Cfr. La Diega, 2018, pp. 3-34

<sup>56</sup> Tomando como ilustrativo o uso do software *COMPAS*, podendo comprometer inúmeros direitos tipicamente assentes no processo penal. Neste sentido, a doutrina aponta para um conjunto de direitos expressamente afetados na sua utilização em sede de Tribunal para determinar o risco da reincidência de um determinado delito, como é o caso reconhecido do *Correctional Offender Management Profiling for Alternative Sanctions (COMPAS)* nos EUA. Desta feita, a sua utilização no caso conhecido no Tribunal Supremo de Wisconsin de 2016, reconhecido como *State v. Loomis - 2016 WI 68, 371 Wis. 2d 235, 881 N.W.2d 749*, onde houve o requerimento de interposição

potencialmente ocorreram novos crimes (PredPol)<sup>57</sup>, bem como os testes por via de detetores de mentiras para garantir a entrada de imigrantes que viajam em boa fé (iBorderCtrl)<sup>58</sup>, entre outras aplicações de técnicas de inteligência artificial.

Para o entendimento destes termos, é relevante a distinção da programação tradicional, como mencionado previamente, em comparação com a aprendizagem autónoma (*machine learning*). A primeira é meramente a combinação entre o *input* dado, processando com um *algoritmo*, conferindo um *output*, enquanto que a última visa treinar a máquina com dados históricos embebidos com o *output*, funcionando como modelo capaz de autonomamente escrever um programa capaz de avaliar padrões que surgem nesse conjunto de dados.

Como podemos denotar, num modelo de *machine learning*, é necessário compreender a qualidade dos dados como *input* ao modelo, podendo introduzir viés, o algoritmo utilizado, no sentido da sua compreensão das operações matemáticas que encaminham para um determinado resultado e, por fim, o próprio modelo que é avaliado por taxas atribuídas ao grau de eficácia do modelo, com a taxa de falso positivos e falso negativos, bem como outros indicadores (Han, 2011, pp. 24 e ss.).

Outra técnica da inteligência artificial é os algoritmos de *deep learning*, os quais podem ser definidos como um subconjunto de técnicas de *machine learning* com um foco em algoritmos relativos à analogia das redes neuronais humanas, decorrendo a função de ativação da sinapse ligando os neurónios, enquanto nas redes neuronais opera os perceptrões (i.e. neurónios) designando cada camada oculta, enquanto um conjunto designa-se por multiperceptrões, também com uma função de ativação. (Han, 2011, 398 e ss.)

Tomando como ilustrativo as redes neuronais, são compostas por redes de *input*, onde sabemos os dados históricos e os dados reais, bem como a camadas ocultas ao

---

do recurso recusado pelo próprio tribunal pois o determinado algoritmo estava tutelado por direitos de propriedade, encaminhando a doutrina nas indagações relativas à violação do princípio do processo equitativo, sem prejuízo do tribunal ter alegado que o uso desta avaliação de risco do COMPAS serviu somente o propósito de corroborar com os elementos factuais encontrados ao longo do processo. Cfr. La Diega, 2018, pp. 3-34; Završnik, 2020, pp. 567-583; Maggiolino, 2019, pp. 1-16; Kehl, *et al*, 2017, pp. 1-36.

<sup>57</sup> Cfr. a hiperligação <https://www.predpol.com>

<sup>58</sup> Este projeto será desenvolvido posteriormente no capítulo III

olhar humano, onde sabemos o algoritmo, mas não compreendemos o seu funcionamento pela elevada complexidade, pautando, assim, estes algoritmos por uma certa opacidade (Restovic, 2020, p. 29 e ss.).

Com efeito, é por estas circunstâncias que a doutrina tem vindo a falar do conceito de *black box*<sup>59</sup> devido à opacidade (Molnar, 2020, p. 785) “*algorithm’s source code, its training data, or other inputs may be proprietary, and can be shielded from public scrutiny on the bases of intellectual property legislation or as confidential business assets*”.

Conjuntamente com a dimensão da proteção de dados<sup>60</sup> protegidos à luz da propriedade intelectual, os quais também poderá ocultar o modelo para usufruto da exclusividade desse segredo. O mesmo pode também decorrer da complexidade do algoritmo que poderá comprometer a compreensão das operações que ocorreram dentro das camadas ocultas e, por essa razão, “[a]s we are putting more trust in machine learning systems and integrating them into our lives, from health to legal system, it is crucial to understand their foundation and limits more thoroughly.” (Lauc, 2020, p. 97)

---

<sup>59</sup> Para a leitura relativa à falta da transparência e as dimensões organizacionais, técnicas e legais do assunto, recomendamos, Cfr. Statewatch, 2020, pp. 8 e ss.

<sup>60</sup> Por proteção de dados entende-se a legislação que protege os dados pessoais, e nos termos do artigo 4.º do RGPD, são considerados aqueles dados que permitam a identificação “...direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular”. Esta definição encontra-se altamente densificada, prevendo uma área de atuação muito vasta, considerando a mera retenção e destruição como tratamento de dados.

## 2. Direitos fundamentais dos imigrantes na UE

No que concerne aos direitos fundamentais do imigrante, é relevante mencionar a leitura garantística destes direitos na UE, enriquecida pelo panorama sociedade tecnológica, esta inserida num contexto mutacional marcado por diversas gerações de direitos fundamentais da pessoa humana<sup>61</sup>. Para a doutrina, a ponderação do impacto das tecnologias sobre os direitos fundamentais é recente, no entanto, reconhecia-se os benefícios da mesma na sociedade, bem como os avanços científicos, os quais poderiam acarretar consequências negativas para os direitos fundamentais<sup>62</sup>.

Estes direitos fundamentais devem ser salvaguardados em todo o processo inerente dos fluxos migratórios<sup>63</sup>, desde o controlo fronteiriço efetuado pelas autoridades locais na fronteira europeia<sup>64</sup>, até o controlo externalizado nos países terceiros, efetuados por autoridades locais e europeias na fronteira extra-UE. Nestas fases do controlo, cabe ao Estado garantir a proteção dos direitos humanos face ao potencial intrusivo das tecnologias (Ruggiu, 2018, pp. 9 e ss.), os quais, o indivíduo poderá reivindicar esses direitos em sede de Tribunais supranacionais (e.g. TEDH), tomando como exemplificativo, contra o Estado.

Estes direitos fundamentais, em grande medida, não devem ser perspetivados como direitos absolutos, ou seja, podem ser limitados em função da prossecução dos interesses dos Estados, devendo para o efeito analisar através de princípios orientadores dessa mesma restrição. Nesse sentido, no enquadramento jurídico da União, encontramos os seguintes parâmetros elencados nos termos do n.º 1 do artigo 52.º da CDFUE:

---

<sup>61</sup> Na esteira do mencionado por Gouveia, 2015, estes direitos fundamentais partem de um conjunto de características advenientes de períodos históricos que marcam a sociedade contemporânea, em particular a sociedade de risco, a sociedade global, a sociedade da informação e a sociedade multicultural com inúmeras preocupações, culminando com a proteção internacional dos direitos humanos Cfr. Gouveia, 2015b, pp. 161-165

<sup>62</sup> Cfr. Ruggiu, 2018, pp. 10 e ss.

<sup>63</sup> Contudo, é necessário compreender que cada Estado tem a prerrogativa de admitir ou recusar a entrada de um estrangeiro, assente numa discriminação entre nacional e o imigrante, contudo, estes instrumentos exigem que seja respeitado um conjunto de direitos mínimos, como é o caso dos direitos humanos, os quais deverão ser respeitados. (Palm, 2020, pp. 9-27)

<sup>64</sup> Neste sentido, parece relevante mencionar que no CFS, existe a dimensão da dignidade humana nos controlos fronteiriços, tomando medidas que respeitem os direitos do indivíduos, proporcional com os objetivos pretendidos, e, principalmente, devem ser informados sobre o que se trata esse controlo específico. Cfr. o considerando 7.º do CFS, no Regulamento (UE) 2016/399.

- I. Legitimidade na lei, devendo ser examinado se a limitação é previsível na lei e acessível para o indivíduo.
- II. Respeitar a essência desses direitos, perceber se a essência desse direito é esvaziada, limitando qualquer exercício desse direito
- III. Respeitar o interesse público reconhecido pela União
- IV. Deverá ser proporcional, não deverá exceder os objetivos a alcançar, ser adequado e ser necessário.

Para a avaliação do presente estudo da proporcionalidade das medidas elencadas nos módulos do projeto iBorderCtrl, seguiremos a metodologia de análise recomendada pela Agência Europeia para a Proteção de Dados (2019) no teste da proporcionalidade das medidas.

### *2.1. Direitos face às tecnologias*

Neste sentido, a dimensão da tutela dos direitos do imigrante subjacentes ao quadro jurídico dos direitos humanos é predominante na esfera política dos Estados, compreendendo-os como uma melhoria da proteção harmonizada com a disseminação de instrumentos de direito internacional e a judicialização dos direitos humanos. O foco deverá ser no meta-direito da proteção de dados, visando garantir a proteção destes para que os demais direitos sejam prosseguidos.

Esta proteção corresponde a um período histórico marcado por atrocidades da guerra, visando salvaguardar os direitos da pessoa humana. Estes direitos, face à sociedade atual evoluíram para uma nova geração que, por um lado, são prosseguidos com o auxílio da tecnologia e, por outro lado, podem ser afetados através destas tecnologias como ferramentas de vigilância e da exploração abusiva dos dados pessoais.

Em matéria de privacidade, é imprescindível considerar o Direito à Privacidade<sup>65</sup>, com feição positiva na proteção e no respeito da esfera da intimidade privada e, na feição negativa, impõe uma limitação da interferência do Estado nos assuntos abrangidos por esta proteção, sem prejuízo deste poder ser desrespeitado em situações de interesses

---

<sup>65</sup> Consagrado como direito fundamental nos termos do artigo 8.º da Convenção Europeia dos Direitos Humanos, juntamente com o artigo 16.º do TFUE

superiores advirem desse mesmo desrespeito, tomando como exemplificativo a prossecução criminal, assente no princípio da proporcionalidade.

Cada vez mais, os direitos tecnológicos devem ser entendidos como meta-direitos, sem os quais, o usufruto dos demais direitos na esfera dos indivíduos não consegue ser prosseguido. Caso não houvesse um direito à não sujeição a decisões automatizadas e definição de perfis, a decisão fundada nesses algoritmos não teria qualquer limitação. Em última análise, poderia comprometer um conjunto enorme de direitos, não por factos objetivos fundados como a prossecução de interesses públicos por parte do Estado, mas por circunstâncias subjetivas com algoritmos com efeitos discriminatórios.

Relativamente ao direito a ser reconhecido como pessoa perante a lei visa salvaguardar os direitos dos imigrantes, entendido como pré-requisito para terem acesso a outros direitos<sup>66</sup> como o acesso ao trabalho, acesso à segurança social ou pensão, entre outros<sup>67</sup>. Caso o migrante não consiga ter acesso a dados necessários para ser reconhecido perante a lei como pessoa, a condição do imigrante degradar-se-á.

No controlo fronteiriço, são inúmeros os direitos que devem ser salvaguardados, em particular orientados pelo princípio da dignidade humana<sup>68</sup>, o princípio da não discriminação<sup>69</sup>, independentemente da etnia, nacionalidade, religião, orientação sexual, entre outros traços caraterísticos. Também compreende a dimensão das decisões automatizadas ou definição de perfis, as quais não devem produzir efeitos discriminatórios, como veremos posteriormente.

---

<sup>66</sup> Cfr. Allinson, 2018, pp. 16-20

<sup>67</sup> Cfr. o artigo 6.º da Declaração Universal dos Direitos Humanos e o artigo 16.º do Pacto de Direitos Cívicos e Políticos

<sup>68</sup> Parece relevante mencionar as palavras de Oliveira Ascensão, 2008, ao mencionar que o direito à dignidade humana dos indivíduos: “[c]om a informática a sua vulnerabilidade passou a ser extrema, porque pelo cruzamento de dados passou a ser possível reconstituir com prática certeza a vida de cada um.”

<sup>69</sup> Como ilustrativo desta possibilidade de discriminação, É relevante compreender os vários casos de estudo compilados pela FRA, em particular o levantamento do acesso aos direitos efetuado pela equipa do Ombudsman francês, onde constante que indivíduos de outras etnias, com menos de 25 anos, são tipicamente mais abordados pelas autoridades, em particular vinte vezes mais do que a população em geral. Este é um dos exemplos em que caso esta discriminação seja a fonte de alimentação do conjunto de dados usados para a tomada de decisão, em virtude de caraterísticas étnicas, o resultado poderá ser discriminação do indivíduo. Cfr. FRA, 2018c, pp. 46-47; Para a compreensão do direito à não discriminação, recomendamos a leitura, Cfr. Toprakseven, 2018, pp. 21-26

Quando reparamos o tipo de dados que predomina na União para o controlo dos fluxos migratórios, verificamos a presença dos dados biométricos nos vários sistemas de informação, em particular, na Eurodac as impressões digitais desde os 14 anos e reconhecimento facial desde os 6 anos, no VIS a impressão digital e reconhecimento facial desde os 12 anos, no SIS II relativo à polícia as impressões digitais, o reconhecimento facial e o perfil de ADN, entre outras bases de dados (FRA, 2017)

## 2.2. *Direitos de cariz tecnológico.*

De facto, relativamente à proteção dos dados<sup>70</sup>, este direito estritamente tecnológico está subjacente um direito abrangente à privacidade<sup>71</sup>, conforme tutelado pelo CDFUE. É relevante mencionar principalmente que este direito abrangente aponta para uma proibição da não interferência na vida privada, enquanto que o primeiro aponta principalmente restringir o processamento dos dados pessoais que produza efeitos legais sobre a esfera do titular.

Este direito não é tipicamente pautado como um direito absoluto<sup>72</sup>, poderá ser restringindo em prol de outros direitos com a proteção jusfundamental por parte do Estado, podendo restringir o direito à livre circulação pela via tecnológica ou não, reconhecendo a supremacia de direitos como o direito à vida, sem prejuízo da ponderação do princípio da proporcionalidade conjugado com os direitos superiores na hierarquia, respeitando os princípios relativos à proteção de dados (FRA, 2018c):

- Legalidade<sup>73</sup>
- Limitação do propósito<sup>74</sup>

---

<sup>70</sup> Cfr. o artigo 8.º da CDFUE

<sup>71</sup> Este direito à vida privada ou direito à privacidade trata-se de um dos fins do Direito na garantia do bem estar dos indivíduos, estando subjacente a tutela dignidade humana. Aliás, na esteira do mencionado por Oliveira Ascensão, (2008), este direito à privacidade cada vez mais tem assumido maior preponderância com as tecnologias e o potencial intrusivo das mesmas: “*Europa e aos outros lugares onde se estendem a civilização ocidental, ocupando um lugar cimeiro e desdobrando-se em múltiplas restrições e proibições. Há explicação para que assim tenha acontecido. A sociedade que nos rodeais é uma sociedade tecnologicamente avançada. O homem, no seio dela, é uma mónada altamente vulnerável: as possibilidades de intromissão na vida de cada pessoa são hoje inúmeras e ameaçadoras.*”. Concordamos com esta posição com o desenvolvimento tecnológico, na medida em que a complexificação das tecnologias comprometerá a transparência da sua compreensão, quer pela intrínseca complexidade do algoritmo, quer pela tutela de direitos de propriedade intelectual sobre determinadas ferramentas, aumenta o potencial intrusivo, bem como o seu efeito nos direitos fundamentais, em particular o direito à dignidade humana. Cfr. Ascensão, 2008, pp. 277-299

<sup>72</sup> Cfr. o artigo 52.º da CDFUE

<sup>73</sup> Cfr. a alínea a) do n.º 1 do artigo 5.º e o artigo 6.º do RGPD,

<sup>74</sup> Cfr. a alínea b) do n.º 1 do artigo 5.º do RGPD e o n.º 2 do artigo 8.º da CDFUE.

- Minimização dos dados<sup>75</sup>
- Limitação da conservação<sup>76</sup>
- Integridade e confidencialidade<sup>77</sup>

Relativamente à segurança dos dados, ou seja, a integridade e a confidencialidade, sem prejuízo da disponibilidade, estes princípios devem ser salvaguardados no ciclo de vida dos dados<sup>78</sup>. O processo de tratamento dos dados deve compreender mecanismos de qualidade dos dados, restrição do acesso somente a pessoas autorizadas, limitação do seu uso, mecanismos de segurança como a encriptação, anonimização ou pseudonomização, autenticação reforçada (e.g. multifator), manter o registo dos logs dos acessos e uso desses dados, entre outros.

Para apurar o risco deste tipo de processamento de dados, é necessário implementar avaliação de impacto da proteção de dados, reconhecendo o caráter obrigatório desta avaliação. Esta obrigatoriedade circunscreve-se a tratamento automatizado de dados, incluindo a definição de perfis<sup>79</sup>, previamente ao tratamento com a informação constante do RGPD, devidos aos riscos colocados aos direitos fundamentais.

Estes cenários que decorrem das decisões automatizadas e do *profiling* são devidamente acauteladas pelo RGPD, onde é mencionado um conjunto de direitos do titular dos dados, sempre que este esteja perante decisões com repercussões legais na esfera deste titular (Malgieri, 2019)<sup>80</sup>:

#### I. Direito a ser informado,<sup>81</sup>

---

<sup>75</sup> Cfr. o artigo 5.º do RGPD

<sup>76</sup> Cfr. a alínea e) do n.º 1 do artigo 5.º do RGPD

<sup>77</sup> Nesta esteira, falamos da segurança dos dados que devem ser garantidos para ser garantido a integridade que, neste contexto poderá significar manter os dados com a mesma substância, sem que estes sejam alterados ou acedidos. Cfr. a alínea f) do n.º 1 do artigo 5.º, com leitura conjunta do artigo 28.º e 32.º do RGPD

<sup>78</sup> Para a compreensão dos princípios, recomendamos consultar o Capítulo II sobre os Direitos Fundamentais do imigrantes tecnológicos face à tecnologia, bem como a obrigatoriedade prevista no RGPD, decorrente do artigo 32.º do RGPD

<sup>79</sup> Cfr. a alínea a) do n.º 3 do artigo 35.º do RGPD, e o artigo 27.º da Diretiva (UE) 2016/680

<sup>80</sup> Cfr. Malgieri, 2019, pp. 1-26

<sup>81</sup> Sempre que os dados são recolhidos junto do titular dos dados, existe um conjunto de dados que deve ser facultado ao mesmo, devido à obrigação legal prevista, (Cfr. a alínea f) do n.º 2 do artigo 13.º do RGPD). Conjuntamente, também o Regulamento prevê as situações em que os dados não são recolhidos junto do titular, o que não pode inibir o direito de acesso à informação, (Cfr. a alínea g) do n.º 2 do artigo 14.º do RGPD). Nesta esteira, o Grupo de Trabalho do artigo 29.º, apela a um conjunto de informações como ilustrativas para esta direito

- II. Direito de acesso à informação<sup>82</sup>
- III. Direito de contestar a decisão<sup>83</sup>
- IV. Direito às decisões terem intervenção humana<sup>84</sup>
- V. Direito a conhecer a lógica, o significado e as consequências<sup>85</sup>,
- VI. Direito a retificar a informação recolhida,<sup>86</sup>
- VII. Direito a medidas técnicas adequadas para proteger os dados<sup>87</sup>;

a ser informado, não submetendo ao envio de informações técnicas e, por vezes, incompreensível para o titular dos dados, cumprindo citar:

*“Instead of providing a complex mathematical explanation about how algorithms or machine-learning work, the controller should consider using clear and comprehensive ways to deliver the information to the data subject, for example:*

- *the categories of data that have been or will be used in the profiling or decision-making process;*
- *why these categories are considered pertinent*
- *how any profile used in the automated decision-making process is built, including any statistics used in the analysis;*
- *why this profile is relevant to the automated decision-making process; and*
- *how it is used for a decision concerning the data subject.*

*Such information will generally be more relevant to the data subject and contribute to the transparency of the processing.”* Cfr. Grupo de Trabalho do artigo 29.º, 2018, p. 31

<sup>82</sup> Também é reconhecido o direito de acesso às informações relativas ao tratamento desses mesmos dados conforme mencionado, Cfr. a alínea h) do n.º 1 do artigo 15.º do RGPD. Por outro lado, na dimensão dos controlos fronteiriços, de acordo com o Manual Schengen, na secção 1.2, verificamos que todos os cidadãos têm o direito a serem informados da natureza do controlo e serem tratados respeitosamente. Cfr. FRA, 2018a, pp. 58 e ss.

<sup>83</sup> Este direito de oposição, circunscreve-se a um direito de maior expressividade face ao direito à limitação do tratamento previsto no artigo 18.º do RGPD, em particular, opor-se a um tratamento de dados pessoais fundando para os intuítos previstos no artigo 21.º do RGPD

<sup>84</sup> Este é um direito existente na leitura atenta do n.º 3 do artigo 22.º, com leitura conjunta do considerando 71.º do RGPD

<sup>85</sup> Este direito prende-se com os modelos explicativos do funcionamento dos algoritmos que já tivemos oportunidade de mencionar previamente, bem como o conceito de legibilidade

<sup>86</sup> Cfr. o artigo 16.º do RGPD e o artigo 16.º da Diretiva 2016/680, bem como o n.º 2 do artigo 8.º da CDFUE

<sup>87</sup> Para o entendimento das boas práticas, recomendamos a leitura desta lista não exaustiva do Grupo de Trabalho do Artigo 29.º relativa ao n.º 1 do artigo 22.º do RGPD conjuntamente com o considerando 71.º:

- *regular quality assurance checks of their systems to make sure that individuals are being treated fairly and not discriminated against, whether on the basis of special categories of personal data or otherwise;*
- *algorithmic auditing – testing the algorithms used and developed by machine learning systems to prove that they are actually performing as intended, and not producing discriminatory, erroneous or unjustified results;*
- *for independent ‘third party’ auditing (where decision-making based on profiling has a high impact on individuals), provide the auditor with all necessary information about how the algorithm or machine learning system works;*
- *obtaining contractual assurances for third party algorithms that auditing and testing has been carried out and the algorithm is compliant with agreed standards;*
- *specific measures for data minimisation to incorporate clear retention periods for profiles and for any personal data used when creating or applying the profiles;*
- *using anonymisation or pseudonymisation techniques in the context of profiling;*
- *ways to allow the data subject to express his or her point of view and contest the decision; and,*
- *a mechanism for human intervention in defined cases, for example providing a link to an appeals process at the point the automated decision is delivered to the data subject, with agreed timescales for the review and a named contact point for any queries .*

*Controllers can also explore options such as:*

- *certification mechanisms for processing operations;*
- *codes of conduct for auditing processes involving machine learning;*

Nesta esteira de direitos, não consideramos o direito ao consentimento, devido a posição de inferioridade face à situação vulnerável que se encontra<sup>88</sup>. Tomemos como ilustrativo a necessidade de refugiados nos campos da Jordânia submeterem ao registo dos dados biométricos da íris para obter comida, aliás, no caso dos refugiados no campo de Azraq, estes foram questionados sobre o uso das tecnologias para recolher dados e estes, por sua vez, sentiram-se desconfortáveis, mas reconheciam que não podiam recusar, sob prejuízo também de perder o alimento (Molnar, 2020, p. 774)

Concomitantemente, é imprescindível mencionar na jurisprudência do TJUE, constatamos a preocupação na limitação do propósito, não devendo estender-se ao objetivo inicial da recolha de dados, tomando como exemplificativo o caso *Heinz Huber contra Bundesrepublik Deutschland*, tendo estendido do propósito inicial para fins de combate à criminalidade.

Neste caso o Tribunal decidiu que o uso dos dados armazenados registados numa base de dados com os cidadãos e não cidadãos da UE dentro do território alemão por mais de 3 meses, é legítimo caso seja utilizado para o propósito inicial no estabelecimento de regras relativas à residência. Em contrapartida, estes dados não podem ser utilizados para combater o crime em geral<sup>89</sup>, como sucedido.

Em contraste, na jurisprudência do TEDH, há inequivocamente a defesa do princípio da limitação do armazenamento no acórdão *S. and Marper v. United Kingdom*. Neste caso, as autoridades do Reino Unido tinham armazenam na base de dados de ADN (e.g. impressões digitais, amostras de células, perfis de ADN) para fins de identificação criminal, sem qualquer restrição temporal.

- 
- *ethical review boards to assess the potential harms and benefits to society of particular applications for profiling.*” Cfr. Grupo de Trabalho do artigo 29.º, 2018, p. 31

Adicionando a estas medidas, deve ser compreendido que no conjunto de dados de treino com o propósito de tratamento de dados por algoritmos, com repercussões em dados reais, esses devem ser verificados qualquer viés que possa comprometer a aleatoriedade destes dados, repercutindo em consequências discriminatórias em virtude dos dados parciais. Cfr. Malgieri, 2019, pp. 5 e ss.

<sup>88</sup> Nas palavras de Molnar (2020), “*Consent cannot be truly informed and freely given if it is given under coercion, even if the coercive circumstances masquerade as efficiency and promise improved service delivery*”

<sup>89</sup> Conforme mencionado no Acórdão do Tribunal de Justiça da União, “no sentido de que se opõe à instauração, por um Estado-Membro, de um sistema de tratamento de dados pessoais específico para os cidadãos da União que não são nacionais desse Estado-Membro, com o objectivo de combater a criminalidade.”

Cfr. Acórdão *Heinz Huber v. Bundesrepublik Deutschland*, 16 December 2008,

Como tal, os titulares requeriam a eliminação desses dados, tendo sido recusado pelas autoridades britânicas, tendo esta situação escalado para o TEDH. Subsequentemente, o Tribunal defendeu que houve a violação do direito à privacidade, incorrendo no risco de estigma nos indivíduos que não tinham cometido nenhuma prática de nenhum crime, afetando negativamente o princípio da presunção da inocência<sup>90</sup>.

### 2.3. *Direitos face a decisões automatizadas e definição de perfis*

Para compreendermos a definição deste termo do *profiling* ou definição de perfis, é relevante compreender a definição deste mesmo termo, o qual não deve ser confundido materialmente com as decisões automatizadas. Nessa esteira, o *profiling* pode ser entendido como categorizar determinados indivíduos de acordo com características pessoais, podendo essas serem mutáveis (e.g. hábitos alimentares, preferências, etc.), bem como características imutáveis (e.g. data de nascimento, altura)<sup>91</sup>.

Subsequentemente, para complementar esta definição, torna-se relevante compreender o enquadramento regulatório, em particular na Diretiva (UE) 2016/680 dedicada para as autoridades competentes:

*“[Q]ualquer 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”* Cfr. o n.º 4 do artigo 3.º da Diretiva (UE) 2016/680 e n.º 4 do artigo 4.º do Regulamento (UE) 2016/679

Simultaneamente, há um aspeto determinante que deverá ocupar parte da nossa discussão, em particular, o propósito para o processamento de determinado tipo de dados, compreendendo que será através deste que compreenderemos a aplicação do

---

<sup>90</sup> Cfr. parágrafo 122.º do Acórdão S. e Marper v. The United Kingdom

<sup>91</sup> Cfr. FRA, 2018a, p. 15

RGPD ou da Diretiva (UE) 2016/680. Ao recorrermos aos mecanismos previstos na Diretiva, compreendemos que as dimensões em causa são a prossecução da investigação criminal, face à constante ponderação dos imigrantes da qualidade destes posicionarem-se potencialmente como imigrantes irregulares. São inúmeros os desafios colocados à definição de perfis, levantados pela Agência Europeia para os Direitos Fundamentais, podendo esses serem:

- I. Estereótipos partindo de dados recolhidos previamente,
- II. Suscetibilidade de introduzir viés nos algoritmos
- III. Estabelecer correlações incorretas para indivíduos ou grupos

Nestes desafios compreendemos que o resultado poderá ser a discriminação na tomada de decisões, caso o algoritmo seja utilizado na tomada de decisões com efeitos legais negativos na esfera individual, salvo as exceções previstas na lei. Neste sentido poderá incorrer na violação do direito à não discriminação tutelado pela CDFUE<sup>92</sup>, bem como da CEDH<sup>93</sup>. Por conseguinte, torna-se necessário compreender os indicadores atuais que os serviços de fronteira dispõem para avaliar a possibilidade de migração irregular, os quais sustentam-se pelos padrões comportamentais exteriorizados, bem como outras particularidades como etnia, nacionalidade, roupa e aparência os quais poderão fomentar a definição de perfis<sup>94</sup>.

---

<sup>92</sup> Cfr. o artigo 21.º da CDFUE

<sup>93</sup> Cfr. o artigo n.º 1 do protocolo n.º 12, bem como o artigo 14.º da Convenção Europeia dos Direitos Humanos

<sup>94</sup> Segundo o estudo que levantou esses indicadores aos serviços de fronteira por parte da FRA (2018a), esses indicadores são tipicamente o comportamento durante a confirmação, o comportamento quando abordado, a nacionalidade, a validade dos documentos, o destino, o local de embarcação, a aparência e comportamento dos coviajantes, o histórico criminal quando acessível, as dimensões da bagagem, etnia, tipo de bagagem, roupa utilizada, tipo de companhia aérea, idade e género. Estes indicadores, muitos dos dados ao serem introduzidos em ferramentas para a tomada de decisões, poderá incorrer em consequências negativas, retomando a possibilidade do viés introduzido, focando em indicadores como a etnia ou aparência como diferenciador. Cfr. FRA, 2018a, pp. 69 e ss.

## Capítulo II | Sistemas de Informação no controlo dos fluxos migratórios na UE

### 1. Enquadramento jurídico do controlo dos fluxos migratórios na UE

Para a compreensão detalhada do enquadramento jurídico-europeu relativo às migrações, é cumpre reconhecer a União Europeia como ator político supranacional, dotado de competências partilhadas no desenvolvimento da política comum relativa à imigração<sup>95</sup>. Enquadramos esta política contrasta num espaço de liberdade de circulação interna<sup>96</sup> para os cidadãos da União dentro do espaço Schengen<sup>97</sup>, integrando-o como acervo comunitário, característica da integração económica pela via do mercado comum<sup>98</sup>. De facto, este espaço Schengen é operacionalizado pela Frontex<sup>99</sup>, auxiliado na dimensão técnica pela eu-LISA<sup>100</sup>, bem como diversas instituições, organismos, agências entre outros<sup>101</sup>.

Conjuntamente, a política de imigração enquadra-se no Espaço de Liberdade, Segurança e Justiça<sup>102</sup> do Tratado de Lisboa de 2009, o qual aboliu a estrutura prévia dos três pilares típicos do Tratado de Maastricht de 1993. Neste tratado, encontrávamos a repartição do primeiro pilar da Comunidade Europeia, como segundo pilar, encontrávamos a Política Externa e Segurança Comum (PESC) e, por fim, a cooperação nos domínios da justiça e dos assuntos internos. Hodiernamente, verificamos a fusão

---

<sup>95</sup> Cfr. a alínea j) do n.º 2 do artigo 4º do Tratado sobre o Funcionamento da UE (doravante TFUE).

<sup>96</sup> Este direito, além de ser consagrado nos tratados da União, também é explanado na Diretiva 2004/38/CE, de 29 de abril, com posteriores alterações

<sup>97</sup> Para uma política externa comum relativa ao controlo fronteiriço, fora necessário enveredar pela criação da zona Schengen, esta criada a partir do Acordo Schengen de 1985, comprimindo 30 Estados europeus, pese embora conte com a Suíça, Islândia, Noruega e Liechtenstein. Cfr. a hiperligação <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/borders-and-visas/schengen/docs/c2019-7131-annex.pdf>. No entanto, Estados-Membros como a Bulgária, Croácia, Chipre e Roménia ainda não aplicam totalmente o acervo Schengen

<sup>98</sup> Cfr. a alínea a) do n.º 2 do artigo 20º, com leitura conjunta do n.º 2 do artigo 26º do TFUE, relativa ao direito de circular livremente do cidadão da União, reforçado pela integração económica do mercado comum.

<sup>99</sup> Esta agência cumpre o propósito de promover uma gestão integrada das fronteiras, realizando as tarefas elencadas no n.º 1 do artigo 10º do Regulamento (UE) n.º 2019/1896 de 13 de novembro

<sup>100</sup> Esta é a Agência que gere os sistemas informáticos de grande escala, conforme podemos observar no capítulo II, bem como no artigo 2.º do Regulamento (UE) 2018/1726 de 14 de novembro com progressivas alterações

<sup>101</sup> Cfr. o artigo 68.º do Regulamento (UE) n.º 2019/1896 de 13 de novembro

<sup>102</sup> Consagrado no Título V do TFUE adotado no Tratado de Lisboa de 2009.

do primeiro pilar com o terceiro pilar neste Espaço de Liberdade de Segurança e Justiça<sup>103</sup>.

Cumprir mencionar que a União, tem como orientação estratégica o combate à imigração ilegal, por vezes mesclando com a criminalidade organizada, tomando como exemplificativo o tráfico de seres humanos<sup>104</sup>, face aos quais poderá contar com o apoio dos países terceiros na gestão desses fluxos<sup>105</sup>. Esta é uma das componentes da *Abordagem Global para as Migração e Mobilidade* (GAMM), consolidada em quatro pilares, sendo esses a imigração legal e mobilidade, a imigração irregular<sup>106</sup>, o tráfico de seres humanos e, por fim, a proteção internacional e a política asilo<sup>107</sup>.

Nesta matéria, cumprirá mencionar a responsabilidade da segurança interna recair sobre cada Estado membro da UE<sup>108</sup>, tomando como princípio orientador a solidariedade<sup>109</sup> entre os membros, em particular nas políticas relativas aos controlos fronteiriços, asilo e imigração, permanecendo uma certa discricionariedade<sup>110</sup> que tem

---

<sup>103</sup> Cumprirá mencionar que, esta diluição de áreas tão distintas num único Espaço, poderá ser vista como a posição política da União face ao fenómeno dos fluxos migratórios, combinando os instrumentos de cooperação policial, em matéria penal e civil no combate à migração irregular. Tomemos como ilustrativo o combate à criminalidade transfronteiriça, nomeadamente o tráfico de pessoas, cada vez mais atribui-se o nexos entre imigrantes e o criminoso, pautando o discurso negativo sobre o imigrante, colocando-o como potencial ameaça. Na esteira do mencionado por Moreno-Lax, 2014, *“the connotations of cross-border crime have been imported into the immigration and asylum discourse. Under this view, the foreigner is not only perceived as alien to the free movement project, but is also reified as a potential danger to it.”* Cfr. Moreno-Lax, 2014, pp. 155 e ss.

<sup>104</sup> Cfr. o n.º 1 do artigo 79.º do TFUE

<sup>105</sup> Cfr. o n.º 3 do artigo 79.º do TFUE

<sup>106</sup> Para o entendimento do termo da migração irregular, recorreremos à definição em Triandafyllidou e Bartolini, 2020, recorrendo à compreensão das dinâmicas relativas a este tipo de imigração, repartindo na irregularidade na qualidade de residente – quando este perde o título de residência ou que foram sujeitos à ordem de retorno – e os imigrantes que atravessam as fronteiras internacionais informalmente, sem qualquer tipo de documentação válida. Cfr. Triandafyllidou e Bartolini, 2020, pp. 15

<sup>107</sup> Para uma leitura evolutiva da dimensão estratégica relativa às imigrações na União, recomendamos a leitura: Valente, *et al*, 2016, pp. 39-65

<sup>108</sup> Conforme mencionado no artigo 72.º do TFUE, estando também reforçado no n.º 2 do artigo 4.º do TUE

<sup>109</sup> Como mencionou a Advogada Geral Sharpston, face a ações desembocadas pela Comissão Europeia contra a Polónia (C-715/17), a Hungria (C-718/17) e a República Checa (C-719/17), mencionou este princípio, caracterizando-o da seguinte forma: *“Solidarity is the lifeblood of the European project”* Cfr. Acórdão do Tribunal de Justiça da União Europeia de 2 de abril de 2020, C 715/17, C718/17 e C719/17, Opinião da Advogada Geral Sharpston, parágrafo 253

<sup>110</sup> Esta discricionariedade impactou amplamente o período relativo à crise migratória sentida na União Europeia pela reconhecida desarticulação dos Estados face à partilha equitativa das responsabilidades em acolher imigrantes, em particular a interpretação do artigo 72.º do TFUE na evasão da responsabilidade, colocando inúmeras adversidades à ordem Europeia, bem como os deveres Cfr. Acórdão do TJUE de 2 de abril de 2020, C 715/17, C718/17 e C719/17, Opinião da Advogada Geral Sharpston, parágrafo 212, 219 e 238.

vindo a fomentar a securitização das migrações nalguns Estados, tomando a tónica na soberania<sup>111</sup>.

O entendimento do fenómeno da irregularização dos imigrantes parte das inúmeras políticas que preconizam restringir a entrada e subsequente permanência (Eule, 2019, p. 4) Estas políticas restritivas assumem o propósito da limitação dos canais legais de entrada para efeitos da migração laboral, do aumento dos requisitos para a reunificação familiar, a dificuldade de regularização de imigrantes que entraram pela via informal, os imigrantes que permaneceram mais tempo do devido, perda do estatuto pelo desemprego<sup>112</sup> e, por fim, a rejeição das aplicações a vistos, estatutos, entre outros. O efeito destas políticas poderá não traduzir-se na redução dos fluxos migratórios como intencionado, mas o aumento da movimentação irregular, expondo-se a situações de maior risco

De facto, a União tem um conjunto de agências dedicadas aos controlos fronteiriços (i.e. Frontex<sup>113</sup>), para a formação das autoridades fronteiriças (i.e. CEPOL<sup>114</sup>), para assuntos relativos ao asilo (i.e. EASO<sup>115</sup>), para o combate à migração ilegal e criminalidade organizada (i.e. Europol<sup>116</sup>), coordenação operacional entre os sistemas de informação da UE (i.e. eu-LISA<sup>117</sup>) os serviços diplomáticos especializados

---

<sup>111</sup> Evidentemente, a decisão de quem entra num determinado Estado revive as tendências securitárias, focadas na soberania numa lógica Vestefaliana à segurança interna no espaço europeu Cfr. Shachar, 2019, pp. 93-147

<sup>112</sup> Segundo Eule, *et al*, (2019, p. 98): “*Not able to renew his expired residence permit due to financial struggles, the illegalised migrant had been continuously fined and sanctioned.*” Esta situação aumenta a exposição do migrante a situações de vulnerabilidade, as quais aumentam o fosso da dificuldade de integração nos Estados-Membros da União

<sup>113</sup> Cfr. o Regulamento (UE) 2019/1896 do Parlamento Europeu e do Conselho, de 13 de novembro de 2019, relativo à Guarda Europeia de Fronteiras e Costeira, que revoga os Regulamentos (UE) n.o 1052/2013 e (UE) 2016/1624

<sup>114</sup> Cfr. o Regulamento (UE) 2015/2219 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, sobre a Agência da União Europeia para a Formação Policial (CEPOL) e que substitui e revoga a Decisão 2005/681/JAI do Conselho

<sup>115</sup> Cfr. o Regulamento (UE) n.o 437/2010 do Parlamento Europeu e do Conselho, de 19 de maio de 2010, que altera o Regulamento (CE) n.o 1080/2006 relativo ao Fundo Europeu de Desenvolvimento Regional no que diz respeito à elegibilidade de intervenções habitacionais a favor de comunidades marginalizadas

<sup>116</sup> Cfr. o Regulamento (UE) 2016/794 do Parlamento Europeu e do Conselho, de 11 de maio de 2016, que cria a Agência da União Europeia para a Cooperação Policial (Europol) e que substitui e revoga as Decisões 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI e 2009/968/JAI do Conselho

<sup>117</sup> Cfr. o Regulamento (UE) 2018/1726 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo à Agência da União Europeia para a Gestão Operacional de Sistemas Informáticos de Grande Escala no Espaço de Liberdade, Segurança e Justiça (eu-LISA), que altera o Regulamento (CE) n.o 1987/2006 e a Decisão 2007/533/JAI do Conselho, e que revoga o Regulamento (UE) n.o 1077/2011, com posteriores alterações

nos assuntos da cooperação externa (e.g. EEAS), sem prejuízo de outras agências com relevância em temáticas específicas no controlo fronteiriço.

Para o sucesso do controlo fronteiriço articulado com os sistemas de informação da UE, a Agência Europeia da Guarda de Fronteiras e Costeira (Frontex) assume a função primordial de promover a gestão integrada das fronteiras<sup>118</sup> na qualidade de ponto de contacto central para a coordenação do controlo fronteiriço, o qual congrega os controlos de fronteira e a vigilância das fronteiras na aceção do CFS<sup>119</sup>, harmonizando os padrões de atuação das guardas de fronteira europeia dos Estados-Membros da UE.

O fundamento subjacente à criação da Frontex<sup>120</sup>, conforme nos aponta Mitsilegas (2015), partiu da desconfiança da U.E nos países de Leste e Centro que aderiram à União, em garantir a segurança das próprias fronteiras. Esta é uma situação de delegação em áreas tradicionalmente conexas com a soberania do Estado<sup>121</sup>, em particular no *ius includendi* e o *ius excluendi*.

Concomitantemente, dentro de um esquema para promover a interoperabilidade entre os diversos sistemas da UE, compete à Agência Europeia para a Gestão Operacional de Sistemas Informáticos de Grande Escala no Espaço de Liberdade, Segurança e Justiça (eu-LISA) gerir os repositórios centrais para efeitos de reporte e estatístico, alimentado pelas diversas bases de dados da União<sup>122</sup>. Esta agência assume as seguintes competências

De facto, a abolição dos controlos nas fronteiras internas<sup>123</sup> fora compensada com o incremento de controlos externos para garantir a segurança dentro do espaço

---

<sup>118</sup> Com a base jurídica sustentada no artigo 77.º do TFUE, bem como o próprio artigo 3.º do Regulamento (UE) n.º 2019/1896.

<sup>119</sup> Em particular, com a leitura conjugada do n.º 10, 11 e 12 do artigo 2.º do CFS, conjuntamente com n.º 3, 4, 5 e 6 do artigo 2.º do Regulamento (UE) n.º 2019/1896.

<sup>120</sup> Com as competências elencadas no artigo 3.º do Regulamento (UE) n.º 2019/1896:

<sup>121</sup> Esta relação entre os Estados membros e a União Europeia, em matéria das migrações, é de complexa articulação, como nos aponta Mitsilegas (2015), “[t]he shared competence between Member States and the European Union in the field of migration law raises complex issues with regard to the degree of sovereignty or discretion left to Member States when they legislate on irregular migration and when they promote legislative choices resulting in the criminalisation of migration.”.

<sup>122</sup> Com as competências elencadas no artigo 10.º do Regulamento (UE) 2018/1726:

<sup>123</sup> Contudo o CFS prevê a possibilidade da reintrodução de fronteiras a nível interno, nos casos previstos do artigo 25.º e ss. do Regulamento (UE) n.º 2016/399, com posteriores alterações.

Schengen<sup>124</sup>, através de regras comuns harmonizadas, entre os Estados aderente ao Acordo Schengen. Relativamente aos instrumentos para o controlo dos fluxos migratórios, é relevante mencionar o Código das Fronteiras Schengen (CFS), onde é delineado as condições de entrada, recusa, a duração das estadias, entre outros.

## 2. As tipologias do controlo dos fluxos migratórios na UE

Nesta esteira, a gestão de fluxos migratórios na UE, é indispensável enquadrar este processo nas tendências atuais do controlo migratório, sendo essas auxiliadas por ferramentas tecnológicas integradas nos sistemas de informação da UE para o controlo dos fluxos migratórios. Desta feita, como a doutrina dedica aos estudos da vigilância fronteiriça, apontaram que a fronteira se encontra em todo lado, principalmente facilitado pelo uso das tecnologias, sem prejuízo da dimensão mental, física dos “muros” erguidos face à entrada dos imigrantes<sup>125</sup>.

Este modelo de fortalecimento do controlo fronteiriço tem vindo cada vez mais ser relevante para os Estados<sup>126</sup>. É por demais evidente a correlação deste aumento do mercado de sistemas de segurança pelo investimento cumulativo dos diversos Estados, em particular na União, tomando como ilustrativo o orçamento dedicado para a Frontex ter aumentado, estimando que o mesmo orçamento entre 2020 e 2021 passe de 346

---

<sup>124</sup> Para o entendimento dos controlos efetuados, recomendamos a leitura do CFS, em particular o anexo VI do Regulamento (UE) n.º 2016/399, onde refere os procedimentos a serem adotados, sempre em vista o respeito aos direitos fundamentais.

<sup>125</sup> Estes muros devem ser lidos como obstáculos à migração, conforme mencionado no relatório promovido pelo *Centre Delàs d'Estudis per la Pau*, sediado em Barcelona, no qual menciona os “muros” mentais como o discurso extremista e xenófobo contra os fluxos migratórios, bem como a violência praticada sobre as minorias, os muros físicos que foram erguidos após a queda do muro de Berlim, na dimensão terrestre, perto de 1000km foram erguidos no espaço Schengen, o equivalente a 6 muros de Berlim, bem como os muros marítimos e, por fim, relevante para o objeto do presente estudo, os “muros” virtuais apresentando por via de ferramentas de vigilância e monitorização com base em conjuntos de dados enormes. Cfr. Benedicto e Brunet, 2018, pp. 1-58; Cfr. Shachar, 2019, pp 93-147

<sup>126</sup> Inclusive, de acordo com a Markets and Markets, 2016, é expetável que o mercado dos sistemas de segurança das fronteiras ascenda aos \$52 milhares de milhões de dólares americanos até 2022 Cfr. a hiperligação [https://www.marketsandmarkets.com/Market-Reports/border-security-system-market-103309188.html?gclid=Cj0KCOiAyKrxBRDHARIsAKCzn8xFhcNkQ\\_Fq2wEecsk4scy7s5qouZpWVRDNwcUEyMeH7Ub24DmFWqAaAgPdEALw\\_wcB](https://www.marketsandmarkets.com/Market-Reports/border-security-system-market-103309188.html?gclid=Cj0KCOiAyKrxBRDHARIsAKCzn8xFhcNkQ_Fq2wEecsk4scy7s5qouZpWVRDNwcUEyMeH7Ub24DmFWqAaAgPdEALw_wcB), consultado a 17 de outubro de 2020

milhões de euros para cerca de mil milhões de euros<sup>127</sup>. Este controlo contempla, como já mencionamos previamente todo o percurso do imigrante, desde o Estado de origem, passando pelos Estados de trânsito até chegar à União, podendo deslocar-se posteriormente dentro da União, sendo controlados em cada fase, cada via de deslocação que optam.

Relativamente a estas tendências, deparamo-nos com os “muros” mentais marcados pelo fenómeno da ilegalização dos imigrantes associado à Crimigração<sup>128</sup>, fomentando o uso de mecanismos coercivos e, em grosso modo, intromissivos na vida privada, intimamente relacionados os sistemas de informação da UE, sendo necessário criar o equilíbrio nas soluções, respeitando a posição do migrante. Em parte, esta dimensão é por vezes associada à proliferação das notícias falsas, podendo afetar a decisão política face à orientação dada à política migratória (Omezi, 2020, p. 234 e ss.)

De facto, a doutrina, reconhece o uso da lei criminal associado ao enquadramento regulador dos imigrantes, bem como o nexos entre a migração e a ilegalização apontada neste processo de securitização das migrações<sup>129</sup>, nomeadamente na junção dos fluxos migratórios à criminalidade organizada<sup>130</sup>, em particular o tráfico de pessoas. Esta

---

<sup>127</sup> Em particular a Frontex ao ter sido expandida para Agência Europeia da Guarda de Fronteiras e Costeira em 2016, incrementando os poderes atribuídos, integrando a cooperação com países terceiros para controlar os fluxos migratórios, foi aumentada o orçamento, bem como a capacidade operacional. Cfr. Akkerman, 2018, pp. 22 e ss.

<sup>128</sup> Para o entendimento deste conceito, recorremos à definição de Mitsilegas, (2015): “*The criminalisation of migration(...) understood as the threefold process whereby migration management takes place via the adoption of substantive criminal law, via recourse to traditional criminal law enforcement mechanisms including surveillance and detention, as well as via the development of mechanisms of prevention and pre-emption.*”. Conjuntamente, esta abordagem de mecanismos jurídico-penais face à gestão dos fluxos migratórios no espaço da União, é necessário mencionar o impacto no discurso político, onde a conotação de crime organizado fora transposto para o discurso das migrações e Asilo, recorrendo às palavras de Moreno-Lax, 2014. Cfr. Mitsilegas, 2015, pp. 1-110.; Cfr. Moreno-Lax, 2014, pp. 146-167

<sup>129</sup> Esta securitização tem a sua emergência, em parte partindo do discurso político, este cada vez mais aponta o imigrantes como a ameaça e, como tal, são desencadeados mecanismos de deportação e detenção face à pressão da opinião pública Cfr. Karamanidou, 2015, pp. 37-61

<sup>130</sup> Como é referido na doutrina, o conceito de “criminalidade organizada” é amplamente discutido na dogmática jurídica, bem como na criminologia, não havendo consenso nesta definição, havendo diversas organizações internacionais com definições distintas, conforme podemos ver em Manuel Anes, J., 2015. Contudo, é reconhecido que se trata de estruturas organizadas com estabilidade ao longo dos tempos, com o objetivo de enriquecimento ilícito, tipicamente através de prestação de serviços e bens de cariz ilícito. Cfr. Anes, 2015, pp. 89-94. Neste sentido, também os sistemas de informação da UE tem expandido o objeto inicial para o controlo dos fluxos migratórios, implicando um controlo contra o terrorismo e a criminalidade organizada, Cfr. FRA, 2018, pp. 114 e ss.

criminalização é entendida na dimensão substantiva penal<sup>131</sup> para regular a migração, aglutinando o uso de mecanismos intrusivos de vigilância e detenção.

Neste sentido, é relevante mencionar a tutela deste direito no caso particular do controlo dentro do espaço Schengen, em particular em Espanha, quando uma mulher é abordada pelas autoridades locais, impedindo que esta circulasse em função da sua tonalidade. Segundo a decisão proferida pelo TEDH, no caso *Rosalind Williams Lecraft v. Espanha*<sup>132</sup>, decidiu que as características das pessoas não podem ser indicativas da possibilidade da situação irregular.

Dessa feita, as autoridades ao realizarem este tipo de controlo para interesse público, a prevenção do crime e monitorização da migração irregular, necessitam de considerar na sua conduta os padrões objetivos para abordar o indivíduo, não em padrões subjetivos. Esta situação, na dimensão do muro “mental” criado contra os imigrantes, deve ser considerado principalmente na definição de perfis formulada pelas autoridades, bem como na tomada de decisões com base em algoritmos.

*Será admissível as autoridades intervirem contra suspeitos com base em algoritmos preditivos, pontuados com taxa de eficácia rondando os 80%, sem infringir os direitos, liberdades e garantias deste? Se sim, quais são as limitações dessa intervenção?* (Macnish, [et al.], 2020)<sup>133</sup>

Este fenómeno convive com os “muros” tecnológicos, sendo essas ferramentas tecnológicas que, por um lado, incrementam a proteção dos imigrantes através da vigilância, tomando como exemplificativo a vigilância marítima onde é decisivo estas tecnologias, sob prejuízo das consequências nefastas como a situação em Lampedusa, por outro lado, subsiste o controlo dos imigrantes através da monitorização e vigilância. O nexo entre a tecnologias e discriminação é cada mais proeminente (Molnar, 2020)

---

<sup>131</sup> De facto, na esteira de Bosworth, 2018 (apud Eule, 2019, p. 103): “*The police officer thus ‘tinkers’ with the tools granted by migration law and those of criminal justice: in the first case, they use criminal justice procedures to achieve migration control-related ends, while in the second case, migration control is used as a means to enforce criminal law*”.

<sup>132</sup> Cfr. FRA, 2018b, p. 29

<sup>133</sup> Poderemos aqui ponderar se haverá um direito à limitação do tratamento dos dados amplo quando relativo a modelos com taxas inferiores ao estabelecido como padrão, nos termos do artigo 18.º do RGPD

Estes sistemas de informação são transversais no controlo dos fluxos migratórios, podendo ser repartido, mesma esteira da doutrina<sup>134</sup>, na dimensão da externalização da responsabilidade, na securitização assente no controlo intrafronteiriço e no controlo extrafronteiriço<sup>135</sup>, por fim, na privatização do risco para o setor privado. Estas dimensões estão intrinsecamente ligadas, como veremos posteriormente ao escrutinar cada tipologia do controlo migratório na UE. Evidentemente, o controlo dos fluxos migratórios compreende a transformação digital acarretada pela sociedade digital, onde os instrumentos tecnológicos auxiliam a ação operacional deste controlo.

Contudo, para o efeito estritamente do controlo fronteiriço e a alocação em migração<sup>136</sup>, cumpre mencionar a previsão no quadro financeiro plurianual entre 2021-2027, do aumento de 160%, e, caso comparemos o orçamento da União Europeia (38\$ mil milhões de dólares americanos) para o controlo fronteiriço diluídos entre 2021-2027. Este será considerável, quando comparado com o orçamento dos EUA atual (32\$ mil milhões de dólares americanos em 2020).

Este orçamento é repartido pelo Fundo para o Asilo, a Migração e a Integração (FAMI)<sup>137</sup>, para as agências descentralizadas<sup>138</sup>, em particular a Frontex, o Fundo integrado, Fundo para a Segurança Interna: Fronteiras e Vistos<sup>139</sup> (FSI), o Instrumento relativo à prestação de apoio de emergência na União<sup>140</sup>. No total, verificamos a alocação do orçamento entre 2014-2020 de 13,5€ mil milhões de euros havendo um

---

<sup>134</sup> Cfr. Spijkerboer, 2018

<sup>135</sup> Como defendido pela doutrina, há evidentemente uma estratégia de securitização assente no *outsourcing* do controlo fronteiriço a países terceiros, tomando os países de trânsito como agentes responsáveis para o controlo dos fluxos migratórios, bem como o *insourcing* através do fortalecimento do controlo interno, visando a deportação, a vigilância destes. Cfr. De Genova, 2017, pp. 102-130

<sup>136</sup> No âmbito do Instrumento de Flexibilidade prevista nas várias decisões anuais para o efeito dos controlos migratórios, asilo, sem prejuízo das situações de contingência,

<sup>137</sup> Cfr o Regulamento (UE) n.º 516/2014, com posteriores alterações

<sup>138</sup> Por tipo de sistema de informação, foi gasto no SIS cerca de 91€ milhões de euros, no VIS cerca de 81€ milhões de euros, na Eurodac cerca de 1€ milhão, na Frontex cerca de 1,6€ mil milhões de euros (aumento de 161% comparativamente ao previsto inicialmente) e, por fim a EASO, cerca de 456€ milhões de euros (aumento de 318% comparativo ao previsto inicialmente) Cfr. D'Alfonso, 2019, p. 25.

<sup>139</sup> Cfr o Regulamento (UE) n.º 515/2014, com posteriores alterações

<sup>140</sup> Cfr o Regulamento (UE) 2016/369,

aumento de praticamente o dobro do valor estimado inicialmente de 7,8€ mil milhões de euros (D'Alfonso, 2019, p. 25).

### 2.1. Securitização

No que concerne à Securitização, este é o processo de transformar um determinado tópico como assunto da segurança, repercutindo efeitos no discurso político sobre o imigrante, em particular, através donexo entre o terrorismo e migração, resultando no incremento dos controlos fronteiriços<sup>141</sup>. Nesse sentido, verificamos políticas de asilo e migratórios nos Estados-Membros cada vez mais restritivas, conforme mencionamos.

Evidentemente, este processo transversal é sentido no robustecimento do controlo dos fluxos migratórios, numa dimensão extra-UE, onde os Estados terceiros colaboram a participar na securitização, deve ser compreendida na dimensão externa, procurando evitar a entrada dos imigrantes dentro da União, através de missões<sup>142</sup> conjuntas no âmbito da Política Comum de Segurança e Defesa (PCSD)<sup>143</sup>, bem como na dimensão interna, onde é fortalecida a vigilância interna, principalmente através do controlo justaposto.

Nesta dimensão, a securitização está subjacente aos mecanismos de policiamento, principalmente pela via marítima, reconhecendo assim que a maioria dos fluxos migratórios decorrem por esta via.<sup>144</sup> Por este fundamento, a vigilância marítima

---

<sup>141</sup> Cfr. Haves, 2017, pp. 183 e ss.

<sup>142</sup> Tomemos o exemplo do uso de *drones* miliares para vigiar as fronteiras terrestres e marítimas, reconhecendo a tendência do “*usage of military, or quasi-military, autonomous technology bolsters the nexus between immigration, national security, and the increasing push toward the criminalization of migration.*” (Molnar, 2020, p. 776)

<sup>143</sup> Como estipulado no TUE, nos artigos 42.º a 46.º do capítulo 2, da secção 2 do título V, intitulado por “Disposições relativas à política comum de segurança e defesa”, esta política terá um entrosamento cada vez maior, não somente pelo enquadramento nos tratados da segurança como componente do próprio espaço de liberdade, segurança e justiça, bem como o conjunto de missões alavancadas no espaço do mediterrâneo, como a operação Sophia (EUNAVFOR MED) com implicações no controlo migratório, a EUCAP Sahel Niger cujo mandato está assignado primariamente ao combate à migração irregular, entre outras missões como a EUBAM Libya, transcendendo a preocupação com a migração irregular para a preocupação com a criminalidade organizada. Tal não deve ser confundido com a marca temporal da crise dos refugiados, pois muitas destas missões continuam a operar, tomando como ilustrativo a operação Sophia e a EUCAP Sahel Niger, entre outras.

<sup>144</sup> Como podemos deparar no relatório da IOM de 2020, relativo aos fluxos migratórios decorridos no ano anterior, ao longo do mediterrâneo, cerca de 104 mil imigrantes chegaram via marítima, contabilizando somente 25 mil imigrantes pela via terrestre. Cfr. Mixed Migration Flows in the Mediterranean, 2020, disponível na hiperligação

é escrupulosamente seguida para interceptar as embarcações destes imigrantes em alto-mar<sup>145</sup>, comprometendo-se com a ação de busca e salvamento<sup>146</sup>, bem como a cooperação com embarcações dos países terceiros.

Simultaneamente, este modelo atual carece de equilíbrio, pois os Estados poderão abster-se de vigiar os fluxos migratórios, caso a interceção marítima imputa responsabilidades acrescidas. Esta dimensão externa, estende-se além das fronteiras marítimas até outros territórios, principalmente nos enclaves como Ceuta e Melilla, situados em Marrocos, bem como as regiões insulares como a Ilha das Canárias<sup>147</sup>. Em grande medida, as parcerias celebradas com países terceiros visam essencialmente corresponder às rotas tidas pelos imigrantes para chegar à União

---

<https://migration.iom.int/reports/europe-%E2%80%94-mixed-migration-flows-europe-monthly-overview-december-2019>, consultado a 28/07/2020

<sup>145</sup> Na mesma esteira do mencionado por Mitsilegas, 2010; pp. 12 e ss., trata-se de uma das diversas formas de controlo de pré-embarcação conforme mencionado pela doutrina, em particular, atendendo ao desfasamento jurisdicional premente nas regras sobre os usos dos mares, conforme mencionado na Convenção das Nações Unidas sobre o Direito do Mar (CNUDM), concluída em 1982 e em vigor desde 1994, nos termos do artigo 89.º, em que é entendido que nenhum Estado poderá apropriar-se legitimamente de mares territoriais em alto mar à soberania destes, vigorando o princípio das liberdade de navegação e a abertura dos espaços marítimos, defendido por Hugo Grócio no final do século XV, permanecendo hodiernamente.

<sup>146</sup> Cfr. De Genova, 2017; pp. 98 e ss

<sup>147</sup> Aliás, a parte substancial das rotas migratórias passam substancialmente pela procura dos enclaves a regiões insulares posicionados geograficamente perto da costa africana, bem como pela via terrestre tipicamente através da Turquia. Cumpre mencionar que as rotas principais são a do Mediterrâneo Central, a do Mediterrâneo Oriental, Balcãs Ocidentais e o Mediterrâneo Ocidental, sem prejuízo de outras rotas (e.g. Rota Circular, África Ocidental e outras) Cfr. a hiperligação [https://what-europe-does-for-me.eu/data/pdf/focus/focus04\\_pt.pdf](https://what-europe-does-for-me.eu/data/pdf/focus/focus04_pt.pdf)

## 2.2. Privatização

Este controlo migratório, conforme mencionado previamente, também é sentido em diversos países, onde os agentes que operam nos serviços de fronteiras decidem a entrada ou recusa dos imigrantes<sup>148</sup>, conjuntamente com os agentes privados como as transportadoras férreas, marítimas, entre outras, podendo ser imputado responsabilidade civil em determinados casos. Numa dimensão da privatização *de facto*, tal é evidente na cooperação com as transportadoras em diversas óticas, em concordância com os instrumentos de Direito Internacional<sup>149</sup>.

Como tendência atual, o legislador europeu tem imputado a responsabilidade, em matéria de controlo dos fluxos migratórios, ao setor privado, em particular as transportadoras<sup>150</sup> com o intuito de privatizar o risco<sup>151</sup>. É de referir a constante delegação deste controlo para o setor privado, em particular às transportadoras aéreas.

---

<sup>148</sup> A legitimidade desta atuação poderá ser justificada nos termos do artigo 13.º do CFS, imanente do Regulamento 2016/399/UE prossequindo a vigilância e a implementação de medidas para recusar a entrada e, como tal, deverá ser detido e ficar sujeito a procedimento por força da diretiva do retorno, nos termos do n.º 1 do mesmo artigo.

<sup>149</sup> Em particular, o Protocolo Adicional contra o Tráfico Ilícito de Imigrantes por Via Terrestre, Marítima e Aérea à Convenção das Nações Unidas contra a Criminalidade Organizada Transnacional, de 2000, imputa as transportadoras comerciais, nos termos do n.º 3 do artigo 11.º, a “verificar se todos os passageiros são portadores dos documentos de viagem exigidos para a entrada no Estado de acolhimento.”

<sup>150</sup> Neste sentido, o enquadramento restritivo para o controlo migratório incrementa as obrigações às transportadoras, nos termos da Diretiva 2001/51/CE, do Conselho, de 28 de Junho de 2001, através de adoção de medidas necessárias, como reencaminhar os nacionais de países terceiros a quem tenham sido recusada a entrada no país (artigo 3.º), sob prejuízo de serem sancionados caso não o façam (artigo 4.º), sem prejuízo da possibilidade de serem ainda sancionados cumulativamente pelos Estados-Membros (artigo 5.º). Conjuntamente, considera-se a Diretiva n.º 2004/82/CE, obrigando as transportadoras à comunicação dos dados com a tutela preventiva no espaço europeu, *grosso modo*, encontrados no passaporte, nos termos do n.º 2 do artigo 3.º da Diretiva, sob prejuízo da aplicação de sanções:

- I. O número e o tipo do documento de viagem utilizado,
- II. A nacionalidade,
- III. O nome completo,
- IV. A data de nascimento,
- V. O ponto de passagem da fronteira à entrada no território dos Estados-Membros,
- VI. O código do transporte,
- VII. A hora de partida e de chegada do transporte,
- VIII. O número total de passageiros incluídos nesse transporte,
- IX. O ponto inicial de embarque.

<sup>151</sup> Esta responsabilização incide principalmente na disposição no plasmado na alínea b) do artigo 23.º do CFS, imanente do Regulamento 2016/399/UE, do Conselho, de 28 de Junho de 2001 inclusive referido desde a Convenção de aplicação do Acordo Schengen de 1985, prevendo a cooperação das transportadoras com o poder público, nomeadamente no artigo 26.º do mesmo acordo, inserido no capítulo 6, intitulado por medidas de acompanhamento. Para um esclarecimento das responsabilidades das transportadoras, é recomendado confrontar com esta leitura, Cfr. Mitsilegas, 2015, pp. 23 e ss.;

Em particular, através do sistema de registo de identificação do passageiro (do inglês *Passenger Name Record* (doravante PNR)).

Como tal, a título exemplificativo, no enquadramento espanhol, as obrigações das transportadoras para o propósito do combate à migração ilegal<sup>152</sup> são diversas, entre as quais, a obrigação controlas os bilhetes de volta não utilizados, devendo para o efeito reportar no prazo de 48h às autoridades espanholas.

Esta atuação subsidiária aos serviços de fronteira é visível no caso ilustrativo do Acordo reconhecido do *Le Touquet*, de 2003<sup>153</sup>, celebrado entre a Bélgica, França e Reino Unido focado no controlo de determinadas rotas previamente ao embarque, principalmente a rota Calais-Dover<sup>154</sup>, com a interação do setor privado neste processo securitário.

### 2.3. Externalização

Nesta dimensão, é notória a presença do controlo dos fluxos migratórios por parte da União disseminada por diversas zonas geográficas, através dos variados instrumentos de cooperação, os quais mencionaremos. Por conseguinte, esta externalização visa principalmente externalizar a responsabilidade por parte da UE aos países vizinhos<sup>155</sup>, apartando a aplicação material do Direito Europeu. Esta tendência da externalização

---

<sup>152</sup> Prevista no artigo 66.º da Ley Orgánica 4/2000, de 11 de janeiro, sobre direitos e liberdades dos estrangeiros em Espanha e a sua integração social, com posteriores alterações

<sup>153</sup> Este controlo justaposto remonta aos anos 90 do século transato, tendo originalmente sido fundado através do protocolo Sangatte, assinado em 1994, com vista em acompanhar o procedimento de entradas e saídas na rota do canal da Mancha e, por conseguinte, agilizar o processo. Deve ser mencionado que o acordo de Touquet entra em vigor após a produção legislativa do reconhecido *Nationality, Immigration and Asylum Act 2002*, no qual delinea os controlos justapostos nos termos do artigo 141.º, intitulado por *EEA ports: juxtaposed controls*. Cfr. Bosworth, 2016, disponível na hiperligação <https://www.law.ox.ac.uk/research-subject-groups/centre-criminology/centreborder-criminologies/blog/2016/02/juxtaposed-border>.

<sup>154</sup> É de reconhecer que este acordo do *Le Touquet* decorre posteriormente da ação levantada por um cidadão britânico nos tribunais britânicos em 1994, chamado Naraine, de origem da Guiana situada na América Latina. Esta ação sucedeu-se posteriormente à recusa por parte da Hoverspeed, a recusa deste cidadão, seguindo as indicações explanadas pelas autoridades francesas. Neste sentido, em 1999 a argumentação do coletivo de juizes fora favorável à empresa que seguia as instruções e requisitos legais previstos, os quais exigiam a posse do visto, mesmo possuindo o passaporte de visitante britânico. Cfr. Mitsilegas, 2010, pp. 12 e ss.

<sup>155</sup> Para uma compreensão desta particularidade da externalização, é recomendada a leitura de Spijkerboer, 2018, pp. 452-469. Aliás, este autor defende que o objeto desta externalização não visa meramente a expulsão do imigrantes do território Europeu, mas visa evadir a responsabilidade do território europeu.

também decorre relativamente aos dados que são transferidos para os países terceiros com estes sistemas de informação da UE de forma distinta<sup>156</sup>, devendo respeitar os princípios do RGPD, submetendo a transferência as garantias adequadas<sup>157</sup>

Tomemos como elucidativo o constante robustecimento dos muros circundantes aos enclaves espanhóis de Ceuta e Melila<sup>158</sup> situados na costa norte africana, como também o caso paradigmático do patrulhamento pela marinha da Líbia com atuação estendida no mediterrâneo.<sup>159</sup> Esta celebrou o Tratado de amizade, parceria e cooperação com a Líbia, onde facultou embarcações para monitorizar os 2000 km da zona costeira desta, coordenada com a União, sendo relevante citar que “[a]voiding legal responsibility through orchestration is not the same as breaching law in pursuit of self-interested policies” (Müller, [et al.], 2020)

Ainda na mesma esteira, fora também decidido no Acordo em Malta de 2017 que a *“Libya receives training as well as funding from the EU. For example, FRONTEX has assisted the Libyan Coast Guard in the reinforcement of Libya's naval borders and equipped maritime forces to obstruct migrant-smuggling boats. Under the MoU the Libyan coastguard is entitled to intercept boats bound for Italy and return all passengers to disembarkation zones in Libya (...). Long-term detention is a routine solution in*

---

<sup>156</sup> Conforme mencionado pela FRA, 2017, p. 27: *“For example, the proposed ETIAS Regulation (Article 55) contains an explicit prohibition for EU Member States to share the information contained therein with third countries, international organisations and private entities (with the exception of Interpol). In contrast, the proposed EES Regulation (Article 38 (2), the SIS II proposal on return (Article 10), the VIS Regulation (Article 31) and the proposal for a revision of the Eurodac Regulation (Article 38) allow for sharing personal data with third countries to identify a third-country national for the purpose of return, albeit with some exceptions. To facilitate police cooperation, a Member State may 66 Ibid, paras 42 and 43. also under certain conditions share SIS II data through Europol (Article 41), Eurojust (Article 42) and Interpol (Article 55), according to Council Decision 2007/533/JAF”*

<sup>157</sup> Cfr. o artigo 46.º do RGPD

<sup>158</sup> É necessário ainda compreender os limites delineados pela recente jurisprudência, em particular admitindo o *refoulement* pelas autoridades espanholas no enclave de Melila, reconhecendo que a entrada dentro das vedações constituía uma violação de ordens diretas, bem como de tratados internacionais, sendo uma posição amplamente contestada pelo Ombudsman de Espanha, Cfr. Acórdão do TEDH de 13 de fevereiro, *N.D. e N.T. contra Espanha*, aplicações n.º 8675/15 e 8697/15

<sup>159</sup> Esta fenómeno assume o propósito de controlar os fluxos migratórios, incidindo a responsabilidade extraterritorial na Líbia para intercepar os imigrantes na zona SAR, evitando o desrespeito ao princípio do *non-refoulement*, reconhecido o estatuto de norma *ius cogens*, visto que estas operações de controlo fronteiriço e da área de busca e salvamento trata-se de direitos e deveres provenientes do direito internacional assentes no Estado soberano da Líbia, sem que acarreta qualquer responsabilidade aos Estados europeus, em particular Itália pela proximidade geográfica com este. Para uma análise detalhada deste policiamento, recomendamos a leitura de Spijkerboer, 2018, pp. 452-459; Cfr. Maccanico, 2020, pp. 1-13; Cfr. Müller e Slominski, 2020, pp. 1-20; Pijnenburg, 2020, pp. 306-332

*Libya, and massive financial support has been channelled to Libya's detention infrastructure” (Palm, 2020, pp. 13)*

Simultaneamente, a União Europeia dispõe de um conjunto alargado de instrumentos para a cooperação com terceiros, conformando com os objetivos delineados na GAMM na dimensão da externalização, contando com fundos, bem como através do diálogo com os países terceiros<sup>160</sup>, bem como fundos dedicados para estimular parcerias.

Contando com os seguintes instrumentos financeiros para a cooperação externa para efeito das migrações<sup>161</sup>, totaliza no período de 2014-2020 cerca de 120 mil milhões de euros do orçamento para o fenómeno migratório, incluindo os apoios ao desenvolvimento como forma de colmatar as *root causes*<sup>162</sup> dos migrantes deslocarem-se, a cooperação no período de crise dos refugiados, como é o caso exemplificativo do Mecanismo em favor aos Refugiados na Turquia, bem como os instrumentos de pré-adesão na transportação do acervo comunitário, mencionado no Serviço de Estudos do Parlamento Europeu, Apap, *[et al.]*, (2019, p. 10-14):

- I. Fundo Europeu de Desenvolvimento
- II. Instrumento de Cooperação para o Desenvolvimento
- III. Instrumento Europeu de Vizinhança
- IV. Fundo Madad
- V. Fundo Fiduciário Bêkou

---

<sup>160</sup> Embora estes acordos não sejam conhecidos desta forma, o intuito generalizado trata-se de evitar a migração irregular, estabelecendo cooperação com países terceiros, conforme mencionado no estudo do comité LIBE em 2015, “[e]astern countries are involved in the Prague Process (Western Balkans, Central Asia, South Caucasus countries and Eastern Europe, except Belarus), the Budapest Process and its Silk Routes Partnership for Migration (Western Balkans, Central Asia, South Caucasus and Eastern Europe) and the Eastern Partnership Panel on Migration and Asylum (South Caucasus and Eastern Europe, except Russia). Southern Mediterranean and Sub-Saharan countries participate in the Rabat Process (North, West and Central Africa), the Africa-EU Migration and Mobility Dialogue (African countries, except Morocco), and the ACP-EU Migration Dialogue (African, Caribbean and Pacific countries), while the Khartoum Process comprises Eastern African countries.” Cfr. Andrade, 2015, pp. 23 e ss.

<sup>161</sup> É necessário mencionar que existem mais de 30 instrumentos legais celebrados para o efeito de apoio técnico e financeiro

<sup>162</sup> As *root causes* são entendidas pelos fundamentos que leva o imigrante a deslocar-se do território originário, quer seja pela dimensão da instabilidade política (e.g. Guerra, perseguição), a dimensão da instabilidade económica (i.e. mercado de trabalho com excesso de mão-de-obra), a dimensão social (e.g. a reunificação familiar, sociedade com valores distintos, sem prejuízo da dimensão individual, por diversas razões poderá levar a optar por migrar na procurar de melhores condições.

- VI. Fundo Fiduciário de emergência da UE para África
- VII. Instrumento de Assistência de Pré-Adesão II
- VIII. Mecanismo em Favor dos Refugiados na Turquia
- IX. Fundo Europeu para o Desenvolvimento Sustentável
- X. Conferência de Londres de 2016
- XI. Conferência de Bruxelas e Conferência de Bruxelas II

Concomitantemente, é de referir no processo de externalização da responsabilidade sobre a gestão dos fluxos migratórios, em particular, a Política de vizinhança da U.E<sup>163</sup>, tendo sido operacionalizada como uma das três vertentes desta ação externa, juntamente com a Política de Alargamento e a Política Europeia de Segurança e Defesa<sup>164</sup>, no âmbito da Política Externa, encontrando como fundamento legal nos Tratados da União<sup>165</sup>.

Simultaneamente, esta externalização materializa-se principalmente nos Acordos de Readmissão com países terceiros da União Europeia, visando a cooperação com países terceiros para a prossecução principalmente da Diretiva do Retorno<sup>166</sup>. Por sua vez, estes Acordos visam assegurar esquemas de retorno assistido dos imigrantes em situação irregular para o país terceiro considerando seguro<sup>167</sup>, assumindo como instrumento de certa relevância para o controlo migratório<sup>168</sup>, tomando como elucidativo os dados estatísticos apresentados no sítio web da Comissão Europeia<sup>169</sup>, cada ano entre 400.000 e 500.000 imigrantes são ordenados a sair da União.

---

<sup>163</sup> Cfr. Carreto, 2018, pp. 81-101

<sup>164</sup> Existem inúmeros caso destas parcerias para efeito de combate à migração irregular, bem como a procura da estabilização de uma determinada região: “*This is true of the JHA dialogues based on the Stabilisation and Association agreements (SAAs) with Albania, Bosnia-Herzegovina, Montenegro, Serbia, FYROM and Kosovo; with Turkey on the basis of the Ankara Association Agreement; and the JLS Subcommittee of the Partnership and Cooperation agreements (PCAs) with Armenia, Azerbaijan, Georgia, Moldova and Ukraine (...) it was finally established under the umbrella of the EU-Russia PCA (...). Concerning the Southern Mediterranean countries, the Social affairs and Migration Working Group created under the umbrella of the Euro-Mediterranean Association agreements with Morocco, Tunisia [, Líbano] and Jordan meets once a year*”. LIBE, 2015, pp. 1-148

<sup>165</sup> Cfr. o artigo 8.º do TUE

<sup>166</sup> Cfr. Diretiva n.º 2008/115/CE de 16 de dezembro

<sup>167</sup> Conforme refere-nos Besharov, 2018, estes acordos não preveem mecanismos de monitorização, supervisão ou escrutínio na forma como os imigrantes serão tratados quando chegarem ao país destinado nesse Acordo.

<sup>168</sup> Existem diversos países com Acordos de readmissão com a União Europeia, nomeadamente 17 Estados terceiros colaborando nesta dimensão da externalização europeia

<sup>169</sup> Cfr. a hiperligação [https://ec.europa.eu/home-affairs/what-we-do/policies/irregular-migration-return-policy/return-readmission\\_en](https://ec.europa.eu/home-affairs/what-we-do/policies/irregular-migration-return-policy/return-readmission_en) sítio web consultado a 26/07/2020

Erguem-se problemáticas da responsabilidade assentes na procura da evasão desta por parte dos Estados da U.E, mas, contrariando estas vontades, o Tribunal Europeu dos Direitos Humanos (TEDH) em inúmeras decisões, verteu a sua posição adjudicando a responsabilização dos Estados da U.E, na circunstância de atuar externamente, nos termos do artigo 1.º da CEDH. Entre o elenco da jurisprudência, é de realçar o caso Al-Skeini<sup>170</sup>, bem como o caso de Medvedyev<sup>171</sup>, neste último, as autoridades francesas intercetavam as embarcações com suspeita de tráfico de droga, sem fundamento jurídico para o efeito, bem como evidências para demonstrar essa mesma comercialização.

---

<sup>170</sup> Acórdão Al-Skeini v. United Kingdom, App n.º 55721/07, Eur. Ct. H.R. 1 (2011)

<sup>171</sup> Acórdão Medvedyev v. France, App n.º 3394/03 Eur. Ct. H.R. (2010)

### 3. Sistemas de informação da UE<sup>172</sup>

É relevante compreender que estes grandes sistemas de informação da UE assumem diversas dimensões das migrações, não restringindo ao controlo fronteiriço, incluindo um conjunto de processos relativos ao processo de asilo, o processo da aplicação de vistos, durante os controlos fronteiriços, emitindo títulos de residência, deter imigrantes em situação irregular, entre outros<sup>173</sup>. Nestes sistemas de informação da UE, também é procurado garantir a interoperabilidade<sup>174</sup> entre os diversos sistemas, ou seja, procurar a troca de dados entre os diversos sistemas para permitir a partilha de informações, principalmente após o pacote legislativo relativo ao ETIAS e o EES.

No âmbito do pacote legislativo relativo às “fronteiras inteligentes”, foi projetado a criação de dois sistemas de informação que complementam a atividade dos anteriores, com o intuito de facilitar a circulação, suavizar o processo de admissão ou recusa, bem como no combate à imigração irregular. Através do ETIAS, com o objetivo de incrementar o sistema VIS e o EES, registando todas as entradas, bem como a lista dos migrantes que permanecem mais que o tempo estabelecido. Dessa feita, a eu-LISA encarregar-se-á no desenvolvimento destes dois sistemas até ser implementado, como previsto para 2022<sup>175</sup>.

---

<sup>172</sup> Segundo Dijkstra, *et al* (2011, pp. 5 e ss), “*The use of technology for border control is at least as old as the Chinese Wall, with many recent successors such as the Great Wall of Tijuana, also known as the Great Wall of Capital, dividing Mexico from the United States to control illegal migration from the South to the North.*”

<sup>173</sup> Cfr. FRA, 2018c, pp. 113 e ss.

<sup>174</sup> Este é um conceito amplamente utilizado na doutrina militar, tipicamente assente num dos vetores do DOTMPLII (Doutrina, Organização, Treino, Material, Pessoal, Liderança, Infraestruturas e Interoperabilidade), sendo relevante para reduzir a complexidade e a articulação dos sistemas de informação, permitindo uma visão integrada de vários sistemas de informação. (Sheth, 1999, pp. 1-25)

<sup>175</sup> Cfr a hiperligação [https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/smart-borders-background\\_en](https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/smart-borders-background_en)

Esta necessidade de criação dos sistemas de informação parte da vontade em procurar controlar os fluxos migratórios, havendo um incremento constante dos sistemas em uso na UE, em especial o SIS<sup>176</sup> (do inglês Schengen Information System), o VIS<sup>177</sup> (do inglês Visa Information System), a EURODAC<sup>178</sup> (do inglês European Dactyloscopy), o EES<sup>179</sup> (do inglês Entry/Exit System), a ECRIS<sup>180</sup> (do inglês European Criminal Records Information System), o ETIAS<sup>181</sup> (do inglês European Travel Information and Authorisation System).

---

<sup>176</sup> Regulamento (UE) n.º 2018/1862 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio da cooperação policial e da cooperação judiciária em matéria penal, e que altera e revoga a Decisão 2007/533/JAI do Conselho e revoga o Regulamento (CE) n.º 1986/2006 do Parlamento Europeu e do Conselho e a Decisão 2010/261/UE da Comissão, com posteriores alterações.

<sup>177</sup> Regulamento (CE) n.º 767/2008 do Parlamento Europeu e do Conselho, de 9 de julho de 2008, relativo ao Sistema de Informação sobre Vistos (VIS) e ao intercâmbio de dados entre os Estados-Membros sobre os vistos de curta duração («Regulamento VIS»), com progressivas alterações.

<sup>178</sup> Regulamento (UE) n.º 603/2013 do Parlamento Europeu e do Conselho de 26 de junho de 2013, relativo à criação do sistema «Eurodac» de comparação de impressões digitais para efeitos da aplicação efetiva do Regulamento (UE) n.º 604/2013, que estabelece os critérios e mecanismos de determinação do Estado-Membro responsável pela análise de um pedido de proteção internacional apresentado num dos Estados-Membros por um nacional de um país terceiro ou um apátrida, e de pedidos de comparação com os dados Eurodac apresentados pelas autoridades responsáveis dos Estados-Membros e pela Europol para fins de aplicação da lei e que altera o Regulamento (UE) n.º 1077/2011 que cria uma Agência europeia para a gestão operacional de sistemas informáticos de grande escala no espaço de liberdade, segurança e justiça (reformulação), com posteriores alterações

<sup>179</sup> Regulamento (UE) n.º 2017/2226 do Parlamento Europeu e do Conselho de 30 de novembro de 2017, que estabelece o Sistema de Entrada/Saída (EES) para registo dos dados das entradas e saídas e dos dados das recusas de entrada dos nacionais de países terceiros aquando da passagem das fronteiras externas dos Estados-Membros, que determina as condições de acesso ao SES para efeitos de aplicação da lei, e que altera a Convenção de Aplicação do Acordo de Schengen e os Regulamentos (CE) n.º 767/2008 e (UE) n.º 1077/2011

<sup>180</sup> Regulamento (UE) 2019/816 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, que cria um sistema centralizado para a determinação dos Estados-Membros que possuem informações sobre condenações de nacionais de países terceiros e de apátridas (ECRIS-TCN) tendo em vista completar o Sistema Europeu de Informação sobre Registos Criminais e que altera o Regulamento (UE) 2018/1726

<sup>181</sup> 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

Tabela 1: Instrumentos da UE selecionados que envolvem o processamento de grandes quantidades de dados para os efeitos de controlo fronteiriço e prossecução policial

<b>Bases de Dados</b>	<b>Sigla</b>	<b>Propósito principal</b>
Sistemas de Informação Schengen	SIS II	Dar entrada e processar alertas para pessoas procuradas ou desaparecidas para salvaguardar a segurança, bem como dar entrada e processamento de alertas para imigrantes para o propósito de recusar a entrada ou estadia, como também para efeitos de decisão de retorno.
Sistema de Informação sobre Vistos	VIS	Facilitar a troca de dados entre os Estados Membros sobre as aplicações a vistos.
Dactiloscopia Europeia	EURODAC	Determinar o Estado Membro responsável para examinar a aplicação de proteção internacional e assistir com o controlo da migração irregular e movimentos secundários.
Sistema Europeu de Vigilância das Fronteiras	EUROSUR	Intercâmbio de informações e cooperação operacional entre as autoridades nacionais dos Estados-Membros da União
Registo de identificação dos passageiros	PNR	Recolha, processamento e troca de dados de passageiros de voos extra-UE, sem prejuízo da possibilidade desse processamento nos voos Intra-UE. Usado apenas para fins de prossecução policial.
Sistema Avançado de Informação sobre Passageiros	API	Recolha e processamento de dados de voos de países terceiros, para gestão de fronteiras e propósitos de prossecução policial.
Sistema de Entrada/Saída	EES	Calcular e monitorizar a duração da estadia autorizada dos imigrantes e identificar imigrantes com tempo abusivo no território da União
Sistema Europeu de Informação e Autorização de Viagem	ETIAS	Avaliar se um visto de um imigrantes coloca riscos de segurança, migração irregular ou de saúde pública.
Sistema Europeu de Informação sobre Registos Criminais	ECRIS-TCN	Partilha de informação sobre registo criminal de imigrantes.

Fonte: Adaptado de FRA, 2018c

Cumprirá mencionar, a aplicabilidade destes instrumentos não tem cobertura por toda a União, à exceção do Repositório de Identidade Central e a Eurodac. Como tal, verificamos em diversos casos a ausência da Dinamarca, bem como a possibilidade do *opt in* pela Irlanda no caso do ECRIS-TCN, por outro lado, Chipre e Irlanda não estão

vinculados pelo novo ETIAS<sup>182</sup> e, nos diversos instrumentos, verificamos uma certa colisão de interesses entre os vários Estados, principalmente no sistema EES, o qual é somente aplicável a vinte e dois Estados Membros da União (FRA, 2018c)

Relativamente aos dados PNR<sup>183</sup>, estes são recolhidos pelas transportadoras aéreas, na dimensão da privatização conforme tivermos oportunidade de mencionar previamente, com as datas de viagem, o contacto, os detalhes de pagamento, a informação da bagagem, outras referências como a dieta alimentar recolhidas e prestadas às unidades de informação dos passageiros<sup>184</sup>. Estas unidades, por sua vez, comparam com as bases de dados relevantes para descobrir indivíduos relacionados com alguma modalidade de crime, bem difundir a informação para os diversos Estados Membros.

---

<sup>182</sup> É relevante mencionar que a quantidade de dados processados no âmbito do sistema ETIAS, é o equivalente aos dados dos sistemas informáticos para este propósito dos EUA (ESTA), do Canadá (eTA) e da Austrália (ETA). (Cfr. Jones, 2020, p. 1-38)

<sup>183</sup> Caso observemos a Diretiva n.º 2016/681/UE, é imposto às transportadoras a cooperação com Estados terceiros, em particular, na partilha dos dados elencados no Anexo I do mesmo diploma, cujo tratamento encontra-se sujeito à finalidade de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave:

- I. *Código de identificação do registo PNR;*
- II. *Data da reserva/emissão do bilhete;*
- III. *Data(s) da viagem prevista;*
- IV. *Nome(s);*
- V. *Endereço e informações de contacto (número de telefone, endereço de correio eletrónico);*
- VI. *Todas as informações sobre as modalidades de pagamento, incluindo o endereço de faturação;*
- VII. *Itinerário completo para o PNR em causa;*
- VIII. *Informação de passageiro frequente;*
- IX. *Agência/agente de viagens;*
- X. *Situação do passageiro, incluindo confirmações, situação do registo, não comparência ou passageiro de última hora sem reserva;*
- XI. *Informação do PNR separada/dividida;*
- XII. *Observações gerais (designadamente todas as informações disponíveis sobre menores não acompanhados com idade inferior a 18 anos, como nome e sexo do menor, idade, língua(s) falada(s), nome e contactos da pessoa que o acompanha no momento da partida e sua relação com o menor, nome e contactos da pessoa que o acompanha no momento da chegada e sua relação com o menor, agente presente na partida e na chegada);*
- XIII. *Informações sobre a emissão dos bilhetes, incluindo número do bilhete, data de emissão, bilhetes só de ida, dados ATFQ (Automatic Ticket Fare Quote);*
- XIV. *Número do lugar e outras informações relativas ao lugar;*
- XV. *Informações sobre a partilha de código;*
- XVI. *Todas as informações relativas às bagagens;*
- XVII. *Número e outros nomes de passageiros que figuram no PNR;*
- XVIII. *Todas as informações prévias sobre os passageiros (dados API) que tenham sido recolhidas (incluindo, tipo e número de documento(s), país de emissão e termo de validade do(s) documento(s), nacionalidade, nome(s) e apelido(s), sexo, data de nascimento, companhia aérea, número de voo, data de partida, data de chegada, aeroporto de partida, aeroporto de chegada, hora de partida e hora de chegada);”*

<sup>184</sup> Cfr. a Comunicação 2018/C 230/05, sobre a lista das unidades de informação de passageiros referido no artigo 4.º da Diretiva (UE) 2016/681.

Por outro lado, existe um controlo robustecido na vigilância aérea na pré-embarcação, principalmente através da recolha de dados do viajante (PNR), integrando a transmissão de dados avançados sobre o passageiro (API) pelas transportadoras, quer em voos internacionais, quer em voos intra-UE, dentro da zona Schengen<sup>185</sup>. Por sua vez, após o check-in, transmitem a informação para os serviços de fronteira para o subsequente cruzamento com as bases de dados da União, Simultaneamente, já nesta fase do controlo fronteiriço, é recolhido outras informações para alimentar as bases de dados atuais da UE (i.e. SIS II, VIS, Eurodac), em particular com dados biométricos e outros, verificação da autenticidade dos documentos, presença na lista de procurados, entre outras ações.

Por outro lado, a União também conta com o Sistema de Informação Schengen, (SIS), inclusive, conta com uma segunda geração (abreviado SIS II) o qual assume o propósito primário de partilha de informações entre os diversos pontos de contacto da rede SIRENE<sup>186</sup> estando encriptada as comunicações durante o ciclo de vida dos dados, bem com o armazenamento na base de dados localizado em Estrasburgo, com o backup em Salzburgo na Áustria. Este sistema gerido 24/7 pela eu-LISA<sup>187</sup>, reparte-se em três dimensões:

- I. Para efeito de **deportação** dos imigrantes irregulares,<sup>188</sup>
- II. Para efeito de controlo **fronteiriço** de imigrantes irregulares<sup>189</sup>
- III. Para efeito de cooperação **policial** e judiciária em matéria penal<sup>190</sup>

---

<sup>185</sup> Na teoria das migrações, é relevante mencionar a tendência dos imigrantes atravessarem os países da União com maior proximidade geográfica, contudo, em grande parte das vezes, os imigrantes deslocam-se para outros Estados-Membros visando melhores condições ou até mesmo reunir-se com os familiares deslocados dentro da União, servindo de países de trânsito os primeiros, havendo movimentos secundários. Como tal, a União decidiu fortalecer esse controlo para evitar essas deslocações, (Cfr. o Regulamento (UE) n.º 2017/458, no reforço dos controlos fronteiriços elencados no CFS do Regulamento (UE) n.º 2016/399, alterando o artigo 8.º)

<sup>186</sup> Cfr. artigo 7.º e 8.º do Regulamento (CE) n.º 1987/2006, designado de Sistema de Informação Schengen de Segunda Geração, bem como nos mesmo artigos nas posteriores alterações, bem como o manual auxiliar inerente à Decisão de Implementação da Comissão de 2013/115/UE, de 26 de fevereiro de 2013

<sup>187</sup> Cfr. o artigo 3.º do Regulamento (UE) n.º 2018/1726

<sup>188</sup> Cfr. Regulamento (UE) 2018/1860 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo à utilização do Sistema de Informação de Schengen para efeitos de regresso dos nacionais de países terceiros em situação irregular, com posteriores alterações, doravante SIS II - Deportação

<sup>189</sup> Cfr. Regulamento (UE) 2018/1861 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio dos controlos de fronteira, e que altera a Convenção de Aplicação do Acordo de Schengen e altera e revoga o Regulamento (CE) n.º 1987/2006, com posteriores alterações, doravante SIS II - Fronteira

<sup>190</sup> Cfr. Regulamento (UE) 2018/1862 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio da

É necessário compreender que este sistema foi recentemente alterado, com a ampliação de dados recolhidos no âmbito dos Sistemas de Informação Schengen, neste caso particular dados biométricos, incluindo impressões da palma da mão, imagens faciais e ADN<sup>191</sup>. Conforme mencionado pela Autoridade Europeia para a Proteção de Dados os dados capturados do ADN poderão divulgar outros dados sensíveis, como doenças, a origem racial, ou outros dados que devem ser acautelados.<sup>192</sup>

Relativamente à arquitetura do sistema SIS II, este, é composto pelo sistema central (CS-SIS), assumindo o suporte técnico, o sistema nacional em cada Estado-Membro (serviço N.SIS II), comunicando com o SIS II central e, por fim, a infraestrutura de comunicação (Gabinetes SIRENE) criado um túnel encriptado entre o sistema central e os sistemas nacionais, de forma a permitir a troca de dados entre as autoridades relevantes para esta troca de informações<sup>193</sup>.

Conjuntamente, no VIS<sup>194</sup>, sistema subjacente à política comum de vistos estabelecida no Código dos Vistos com condições harmonizadas e procedimentos para emitir vistos para estadias de curto prazo, com a lista dos países terceiros com acordos de facilitação de concessão de vistos, podendo incluir a dispensa a posse de visto<sup>195</sup>,

---

cooperação policial e da cooperação judiciária em matéria penal, e que altera e revoga a Decisão 2007/533/JAI do Conselho e revoga o Regulamento (CE) n.º 1986/2006 do Parlamento Europeu e do Conselho e a Decisão 2010/261/UE da Comissão, com posteriores alterações, doravante SIS II - Policia

<sup>191</sup> O nosso ADN é um registo que pode exteriorizar dados clínicos sensíveis para o titular desses dados, podendo comprometer a privacidade deste indivíduo, em particular, caso esses dados sejam do conhecimento de terceiros, principalmente em situações de exfiltração de dados.

<sup>192</sup> Para o entendimento da posição da AEPD, recomendamos a consulta da Opinião às decisões da Comissão para implementação de padrões mínimos e padrões técnicos para a recolha dos dados biométricos Cfr. a hiperligação [https://edps.europa.eu/sites/edp/files/publication/20-08-26\\_edps\\_comments\\_on\\_draft\\_commission\\_implementing\\_decisions\\_on\\_minimum\\_standards\\_and\\_technicalities\\_for\\_biometric\\_data\\_in\\_sis\\_in\\_field\\_of\\_border\\_checks\\_and\\_return\\_and\\_police\\_and\\_judicial\\_cooperation\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/20-08-26_edps_comments_on_draft_commission_implementing_decisions_on_minimum_standards_and_technicalities_for_biometric_data_in_sis_in_field_of_border_checks_and_return_and_police_and_judicial_cooperation_en.pdf)

<sup>193</sup> Esta informação poderá ser obtida a partir da leitura do artigo 4.º, conjuntamente com o artigo 7.º do Regulamento (UE) 2018/1862 e o Regulamento (UE) 2018/1861

<sup>194</sup> De acordo com o Regulamento VIS, verificamos esta lista taxativa da tipologia de dados admissíveis no âmbito do Regulamento:

- I. Dados alfanuméricos sobre o requerente e os vistos pedidos, emitidos, recusados, anulados, revogados ou prorrogados, a que se referem os pontos 1 a 4 do artigo 9.º e os artigos 10.º a 14.º;
- II. Fotografias, conforme referido no ponto 5 do artigo 9.º;
- III. Impressões digitais, conforme referido no ponto 6 do artigo 9.º;
- IV. Ligações para outros pedidos a que se referem os n.º 3 e 4 do artigo 8.º

<sup>195</sup> Para que compreendamos o quadro completo das exceções, é necessário escrutinar as exceções dedicados para serviços diplomáticos, serviços oficiais ou passaportes especiais (Cfr. o n.º 1 do artigo 6.º do Regulamento (CE) n.º 810/2009, com posteriores alterações, designado por Código de Vistos), bem como estudantes em excursão, exceções para refugiados e apátridas, para membros desempenhado funções na NATO (Cfr. o n.º 2 do artigo 6.º do Código de Vistos), pessoas com atividade paga durante a estadia (Cfr. o n.º 3 do artigo 6.º do Código de Vistos)

contemplar a consulta prévia, bem como informações posteriores<sup>196</sup>, ou outras situações específicas, devendo notificar a Comissão Europeia<sup>197</sup>. Segundo o levantamento realizado por Jones (2019, p. 9), a União armazena cerca de 42 milhões de conjuntos de dados biométricos em 2018 somente com o sistema VIS.

No que concerne à Eurodac, este é um sistema para facilitar o controlo dos imigrantes que pediram asilo, ficando registados numa base de dados, de forma a que o mesmo imigrante não peça asilo em múltiplos Estados-Membros, sobrecarregando-os com esses pedidos. Cada vez mais, a tecnologia biométrica é utilizada no âmbito dos sistemas da informação da UE, retendo esses dados biométricos em bases de dados para posterior comparação, não sendo exclusivo do sistema Eurodac.

Para a finalidade do combate da criminalidade, também é comparado os dados relativos nas bases de dados da Europol (ECRIS-TCN), também a ser desenvolvido uma nova versão ao sistema anterior, cujo objetivo é armazenar a informação do registo criminal e, para o efeito de controlo fronteiriço, fazer-se *queries* à base de dados para ver se o indivíduo em particular encontra-se nesta lista, sem prejuízo da cooperação com a Interpol, com a base de dados Documentos de Viagem Roubados e Extraviados (SLDT) e Documentos de Viagem Associados a Notificações (TDAWN).

Relativamente ao ETIAS, este sistema tem como intuito avaliar o risco de terceiros com exceção de visto em tornarem-se imigrantes irregulares, provarem ser um risco para a segurança ou saúde pública<sup>198</sup> previamente à conceção da autorização para viajar, contemplando a fase inicial da verificação da identidade, dos documentos e questões<sup>199</sup>. Esta avaliação parte da comparação automatizada com as diversas bases de dados com a informação prestada pelo viajante<sup>200</sup>, onde o sistema ETIAS atribuirá a

---

<sup>196</sup> Por outro lado, também é de mencionar a lista dos países que carecem de visto para entrar na União, bem como uma lista de exceção quanto à entrada na União, em particular com vistos de residência, podendo encontrar no Regulamento n.º 2018/1806, onde é lista os terceiros que necessitam e não necessitam de visto para entrar, em particular nos Anexos I e II.

<sup>197</sup> Nos termos do n.º 1 do artigo 53.º do Código de Vistos

<sup>198</sup> Ao correlacionar com os dados da Organização Mundial da Saúde (WHO) e o Centro Europeu de Prevenção e Controlo das Doenças (ECDC) relativos a surtos de doenças e a informação epidemiológico dos países afetados.

<sup>199</sup> Será realizada *queries* às várias bases de dados, em particular a do ETIAS, SIS, EES, dados da Europol, SLDT (Interpol), Eurodac, ECRIS, TDAWN (Interpol), ETIAS Watchlist e o ETIAS Screening rules.

<sup>200</sup> O requerente tem de fornecer diversos tipos de dados que são analisados conjuntamente com os indicadores de risco, nos termos do n.º 2 e ss. do artigo 17.º do Regulamento (UE) 2018/1240:

“O requerente indica os seguintes dados pessoais no formulário de pedido:

avaliação de risco com bases em indicadores<sup>201</sup> designados por *screening rules*, através do qual o perfil do viajante será avaliado.

Quanto ao Sistema de Entrada/Saída (EES), este será implementado para todos os cidadãos de países terceiros ao Espaço Schengen<sup>202</sup>, visa complementar o ETIAS na dimensão de visitantes de curta duração, com o registo também de 10 impressões

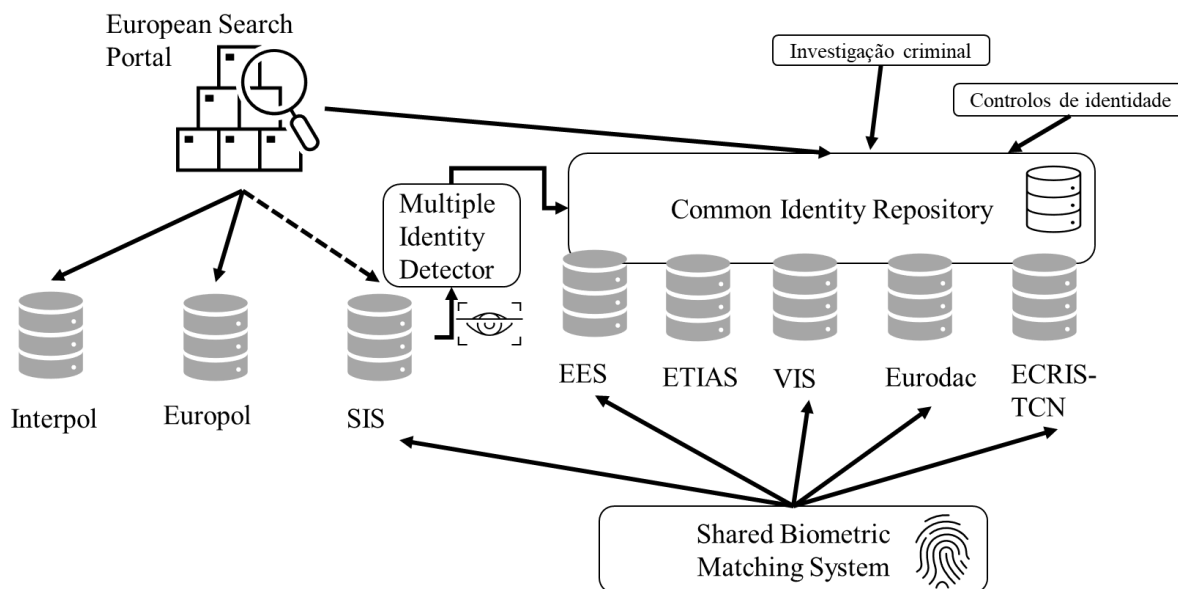
- 
- a) *Apelido, nome(s) próprio(s), apelidos de nascimento, data de nascimento, local de nascimento, país de nascimento, sexo, nacionalidade atual, nome(s) próprio(s) dos progenitores;*
  - b) *Outros nomes (pseudónimos, nomes artísticos, nomes habituais), se aplicável;*
  - c) *Outras nacionalidades se for o caso;*
  - d) *Tipo, número e país de emissão do documento de viagem;*
  - e) *Data de emissão e data de caducidade da validade do documento de viagem;*
  - f) *Endereço do domicílio do requerente ou, se não existir, a cidade e o país de residência;*
  - g) *Endereço de correio eletrónico e, se aplicável, números de telefone;*
  - h) *Habilitações literárias (ensino primário, secundário, superior ou sem habilitações);*
  - i) *Profissão atual (tipo de emprego); caso o pedido seja tratado manualmente em conformidade com o procedimento previsto no artigo 26.o, o Estado-Membro competente pode, em conformidade com o artigo 27.o, solicitar ao requerente que forneça informações suplementares sobre a designação exata do cargo e o empregador ou, no caso dos estudantes, o nome do estabelecimento de ensino;*
  - j) *Estado-Membro previsto para a primeira estada e, a título facultativo, o endereço da primeira estada prevista;*
  - k) *Para os menores: apelido e nome(s) próprio(s), endereço do domicílio, endereço de correio eletrónico e, se disponível, número de telefone da pessoa que exerce as responsabilidades parentais ou a tutela legal do requerente;*
  - l) *Se invocar a qualidade de membro da família referida no artigo 2.o, n.o 1, alínea c):*
    - i) *a sua qualidade de membro da família,*
    - ii) *o apelido, nome(s) próprio(s), data de nascimento, local de nascimento, país de nascimento, nacionalidade atual, domicílio, endereço de correio eletrónico e, caso disponível, o número do telefone do membro da família com quem o requerente esteja ligado por vínculos familiares,*
    - iii) *os vínculos familiares com o referido membro da família em conformidade com o artigo 2.o, n.o 2, da Diretiva 2004/38/CE;*
  - m) *No caso de um pedido preenchido por uma pessoa que não seja o requerente: o apelido, nome(s) próprio(s), nome da empresa ou organização, se for o caso, endereço de correio eletrónico, endereço postal e número de telefone, caso disponível dessa pessoa; relação com o requerente e uma declaração de representação assinada. (...)*
4. Além disso, o requerente responde às seguintes perguntas:
- a) *Se foi condenado por qualquer das infrações penais enumeradas no anexo no decurso dos 10 anos anteriores e, no caso de infrações terroristas, no decurso dos 20 anos anteriores, e, em caso afirmativo, quando e em que país;*
  - b) *Se esteve presente numa zona específica de guerra ou de conflito nos 10 anos anteriores, especificando os motivos dessa estada;*
  - c) *Se foi objeto de qualquer decisão de abandono do território de um Estado-Membro ou de qualquer país terceiro constante da lista do anexo II do Regulamento (CE) n.o 539/2001, ou se foi objeto de uma decisão de regresso emitida nos 10 anos anteriores. (...)*
8. Após o envio do formulário de pedido, o sistema de informação ETIAS recolhe o endereço IP a partir do qual o pedido foi apresentado.”

<sup>201</sup> Esses indicadores são continuamente revistos, avaliados, contudo existem determinados fatores que são contemplados na avaliação, desde logo a aparência, língua, raça, cor da pele, pensamentos políticos e religiosos, deficiências, orientação sexual. Cfr. a hiperligação <https://etias.com/articles/what-will-be-the-etias-screening-rules>

<sup>202</sup> Para tal, está associado um documento de identificação que poderá também ser automatizado, com a reconhecimento facial carecendo de confirmação pelo agente no controlo fronteiriço. Cfr. Cantarero, *et al*, 2013, pp. 1-4. Para compreender onde será operado o EES, sem prejuízo de certas particularidades como a derrogação do uso das funcionalidades biométricas no EES, cfr. o artigo n.º 4 do Regulamento (UE) 2017/2226 de 30 de novembro de 2017

digitais. Também é discutido a dimensão da transferência dos dados<sup>203</sup>, quer para Estados terceiros, quer para o setor privado, o que coloca inúmeras indagações em termos de dados pessoais.<sup>204</sup>

Figura 1: Sistema da Interoperabilidade previsto no Regulamento (UE) 2019/817



Fonte: Adaptado de Comissão Europeia, 2017, COM/2017/0793 final - 2017/0351 (COD)

Após o estabelecimento da *framework* da interoperabilidade para estes sistemas da informação da UE, procurará que as bases de dados comuniquem entre si, centralizando o motor de pesquisa no Portal europeu de pesquisa (do inglês European Search Portal) para capacitar a realizar *queries* às inúmeras bases dados supramencionadas, verificando se existe algum dado que esteja a ser pesquisado.

Por um lado, permitirá comparar de forma eficiente os dados biométricos nos serviços biométricos partilhados<sup>205</sup>, recolhidos nas diversas bases de dados como já mencionamos, bem como o acesso ao repositório comum de dados de identificação<sup>206</sup> e, por fim, um detetor de múltiplas identidades para qualquer tentativa de personificar outrem. Por um lado, congregará a plataforma designados por Sistema Automático de Identificação Dactiloscópica (AFIS) e, por outro lado, o repositório comum de dados de

<sup>203</sup> Cfr. o n.º 2 do artigo 27.º do Regulamento

<sup>204</sup> Cfr. *Opinion of the European Data Protection Supervisor on the Proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP)*

<sup>205</sup> Do inglês *Shared Biometric Matching System*

<sup>206</sup> Do inglês *Common Identity Repository*

identificação (CIR) prevê-se uma componente com dados biográficos limitados ao necessário<sup>207</sup>.

---

<sup>207</sup> Serão aqueles dados que constam no documento de viagem, os quais incluem o nome próprio, sexo, data de nascimento e o número do documento de viagem

## Capítulo III | O caso do iBorderCtrl

### 1. O Controlo Fronteiriço Automático<sup>208</sup>: o projeto iBorderCtrl

É notória a tendência na última década, da adoção de processos automatizados no controlo fronteiriço, com o custo-benefício no controlo fronteiriço, principalmente nos aeroportos, alocando os recursos humanos para indivíduos pautados de alto risco, após a triagem dos controlos automatizados dos sistemas de Automated Border Control (ABC), também conhecido como IBorder<sup>209</sup>. Esta tecnologia deve ser entendida com as tendências atuais do controlo fronteiriço contemporâneo (Pöttsch, 2015):

- I. Informatização do corpo traduzido em bits para as bases de dados;
- II. Mobilização o controlo com unidades móveis ampliando a dimensão do controlo da fronteira;
- III. Impacto dos titulares afetos por esse controlo na dimensão do uso inadequado, devendo registar os eventos anormais;
- IV. Interatividade da ferramenta com as múltiplas tecnologias coordenadas;
- V. Afetação dos direitos individuais, bem como afetar a esfera privada dos cidadãos e, por fim;
- VI. Justificação do seu uso alegadamente através das ameaças existentes, configura um potencial problema da securitização.

Relativamente à arquitetura do sistema de controlo fronteiriço automático, existem certas componentes como as barreiras físicas (e-Gates), o leitor de documentos para proceder com a viagem, equipamentos para capturar os dados biométricos (câmaras e leitores de impressões digitais), a interface do utilizador (monitor, sinais LED, equipamentos de áudio, botão de pânico), unidade de processamento e equipamentos de rede (PC, hubs, controller) e, por fim, câmaras e sensores de vigilância (CCTV, deteção de *tailgate*, deteção de bagagem deixada). Por outras palavras, este processo passa pela validação do passaporte, pela extração da amostra biométrica e pelo reconhecimento facial e, posteriormente ao resultado, abrir as barreiras físicas (Frontex, 2015). Estes

---

<sup>208</sup> Do inglês *Automated Border Control*

<sup>209</sup> Este termo deve ser inserido no contexto da sociedade tecnológica, nos mecanismos contemporâneos utilizados no controlo fronteiriço por diversos Estados à escala internacional, combinando o uso de ferramentas tecnológicas que permitem automatizar o controlo através de técnicas como ordenar, definir perfis, categorizar, prever, filtrar entre outras (Pöttsch, 2015, p. 8)

sistemas tiveram a sua evolução, marcada por características distintas, as quais encontram-se explicitadas em Gorodnichy (2014, p. 121), repartindo em três gerações:

*“The 1st generation (Gen-1 ABC machines): These ABC machines serve only the registered travelers. Example of such machines are NEXUS’s clearance kiosks [9] based on iris verification (Canada/U.S. border) and IRIS machines in UK demounted in 2012.*

*The 2nd generation (Gen-2 ABC machines): These machines are used worldwide. They are based on the e-passport/eID technology. They serve all travelers, including registered travelers, via a simplified checking procedure. The definitions and analysis of such systems are best developed by Frontex*

*The 3rd generation (Gen-3 ABC machines): They represent a concept of the next-generation system that is being developed by many countries in support of the eBorder process of the future. Gen-3 ABC system extends the border control from a Checkpoint solution to an Air Traveller Continuum solution. It makes use of the entire eBorder traveller screening infrastructure”*

Tipicamente os sistemas ABC assentam num módulo de confirmação do documento de identificação pela via de um leitor do chip do documento de identificação, quer seja o cartão de identificação nacional, quer seja o passaporte, contendo a reconhecimento facial, posteriormente comparada com a imagem facial em tempo real através de reconhecimento biométrico facial. Para uma visão completa do processo, este pode ser repartido pelas seguintes fases (Gorodnichy, [et al.], 2014):

- Fase I. Inicialização da máquina ABC ao dar dados pessoais na altura da compra do bilhete de viagem;
- Fase II. Estimativa inicial do fator risco, usando ferramentas tecnológicas, recorrendo dados do momento da compra do bilhete de viagem;
- Fase III. Correção do fator risco usando ferramentas para avaliar o risco com base na vigilância do edifício, em particular, a informação da atividade do viajante no aeroporto é recolhida e analisada;

Fase IV. Correção do fator risco usando ferramentas de verificação (*e-passport*) e, adicionalmente, com as técnicas de avaliação de risco (verificar nas *watchlists*);

Fase V. Correção do fator risco ao avaliar manualmente pelo serviço de fronteira caso necessário. Posto isto, a decisão final é tomada.

Este processo de automatização dos controlos fronteiriços tem sido acompanhado pelas instituições/organizações internacionais, com o intuito de compreender os efeitos discriminatórios do uso destas tecnologias. Tomemos como ilustrativo o relatório preparado por E. Tendayi Achiume, no âmbito da Assembleia Geral das Nações Unidas, através da resolução 70/137 estipulando esta necessidade e a resolução A/75/50289 da Assembleia Geral, prosseguindo a necessidade estipulada deste relatório.

Relativamente às tecnologias utilizadas nestes sistemas automáticos, com a subsequente aplicação, podemos encontrar diversas, como exemplificativo, a deteção de humanos ocultados (FAST project), deteção de padrões comportamentais anormais (CAPPS), autenticação através dos dados biométricos e a avaliação do risco (NEXUS), bem como outras tecnologias (Gorodnichy, 2014).

No caso do EES, com reconhecimento das impressões digitais face ao contido no chip do documento de identificação<sup>210</sup>, tomando o caso do Cartão de Cidadão<sup>211</sup>, ou até outras bases de dados que mencionamos previamente. Nesta dimensão, ocorreram diversos projetos relativos à automatização do controlo fronteiriço, sendo esses<sup>212</sup>:

- I. IBorderCtrl
- II. Bodega
- III. MobilePass
- IV. Newpass

---

<sup>210</sup> Com leitura conjunta da alínea c) do n.º 1 do artigo 17.º e do considerando 21.º do Regulamento (UE) 2017/2226 de 30 de novembro de 2017, compreendemos a particularidade de idealmente confirmar com 4 impressões digitais distintas, salvo nos casos previstos como o caso de menores de 12 anos e impossibilidade física, conforme previsto no n.º 3 e n.º 4 do artigo 17.º respetivamente, bem como a redução do número de impressões digitais caso combinado com reconhecimento facial, conforme mencionado no considerando 20.º do mesmo regulamento.

<sup>211</sup> Para a validade do cartão de cidadão enquanto elemento para a identificação eletrónica, tendo que ser comunicado no âmbito do regulamento eIDAS, nos termos no n.º 3 do artigo 9.º do Regulamento (UE) n.º 910/2014, respeitando os requisitos elencados no Regulamento.

<sup>212</sup> Cfr. a hiperligação <http://www.projectprotect.eu/about/related-projects>

- V. BioP@ss
- VI. ABC4EU
- VII. Fastpass
- VIII. Tabula Rasa
- IX. Beat
- X. Actibio
- XI. Ingress
- XII. Effisec
- XIII. Fidelity
- XIV. Hide

Neste conjunto de ferramentas pautadas pela automatização do processo de gestão dos fluxos migratórios, parte da doutrina defende a sua importância como solução às exigências do enquadramento regulatório do terrorismo<sup>213</sup> (Crockett, [et al.], 2020). Estas soluções possibilitam suavizar o processo, de forma a que não seja sobrecarregado os serviços de fronteira desse controlo isoladamente

---

<sup>213</sup> Para detalhar este ponto, devemos considerar o Regulamento (UE) 2017/458, o qual exige, ao contrário do previamente mencionado no 3.º parágrafo do n.º 2 do artigo 8.º do Regulamento (UE) 2016/399, “*No entanto, e de modo não sistemático, ao efetuarem os controlos mínimos dos beneficiários do direito à livre circulação ao abrigo do direito da União, os guardas de fronteira podem consultar as bases de dados nacionais e europeias a fim de assegurar que essas pessoas não representam uma ameaça real, presente e suficientemente grave para a segurança interna, a ordem pública e as relações internacionais dos Estados-Membros, ou uma ameaça para a saúde pública.*”, tendo este artigo sido alterado pelo primeiro para permitir o controlo de todos os cidadãos europeus nas fronteiras, o que evidentemente aumentará o tráfego de pessoas.

Cumpra escrutinar o sistema inteligente portátil para o controlo fronteiriço, designado por iBorderCtrl<sup>214</sup>, tendo por vista o desenvolvimento da gestão das fronteiras Schengen, coordenado pela *European Dynamics Luxembourg SA*, para a promoção das Sociedades Seguras, considerada como um dos 7 grandes desafios para a sociedade<sup>215</sup>, no âmbito do Horizonte 2020, contando com o financiamento de €1,695 mil milhões, tendo sido alocado 4,5€ milhões de euros ao projeto iBorderCtrl.

Todos os módulos que mencionaremos posteriormente articulam-se com os equipamentos móveis para o controlo fronteiriço, tomando como exemplificativo o uso de *tablets* para servirem de intermediários da informação recolhida no ato do controlo fronteiriço, transmitida para os servidores do sistema iBorderCtrl (2016c). Conjuntamente, nos relatórios periódicos produzidos pela iBorderCtrl, em particular no período de 1 de março de 2018 a 31 de agosto de 2019, alguns aspetos positivos foram levantados ao longo da experiência deste sistema nos países alocados<sup>216</sup>:

- I. Aumento significativo da eficiência e segurança do viajante e menos travessias ilegais;
- II. Redução dos custos/tempo na fronteira, permitindo o uso de equipamentos pessoais dos viajantes e unidades portáteis para os operadores;
- III. Introdução de um passo de pré-registo para informar os viajantes sobre os seus direitos, os procedimentos da viagem, os dados recolhidos na UE, bem como por requisitos nacionais;

---

<sup>214</sup> Para uma consulta detalhada do projeto, recomendamos Cfr. <https://cordis.europa.eu/project/id/700626>

<sup>215</sup> Neste tópico, o foco tido pela União versa diversos aspetos da sociedade, pese embora não mencione diretamente a migração irregular como objetivo a combater, é notório nas diversas linhas de orientação a preocupação na gestão fronteiriça dos fluxos migratórios, tomando como assunto securitário, como podemos denotar na alínea g):

- a) Saúde, alterações demográficas e bem-estar;
- b) Segurança alimentar, agricultura e silvicultura sustentável, investigação marinha, marítima e de águas interiores, e bioeconomia;
- c) Energia segura, não poluente e eficiente;
- d) Transportes inteligentes, ecológicos e integrados;
- e) Ação climática, eficiência na utilização de recursos e matérias-primas;
- f) A Europa num mundo em mudança – sociedades inclusivas, inovadoras e reflexivas;
- g) Sociedades seguras – Proteger a liberdade e a segurança da Europa e dos seus cidadãos.

Estas diretrizes podem ser consultadas aqui no seguinte link [https://ec.europa.eu/programmes/horizon2020/sites/horizon2020/files/H2020\\_PT\\_KI0213413PTN.pdf](https://ec.europa.eu/programmes/horizon2020/sites/horizon2020/files/H2020_PT_KI0213413PTN.pdf), consultado a 17 de outubro de 2020,

<sup>216</sup> Cfr. a hiperligação <https://cordis.europa.eu/project/id/700626/reporting>

- IV. Aumentar a escalabilidade, reduzir a carga de trabalho e erros subjetivos dos agentes humanos;
- V. Aumento do controlo objetivo por meios automatizados não invasivos, sem consumir muito tempo e;
- VI. Fornece uma plataforma de controlo fronteiriço mais robusta e eficiente.

Este projeto contempla uma primeira versão (IBorderCtrl, 2016a), uma segunda fase (IBorderCtrl, 2016b), algumas especificações da recolha de dados dos equipamentos (IBorderCtrl, 2016c), a primeira parte dos planos de comunicação e disseminação (IBorderCtrl, 2016d), a segunda parte dos planos de comunicação e disseminação (IBorderCtrl, 2016e), bem como outros dados como *flyers* e outros dados não publicamente disponíveis. Será recolhida a informação relativa ao funcionamento, alguns aspetos mencionados neste sistema, medidas de segurança inerentes, entre outras dimensões.

Simultaneamente, este projeto tem como objetivo de permitir os controlos fronteiriços mais rápidos aos imigrantes que atravessam as fronteiras terrestres (e.g. rodovia, ferrovia, da União, com as tecnologias do futuro da gestão das fronteiras Schengen, aumentando a eficiência, reduzindo o tempo na fronteira, utilizar um passo de pré-registo, reduzir o controlo subjetivo, passando para um controlo objetivo (IBorderCtrl, 2016a). Este projeto requiere o consentimento informado do titular dos dados para os serviços de fronteira poderem registar os dados neste projeto, sem prejuízo deste carácter particular subsistir durante o período do projeto. Contudo, este direito ao consentimento não acautela a possibilidade de optar por uma avaliação de um guarda de fronteira, ao invés da máquina<sup>217</sup>

O detalhe das informações relativos a este projeto é amplamente ocultado por interesses comerciais, bem como por propriedade intelectual, assumindo um estatuto de parcialmente acessível<sup>218</sup>. Neste sentido, o membro do parlamento europeu Patrick

---

<sup>217</sup> Cfr. a hiperligação <https://ai-lawhub.com/2020/07/13/ai-and-foreign-travel/>

<sup>218</sup> De facto para o efeito de acesso à informação relativa a avaliação dos protótipos (iBorderCtrl, 2016f), verificamos a seguinte mensagem no anexo: “Partially accessible on the basis of Article 4.1 (b) of REGULATION (EC) No 1049/2001: protection of privacy and the integrity of the individual, in particular in accordance with

Breyer, em março de 2019, intentou uma ação contra a Comissão Europeia para obter o acesso aos documentos relativos à execução do projeto iBorderCtrl (i.e. o caso T-158/19). Este sistema já foi sujeito à avaliação de impacto dos dados pessoais (DPIA), pese embora essa informação não esteja publicamente disponível, foi considerada no redesenho maioritariamente no módulo de deteção de mentiras na segunda versão (iBorderCtrl, 2016b, p. 12)

Simultaneamente, este projeto teve a sua cessação a 31 de agosto de 2019, após terem sido testados nos aeroportos<sup>219</sup>, nos quais apresentava-se o objetivo de integrar uma componente voluntária ao RTP<sup>220</sup>, bem como uma solução auxiliar ao EES e ao ETIAS.<sup>221</sup> É relevante compreender que este sistema integra métodos de Inteligência Artificial que serão escrutinados posteriormente, cumprindo mencionar os módulos<sup>222</sup> inerentes ao funcionamento desta solução:

- I. Sistema de deteção automática de mentiras (ADDS)
- II. Reconhecimento biométrico (BIO)
- III. Ferramenta para reconhecimento facial (FMT)

---

*Community legislation regarding the protection of personal data and of Article 4.2 1st indent of REGULATION (EC) No 1049/2001: protection of commercial interests of a natural or legal person, including intellectual property*” Cfr. a hiperligação [https://www.asktheeu.org/de/request/6091/response/19436/attach/3/700626%20iBorderCtrl%20Annex%20I.pdf?cookie\\_passthrough=1](https://www.asktheeu.org/de/request/6091/response/19436/attach/3/700626%20iBorderCtrl%20Annex%20I.pdf?cookie_passthrough=1)

<sup>219</sup> Esses pontos de controlo fronteiriço foram os da Hungria, Letónia, Grécia.

<sup>220</sup> É relevante mencionar que este programa foi abandonando, dando espaço a presença do iBorderCtrl. Cfr. a hiperligação [https://www.europarl.europa.eu/legislative-train/theme-towards-a-new-policy-on-migration/file-registered-traveller-programme-\(2013-smart-borders-package\)](https://www.europarl.europa.eu/legislative-train/theme-towards-a-new-policy-on-migration/file-registered-traveller-programme-(2013-smart-borders-package))

<sup>221</sup> Tomando as palavras de Carlos-Roca (2018), “*iBorderCtrl initiative will provide the first steps towards the proposed European Travel Information and Authorization System (ETIAS) that would allow bona fide travelers to submit their information ahead of their travel in order to reduce their time at the border crossing point.*”

<sup>222</sup> Sendo repartido numa fase prévia à viagem e uma fase do controlo na fronteira:

- I. O controlo prévio à viagem
  - a) Nesta fase é espectável a recolha de dados iniciais, documentação necessária para a viagem, dados de veículos.
  - b) Conjuntamente, uma entrevista curta e automática com um *avatar*, com capacidade integrada de deteção de mentiras e com capacidade de correlacionar com dados pré-existentes na base de dados.
  - c) Simultaneamente análise de multifatores e abordagem de risco, registando os dados e correlacionados com dados em fonte aberta ou sistemas externos como SIS II, VIS, EURODAC, entre outros.
  - d) Por fim, exige-se o consentimento aos viajantes.
- II. O controlo na fronteira
  - a) Confirma a informação previamente registada, com um conjunto de equipamentos portáteis necessários para capturar a informação (e.g. câmara fotográfica, sensor de impressão digital, leitor de documentos, entre outros),
  - b) Bem como a identidade, na mesma ótica do sistema EES, com a particularidade de comparar a fotografia tirada no momento com a capturada na entrevista com o *avatar*.

- IV. Ferramenta de análise da autenticidade do documento (DAAT)
- V. Ferramenta de deteção de humanos ocultados (HHD)
- VI. Sistema externo de legado e interface social (ELSI)
- VII. Ferramenta baseada na avaliação de risco (RBAT)
- VIII. Ferramenta de análise integrada de controlo fronteiroço (BCAT)

Entre os vários tipos de dados recolhidos<sup>223</sup>, verificamos os dados biométricos, reconhecendo os tipos de reconhecimento biométrico, aglutinando a análise fisiológica como o reconhecimento por ADN<sup>224</sup>, o reconhecimento facial<sup>225</sup>, a impressão digital<sup>226</sup>, a veia da palma da mão<sup>227</sup>, a íris e a retina. (FRA, 2018a, p. 25). Ainda, a análise comportamental, como a maneira de andar, os gestos, a voz, entre outros, como veremos posteriormente (iBorderCtrl, 2016c, p. 33). Cumpre ainda mencionar os diversos parceiros neste sistema do iBorderCtrl, atuando como responsáveis dos dados principais, caso observemos a carta do consentimento informado direcionado para os indivíduos que participaram neste projeto<sup>228</sup>:

- European Dynamics Luxembourg SA, responsável por manter e desenvolver a aplicação e a interface do viajante, o sistema de back-end que inclui a base de dados central, o módulo DAAT e o módulo RBAT;
- Manchester Metropolitan University, enquanto responsável na manutenção e desenvolvimento do sistema ADDS;

---

<sup>223</sup> Neste sentido, os dados recolhidos nesta fase são os seguintes: “(1) *Personal data such as name, surname, address, nationality, sex, vehicle registration, answers to the avatar interview questions, etc. and, (2) special categories of data such as biometric data - fingerprints, palm vein images, facial images and (facial) gestures.*” Cfr. a hiperligação [https://iborderctrl.no/informed\\_consent](https://iborderctrl.no/informed_consent)

<sup>224</sup> Tipicamente recolhido nas bases de dados como o Regulamento (UE) 2018/1862 (SIS II – Polícia), nos termos do artigo 20.º.

<sup>225</sup> Também encontramos no Regulamento (UE) 2018/1862 (SIS II – Polícia), nos termos do artigo 42.º, 43.º, com leitura conjunta do considerando 22.º, no Regulamento (UE) 2018/1861 (SIS II – Fronteiras), nos termos do artigo 32.º e 33.º, com leitura conjunta do considerando 20.º, no Regulamento (UE) 2018/1860 (SIS II – Retorno), nos termos do artigo 4.º, no Regulamento 2017/2226 (EES), nos termos do artigo 15.º, o artigo 23.º, 24.º, 25.º, 26.º, e no Regulamento (UE) 2019/816 (ECRIS-TCN), nos termos do n.º 1 e n.º 2 do artigo 6.º.

<sup>226</sup> Para resumir o enquadramento legislativo, praticamente todos os sistemas de informação da UE usam dados biométricos como meio de autenticar, excluindo o ETIAS.

<sup>227</sup> Encontramos o Regulamento (UE) 2018/1862 (SIS II – Polícia), no Regulamento (UE) 2018/1861 (SIS II – Fronteiras), no Regulamento (UE) 2018/1860 (SIS II – Retorno) com este tipo de leitores das veias da palma da mão.

<sup>228</sup> Cfr. a hiperligação [https://iborderctrl.no/informed\\_consent](https://iborderctrl.no/informed_consent)

- Stremble Ventures Ltd, responsável para a manutenção e desenvolvimento do BCAT e da componente do ELSI, o qual permite interligar com as bases de dados externas, bem como as redes sociais;
- Everis Aeroespacial y Defensa SL, responsável pela manutenção e desenvolvimento do FMT e o BIO.
- BioSec Group Ltd., responsável para manter a desenvolver o componente da leitura da veia da palma da mão do BIO
- JAS technologie sp z o.o. (Ltd), responsável por manter e desenvolver a aplicação e a interface do Guarda de Fronteira via unidade portátil, integrando os diversos módulos, bem como as instâncias locais criadas para aceder às bases de dados do sistema iBorderCtrl;
- Institute of Communication and Computer Systems (ICCS), responsável por desenvolver e manter a componente do HDD.

Numa dimensão da segurança da informação, algumas ferramentas utilizadas neste projeto encontram-se assentes em soluções de fonte aberta, tipicamente contempla determinadas vulnerabilidades que podem ser exploradas por atacantes, tendo acesso dos dados, entre os quais, dados biométricos<sup>229</sup>. (iBorderCtrl, 2016c)

### *1.1. Reconhecimento biométrico*

Relativamente ao módulo BIO, este integra a componente do reconhecimento biométrico, em particular, através do reconhecimento da impressão digital<sup>230</sup>. Este

---

<sup>229</sup> É mencionado o uso de ferramentas de networking para analisar algumas características da rede, bem como o uso de sistemas de gestão de conteúdo como o Drupal, acarretando algumas vulnerabilidades que deverão ser mitigadas.

<sup>230</sup> Para o entendimento da definição de dados biométricos, devemos atender à definição no n.º 14 do artigo 4.º do RGPD, compreendendo que este dado sensível, também nos termos do considerando 51.º do RGPD, serve o propósito de identificar única e exclusivamente um indivíduo. Ao focarmos na particularidade dos dados recolhidos pelas autoridades e armazenados nas bases de dados da União Europeia, compreendemos que um dos dados mais recolhidos dos imigrantes são dados biométricos, e, como tal, este dado é considerado como um dado sensível (Cfr. n.º 1 do artigo 9.º do RGPD e o n.º 1 do artigo 10.º da Diretiva (UE) 2016/680). A regra geral é da

módulo procura reconhecer as papilas do dedo, bem como outras variações que permitem identificar um indivíduo partindo desse dado biométrico, recorrendo às melhores práticas da atualidade.

Este módulo procura seguir as melhores práticas internacionais elencadas no projeto do IBorderCtrl (2016c) “*These include: accuracy (based on several criteria including error rate, FAR, FRR, identification rate etc.), anti-spoofing capabilities (anti-spoofing protection is a must have capability for the right biometric modality), user acceptability (understanding which modalities are acceptable versus those that may cause user acceptance issues is important), cost effectiveness (depending on the underlying technology and hardware characteristics, certain modalities may be more cost effective than others), international standard and certification (there are international standards often required for large scale identification projects), compatibility (it is important that the devices are supported and compatible between the system’s operating system and the deployed biometric software) and last but not least the exact device specification”* [sublinhado nosso]

Posteriormente, através do software, permite converter em dados, usando um modelo de reconhecimento com o uso de algoritmos. Este módulo também prevê o reconhecimento de veias da palma da mão, através de sensores infravermelhos, permitindo comparar com a da base de dados.

## 1.2. Ferramenta de reconhecimento facial

Quanto ao módulo FMT<sup>231</sup>, este compara a imagem facial recolhida em tempo real com os dados da base de dados ou com o documento de identificação, autenticando o indivíduo para prosseguir. Este módulo, congrega a câmara digital (*hardware*) para tirar a fotografia, a deteção facial dessa mesma fotografia (*software*), analisando a geometria e as características faciais para o intuito de identificar o risco inerentes ao imigrante tentar dissimular a sua identidade.

Por outras palavras, este módulo pretende garantir que o indivíduo registado no sistema, seja o mesmo indivíduo que se apresenta no controlo fronteiriço (Carlos-Roca, [et al], 2018). Relativamente à sua arquitetura, esta é composta por um componente API para servir de interface para o sistema externo, ou seja, a forma de interagir com o sistema pela via da unidade portátil do guarda de fronteira.

Por outro lado, dentro deste sistema também encontramos o mecanismo de reconhecimento facial, através de algoritmos de aprendizagem automática para essa deteção, incluindo de aprendizagem profunda, em particular as redes neuronais convolucionais, fornecidos pela Herta Security. (Carlos-Roca, [et al], 2018) para processar os pontos nodais, adequando às características encontradas para incrementar a eficácia do modelo<sup>232</sup>.

---

<sup>231</sup> Relativamente ao procedimento do controlo fronteiriço (Carlos-Roca, 2018) “iBorderCtrl provides to border guards at the Border Crossing Point (BCP) a portable device and an application designed for them. The Portable Unit includes the set of devices that the border guard needs to capture information (camera, fingerprint sensor, document reader, etc.). The application guides them in the use of the devices and shows them the information gathered in the pre-registration phase. One of the steps of this process is the validation of the identity of the traveler using facial recognition.

During the BCP crossing phase three different checks are made by the FMT. The first check matches the images taken by the portable unit camera and the HD image obtained from the passport or other external system (such as Visa Information System or Schengen Information System). This check provides the risk that the person at the border crossing point is not the same one that in the documents.

If the person at the BCP is an iBorderCtrl user then the second check matches the image from the travel document with the biometric model of the user. This check measures the risk that the person in the documents is not the same one that performed the avatar interview during the pre-registration process. The third check evaluates the risk that the person at the BCP (images taken by the camera in the portable unit) is the same one that undertook the interview during the pre-registration.”

<sup>232</sup> Cfr. a hiperligação <https://hertasecurity.com/company/innovation/>

### *1.3. Ferramenta de avaliação da autenticidade do documento*

Já no módulo DAAT, assume o propósito de identificar padrões indiciantes de fraude dos documentos de viagem, visando comprovar a autenticidade dos mesmos. Estes são verificados na procura de qualquer tentativa de fraude de forma automática, pontuando com o nível de fraude. Este módulo reparte-se em duas componentes:

- I. Avaliação do risco relativo aos documentos fornecidos;
- II. Dá visibilidade das características de segurança a serem processadas

Neste sentido, para permitir o funcionamento deste módulo, são considerados diversos tipos de sensores para ler os dados dos passaportes, em particular leitores embebidos com a tecnologia OCR<sup>233</sup>, o uso da tecnologia RFID<sup>234</sup> para aceder aos dados armazenados dentro do passaporte, os códigos QR<sup>235</sup> para ler o código gerado previamente à viagem. (IBorderCtrl, 2016c)

Como já mencionamos previamente, este é um módulo típico dos controlos fronteiriços, sem trazendo grande novidade, a não ser a procura das melhores práticas internacionais conforme mencionamos previamente

---

<sup>233</sup> Definido por Reconhecimento ótico dos caracteres

<sup>234</sup> Definido por Identificação por radiofrequência

<sup>235</sup> Definido por Resposta Rápida

#### 1.4. Ferramenta de detecção de humanos ocultos

No módulo HHD, este componente visa apoiar os guardas encontrar substâncias ou pessoas escondidas dentro de viaturas ou contentores, através de raio X, ruído acústico, detetores de palpitação do coração, entre outros (IBorderCtrl, 2016b). Este último estará conectado via USB ou Bluetooth a um computador portátil ou tablet que o guardará carregará para efetuar este tipo de controlo.

Esta necessidade prende-se com a imigração ilegal, a possibilidade de tráfico de droga, tráfico de pessoas, entre outros. A imigração ilegal ocorre frequentemente por via encoberta, nomeadamente em veículos, sendo a segunda maior tendência da forma de entrada dentro da União (IBorderCtrl, 2016c, p. 92)

Relativamente ao processo de admissão dentro das fronteiras através deste módulo implementado, tal decorre da seguinte forma (Watson, 2020): *“When the traveller arrives at the border crossing, border guards will be able to use sophisticated technology to assist their checks, such as the Hidden Human Detection Tool for searching vehicles. The documents are rechecked though, because the main checks have already taken place in advance, this is for primarily verification purposes and therefore takes less time. Any areas that the algorithm flags are investigated. The final entry decision is ultimately the responsibility of a human border guard who is guided by the algorithm risk score”*.

### *1.5. Sistema externo de legado e interface social*

No que concerne ao ELSI, este assume o propósito de cruzar os dados com as outras bases de dados, de forma a garantir a interoperabilidade entre os sistemas já existentes na União. Esta componente essencial, principalmente para relacionar com a base de dados SIS II que, como vimos previamente, está separada do repositório central por questões técnicas. (iBorderCtrl, 2016a). Esta interoperabilidade permitirá realizar *queries* às diversas bases de dados de forma centralizada, com o intuito do Guarda de fronteira ter uma resposta com base na análise do registado nas várias bases de dados.

### *1.6. Ferramenta de análise integrada de controlo fronteiriço*

Por outro lado, o BCAT permite a análise de determinados padrões, dados de tráfego, dados estatísticos, entre outros, para tomar decisões estratégicas de policiamento dos guardas, para evitar atividades ilícitas, entre outras. Possibilita a análise de dados de forma avançada para também adquirir conhecimento sobre uma determinada tendência que ocorre, bem como a avaliação do próprio sistema do iBorderCtrl e a sua efetividade (iBorderCtrl, 2016a)

Posteriormente ao controlo pelo módulo HDD (Watson, 2020), *“the traveller moves on, all the data about this individual is anonymously fed back into the system. This is processed through the integrated Border Control Analytics Tool (BCAT) which seeks to identify patterns and develop knowledge which will allow the system to improve its capacity to adapt to new situations. In essence, it is recycling its output data as training data”*.

Este output será relevante para desenhar padrões mencionados previamente, para a tomada de decisões, sendo relevante ponderar a possibilidade deste modelo potenciar a discriminação. Caso não seja implementado controlos como a revisão dos dados históricos para balancear, sob prejuízo de incorrer em *overfitting* (Han, 2011) ou seja, o mesmo conjunto de dados históricos não serem possíveis de transpor para a análise de

novos dados, bem como os controlos de qualidade dos dados, caso contrário assumiram efeitos contraproducentes<sup>236</sup>.

### *1.7. Ferramenta baseada na avaliação de risco*

Concomitantemente o RBAT visa correlacionar o risco estimado da fase prévia à viagem, ao processar os dados e documentos dos imigrantes, apoiando na tomada de decisão. Após esta primeira análise prévia, será atribuído uma pontuação de vários tipos de riscos identificados, em particular, o risco dos imigrantes ao tencionarem permanecer na União sem ter informado, tornando a sua situação futura irregular.

Esta é uma ferramenta de apoio à decisão dos serviços de fronteira para admitir ou não a entrada dos imigrantes dentro da União Europeia, partindo de uma análise de risco dos elementos recolhidos nos demais módulos, procurando as irregularidades, tratando-as caso seja possível, bem como em casos onde surjam dúvida sobre determinados riscos. (IBorderCtrl, 2016a)

O peso dos componentes parte da discricionariedade dos Guardas de fronteira, podendo estabelecer regras como condições, regras como ações, bem como as características a serem definidas com maior pendor para o agente, podendo tomar como ilustrativo os dados como nome, género, nacionalidade, país de residência, endereço eletrónico, telemóvel, entre outros.<sup>237</sup>

---

<sup>236</sup> Tomemos este exemplo como ilustrativo desta preocupação em Watson (2020), “[t]he risk score is not aligned against what transpires when the person enters the country. For example, the algorithm identifies that two people who receive a similar, or even the same, risk score share the characteristics that they both have green eyes, olive skin and have liked the Starbucks Coffee page on Facebook. Regardless of whether the risk score that was attributed to these people transpired to be an accurate reflection of their behaviour when they enter the Schengen Area, this information will be used to inform decisions about similar people in the future.”

<sup>237</sup> Cfr. a hiperligação [http://www.fly-sec.eu/files/content/documents\\_1/Speakers/Presentations/iBorderCtrl\\_FLYSEC%20event\\_28Jun18\\_sm.pdf](http://www.fly-sec.eu/files/content/documents_1/Speakers/Presentations/iBorderCtrl_FLYSEC%20event_28Jun18_sm.pdf)

## 1.8. Sistema de deteção automática de mentiras

Relativamente ao funcionamento desta deteção facial de mentiras ADDS visa detetar aqueles imigrantes que se deslocam em boa fé ou não (Sánchez-Monedero, 2020). É necessário enquadrar o uso de detetores de mentiras assentes na tecnologia mais próxima desta, sendo essa o polígrafo (O’Shea, [et al.], 2018). Esta deteta as mentiras partindo das mudanças fisiológicas relacionadas com o stress, tomando o batimento cardíaco, a pressão sanguínea e os batimentos cardíacos. Na mesma esteira, também a proliferação de sistemas de deteção de mentiras começam a assumir presença, tomando, como ilustrativo, o sistema de aprendizagem automática profunda de deteção de mentiras como o *Silent Talker*.

Esta componente do *Silent Talker* do módulo ADDS trata-se um sistema de definição de perfis psicológico adaptativo<sup>238</sup>, ou seja, detetar os sinais não visuais (e.g. dados dos olhos, dados faciais, dados do angulo facial, entre outros<sup>239</sup>. Estes gestos faciais, permitem classificar com o binómio verdade/mentira e, posteriormente, definir os perfis com base na deteção desses sinais<sup>240</sup>. Para cada uma das questões<sup>241</sup> colocadas pelo Avatar<sup>242</sup>, é atribuída uma pontuação e classificação através do modelo de redes

---

<sup>238</sup> Cfr. a hiperligação <https://www.silent-talker.com>

<sup>239</sup> É reconhecido que as expressões faciais, ou seja a linguagem corporal, transmite também uma mensagem que deve ser interpretada por terceiros, aliás, no estudo da psicologia pelo Alberth Mehrabian na década de 50, sobre este tópico, refere-se que 55% da mensagem é passada pela linguagem corporal, a entoação apoia em 38% e somente 7% o conteúdo da mensagem (Pease, 2004, p. 27, disponível na hiperligação <http://index-of.co.uk/Social-Interactions/The%20Definitive%20Book%20of%20BODY%20LANGUAGE%20-%20Barbara%20Pease.pdf> )

<sup>240</sup> Existem certas particularidades que devem ser compreendidas, desde logo a necessidade dos focos de luz incidirem frontalmente no indivíduo, sob prejuízo de caso desse foco de luz produzir sombras, resultando numa avaliação do *avatar* menos eficaz (IBorderCtrl, 2016b, p. 14)

<sup>241</sup> Essas questões são as seguintes (O’Shea, et al, 2018):

1 What is your family name?

2 What is in your case?

3 Have you seen any posters of prohibited items?

4 Are there any items from the lists of prohibited items in your case?

5 How many items are in the case?

6 If you open the case and show me what is inside, will it confirm that your answers were true?

7 What is your first name?

8 When were you born?

9 Where were you born?

10 What is your current citizenship?

11 Please tell me the name of a friend or family member who can confirm your identity?

12 What is the relationship of this person to you?

13 Where does this person live?

<sup>242</sup> Para o entendimento da definição do *avatar*, este pode ser definido como um agente conversacional que “is an AI system that engages a human user in conversation to achieve some practical goal, usually a task perceived as challenging by the user (...) The state of the art of this combination of technologies suggest that Avatars will be suitable for detecting deception in border crossing interviews, as they are effective extractors of information from

neuronal, atualiza o servidor da base de dados, alterando no fim a atitude do *avatar* com base na pontuação de risco atribuída ao viajante (O’Shea, [et al.], 2018)

Este componente da *iBorderCtrl* integra um pré-processamento para embranquecer a imagem<sup>243</sup>, posteriormente alavancar com o algoritmo de *back propagation* no modelo das redes neuronais artificiais, assentes em tecnologia de *Deep Learning*<sup>244</sup>, podendo esta necessidade ser prejudicial para indivíduos com a tonalidade da pele mais escura (Sánchez-Monedero, 2020). Em particular, utiliza biomarcadores para verificar a mentira, avaliando micro expressões faciais não verbais, prevendo se estará a mentir ou não<sup>245</sup>.

Este modelo, tendo sido testado pelos especialistas, reparou que, ao estudar este módulo do projeto *iBorderCtrl*, que as taxas na matriz de confusão, ou seja, onde comparamos os resultados onde 73,6 % dos resultados deu positivo, ao detetar a mentira quando a pessoa realmente mentiu e, 24,45% dos resultados deu positivo, ao detetar a mentira quando a pessoa realmente não mentiu, e, por outro lado, também o resultado de falsos negativos é alto, no sentido de 26,34% dos inquirido não deu resultado positivo, quando a pessoa esta a mentir.

Para a operacionalização adequada deste módulo, é relevante compreender os sinais do foro psicológico do imigrante, pois em virtude das experiências anteriores, poderá ser evidente a exteriorização de comportamentos indiciantes de perturbações. Essas, possivelmente, foram provocadas por experiências negativas ou pela perseguição por motivos de natureza política, raça, entre outros.

Conforme menciona Molnar (2020), “*it is unclear how this system will be able to handle cultural differences in communication or account for trauma and its effects on memory, such as when dealing with a traumatized refugee claimant. Refugee and immigration claims are filled with nuance and complexity, qualities that may be lost on*

---

*humans and therefore can applied to deception detection tasks. Secondly, they can provide dynamic responses to user inputs and can simulate affective signals”* (O’Shea, et al, 2018).

<sup>243</sup> Cfr. Idem, pp. 1-7

<sup>244</sup> No caso das Redes neuronais, recorre-se à compreensão do funcionamento do cérebro para transpor para as redes neuronais. Por sua vez, reparte-se numa componente da aprendizagem onde será detetado as características que foram previamente filtradas por camadas do *input* dos dados, as camadas ocultas e, subsequentemente, o *output*. Este *input* parte dos dados históricos que servem para analisar os dados atuais.

<sup>245</sup> Cfr. Sánchez-Monedero, et al, 2020, p. 6

*automated technologies, leading to serious breaches of internationally and domestically protected human rights in the form of bias, discrimination, privacy breaches, and due process and procedural fairness issues, among others.”*

## 2. Proteção dos direitos dos imigrantes?

Neste sentido, este sistema contempla avanços significativos na ciência dos controlos fronteiriços automatizados, incorporando as tendências atuais da tecnologia da inteligência artificial, bem como algumas das melhores práticas. Contudo é relevante considerara alguns aspetos negativos que merecem foco, partindo da ótica do direito à proteção de dados enquanto meta-direito, verificamos no desenho deste sistema certas vulnerabilidades que podem comprometer a proteção dos direitos dos imigrantes neste sistema do iBorderCtrl:

- I. Tomada de decisões com base em taxas de eficácia reduzidas, pelo menos no módulo de deteção de mentiras, por conseguinte, essa incerteza caso não seja revista por algum indivíduo, em última análise, estaremos a tomar decisões erradas com efeitos sobre a esfera jurídica do imigrante.
- II. Para nós, a mera inserção de um botão de pânico para essas situações não é suficiente, pois o indivíduo poderá inequivocamente transmitir esses gestos faciais sem este aperceber-se e dizendo a verdade, tão pouco a carta a explicitar o tratamento servirá, uma vez que não é transmitido a informação sob o funcionamento do algoritmo devido aos interesses comerciais. Recomendamos a doutrina da legibilidade para o entendimento do algoritmo e as suas consequências.
- III. A decisão fundada num grau de certeza de 75% não deve consubstanciar uma decisão, sob prejuízo de aceitar-se margens de erros demasiado amplas com efeitos nocivos na esfera dos imigrantes. Neste sentido, parece relevante ponderar sobre as métricas a serem estabelecidas quando relacionando com o tratamento de dados pessoais pela via de decisões automatizadas, exigindo-se taxas de erro inferiores às mencionadas previamente, também repartidas por grupos repartidos no conjunto de dados históricos, para evitar a discriminação em virtude de características étnicas, tonalidade, género entre outras.
- IV. Mesmo com dados aparentemente objetivos, parece ser necessário compreender o tipo de pontuação dado ao *input*, como tivemos oportunidade de mencionar no caso do módulo RBAT, o peso atribuído a

cada uma das categorias em análise, os vetores analisados com as ferramentas de *deep learning*, devem ser escrutinados, pois o seu uso ainda deve ser amplamente estudado para compreendermos as operações que decorrem internamente nas camadas das redes neuronais.

- V. Por outro lado, ao utilizar algoritmos subjacentes ao funcionamento de redes neuronais, coloca-se em causa a transparência e visibilidade do funcionamento real do modelo. Tal deve-se à existência de camadas ocultas, cujo funcionamento é ainda pouco perceptível pelos especialistas, resultando no fenómeno de “*black box*”. Desta feita, tomemos como ilustrativo a não divulgação das informações relativas ao projeto do iBorderCtrl. Ou seja, é perceptível conhecer os inputs e os outputs, mas não o raciocínio matemático dentro do algoritmo. Esta ponderação não poderá ser escondida por questões de performance, as quais podem ser amplamente afetadas caso as técnicas utilizadas sejam assentes na aprendizagem autónoma, com algoritmos com menor eficácia.
- VI. Análise de características comportamentais que podem comprometer o resultado final, reconhecendo que alguns imigrantes poderão deslocar-se do seu país de origem por motivos políticos, como é o caso da guerra ou da perseguição, podendo permanecer danos psicológicos nesse indivíduo e, esses indicadores, poderem ser perspetivados como indiciantes de mentira. Parece necessário possibilitar a recusa do tratamento automatizado informada pela via da deteção de mentiras, sem que seja negada a entrada.

Mesmo este direito não ser reconhecido como um direito absoluto, na aceção do n.º 2 do artigo 8.º da CDFUE, deverá orientar a restrição deste direito fundamental nos termos do n.º 1 do artigo 52.º da CDFUE. Seguindo a metodologia da AEPD (2020), parece ser necessário segmentar a análise principalmente nos módulos da ADDS e a HHD apresentado no sistema iBorderCtrl, conduzindo um conjunto de tópicos a serem avaliados<sup>246</sup>. Relativamente à legitimidade no espírito da lei, o foco passa pelo

---

<sup>246</sup> Em particular, as seguintes fases elencadas com as respetivas instruções baseadas na doutrina, bem como na jurisprudência europeia (AEPD, 2020):

consentimento<sup>247</sup>, contudo, este consentimento só é efetivo se na operacionalização deste modelo mantenha-se a possibilidade discricionária de submeter a este controlo com base em decisões automatizadas.

Relativamente à essência do direito, a retenção desses dados das questões na base de dados centralizada, bem como a interoperabilidade com as outras bases de dados, permitindo definir os perfis, extravasa o direito à privacidade que, por um lado, poderá comprometer a entrada do imigrante com base nos registos e, por outro lado, também dificultará terceiros que apresentem-se com características semelhantes desse imigrante, coincidindo com os dados históricos nas ferramentas de análise. Contudo, o módulo do HHD, por assumir interesses transnacionais de criminalidade encoberta, desde que o intuito não se confunda com a imigração ilegal, trata-se de interesses conjunto das partes, quer do imigrante, quer do Guarda de fronteira.

No que concerne ao respeito do interesse público, é reconhecido nas diversas agendas esse interesse em combater a imigração irregular, habilitando este sistema a combater a imigração por via oculta em veículos, a imigração irregular por excesso de tempo de estadia, dissuadindo o guarda de fronteiras sobre a sua permanência, a tentativa de entrada noutra país da União e, por fim, limitar as deslocações internas destes imigrantes, tratando assim de dados sensíveis (e.g. biométricos, clínicos, nacionalidade)<sup>248</sup>

Quanto à proporcionalidade da medida, ao tentarmos controlar os sinais não visuais dos migrantes, atribuindo uma pontuação de risco com os avatares, estamos a tomar decisões com base em exteriorizações que poderão não traduzir realmente a maneira como imigrante encara a sua estadia na União, procurando ou não deslocar-se

---

*“Step 1: assess the importance (‘legitimacy’) of the objective and whether and to what extent the proposed measure would meet this objective (effectiveness and efficiency);*

*Step 2: assess the (scope, extent and intensity of the) interference in terms of effective impact of the measure on the fundamental rights to privacy and data protection*

*Step 3: proceed to the fair balance evaluation of the measure*

*Step 4: analyse conclusions on the proportionality of the proposed measure. If the conclusion is ‘not proportionate’, identify and introduce safeguards which could make the measure proportionate.”*

<sup>247</sup> Nos termos da alínea a) do n.º 1 do artigo 6.º, sendo escrutinado no artigo 7.º do RGPD e o considerando 32.º do mesmo diploma

<sup>248</sup> Nos termos da alínea g) do n.º 2 do artigo 9.º do RGPD, é admissível o tratamento por interesse público caso respeita a essência, preveja medidas adequadas que salvaguardem os direitos fundamentais e os interesses dos titulares.

em boa fé. Para nós, para o objetivo em particular não é excessiva pelo fundamento deste objetivo ter um escopo demasiado alargado, com carácter amplamente subjetivo, não devendo servir de objetivo para este controlo, pois a adequação partirá da avaliação para atingir um conceito vago que, conforme mencionado pela doutrina, no caso do DAAT, está comprovada a ineficácia deste modelo, bem como de técnicas de deteção de mentiras, pelas restrições mencionadas previamente. Por fim, a necessidade dessa medida é reconhecida para conseguirmos controlar os fluxos imigratórios que podem tornarem-se irregulares, pese embora os modelos atuais não sirvam esse propósito.

Caso reparemos nos parceiros para este projeto, reparamos que estão externalizados os módulos deste sistema para entidades terceiras, carecendo a análise de risco de terceiros, com o intuito destes implementem salvaguardas que protegem os dados. Conjuntamente, dentro de cada módulo, também verificamos subcomponentes que estão sobre a tutela de terceiros para efeitos de propriedade intelectual, o que dificulta a transparência e a capacidade de auditá-los. Neste sentido, no cenário apresentado atual deste sistema, existem inúmeras vulnerabilidades que não podem ser mitigados os riscos com controlos, como é o caso da deteção de mentiras, somente se houver a possibilidade de atribuir a discricionariedade no migrante de recusar esse controlo, tendo ser previamente informado.

Neste panorama deste sistema iBorderCtrl, com a capacidade de criar a interoperabilidade com os sistemas de informação existentes na União, é recomendado que seja escrutinada a necessidade dos dados recolhidos no âmbito dos outros controlos fronteiriços, em particular, com a sensibilidade das parcerias de entidades privadas com acesso a essas informações sensíveis e, por outro lado, Estados com regimes autoritários com acesso a esses mesmos dados, podendo resultar no aumento da discriminação num controlo preventivo dos fluxos através da segurança e não no investimento nas *root causes*.

Categorias	Melhorias
Sistema do iBorderCtrl	<ul style="list-style-type: none"> <li data-bbox="502 1868 1378 2024">• Possibilitar a recusa do tratamento automatizado informada pela via da deteção de mentiras, sem que seja negada a entrada.</li> </ul>

	<ul style="list-style-type: none"> <li>• Corrigir as taxas de erro do modelo.</li> <li>• Utilizar técnicas com maior compreensão científica, para efeitos de transparência.</li> <li>• Introduzir mecanismos de controlo da qualidade dos dados.</li> </ul>
Técnicas de inteligência artificial	<ul style="list-style-type: none"> <li>• Analisar o código fonte</li> <li>• Verificar os dados históricos</li> <li>• Controlar o input</li> <li>• Analisar a taxa de eficácia</li> <li>• Aplicar a legibilidade</li> </ul>
Interoperabilidade	<ul style="list-style-type: none"> <li>• Rever a necessidade dos dados recolhidos</li> <li>• Restringir a partilha de dados na plataforma de pesquisa ao necessário, sob prejuízo de acentuar a criminalização do imigrante</li> </ul>

## Considerações finais

Como já tivemos oportunidade de mencionar, as ferramentas tecnológicas são de tremenda utilização no controlo dos fluxos migratórios da União, permitindo a monitorização, a vigilância e, em determinadas situações, tomando como ilustrativo o projeto do iBorderCtrl, através do uso de algoritmos baseados em técnicas de aprendizagem automática, antecipar uma decisão sobre a entrada ou recusa face a um conjunto de pressupostos posteriormente validados por mão humana.

Caso mencionemos a possibilidade da interoperabilidade entre os sistemas de informação da UE com este sistema, podemos depreender a possibilidade da definição de perfis com base em dados que revelam, por um lado, dados pessoais armazenados nas diversas bases de dados, incluindo traços pessoais, comentários dos guardas de fronteira, dados que caracterizam esse imigrante. Por outro lado, através deste projeto, é possível extrair dados não visuais, conforme mencionado, que podem indiretamente caracterizar dados de saúde (e.g. depressão).

Já na dimensão da avaliação do modelo relativo à deteção de mentiras, é relevante perceber que a taxa de falsos positivos e falso negativos é muito alta, de acordo com o estudo ao projeto do iBorderCtrl, bem como estes projetos, ao manobrar com dados pessoais, parte deles sensíveis (e.g. dados biométricos), deverá ser salvaguardada com medidas de segurança adequadas, sendo que o uso de programas em fonte aberta aumentam a superfície de exposição, a menos que haja um acompanhamento contínuo no seu desenvolvimento.

Relativamente ao quadro geral dos sistemas de informação da UE, reparemos algumas particularidades que capturam a nossa atenção face à necessidade de medidas de segurança para a promoção do direito à segurança e à privacidade dos migrantes, devendo colocar as seguintes questões de segurança e proteção de dados:

- I. Gerir os riscos de terceiros na partilha e tratamento dos dados com o setor privado? E com os outros Estados?
- II. Segregação das responsabilidades? Com a devida restrição de acessos?
- III. Segurança no desenvolvimento web?

- IV. Baseline dos eventos de segurança? Com o registo dos *logs* dos diversos dispositivos?
- V. Resposta a incidentes de segurança? Com planos definidos?
- VI. Definição de perfis? Com o acesso a dados irrestritamente das várias bases de dados?

É necessário compreender que a integração de diversos tipos de dados que, mesmo que não sejam os dados sensíveis em sentido estrito, nos termos do RGPD, existem inúmeros outros dados que podem descrever indiretamente dados sensíveis, podendo tomar como ilustrativo a alimentação que determinado indivíduo tenha (PNR), determinadas roupas que possam induzir uma determinada religião (ETIAS), a nacionalidade conjugada com a função no país proveniente, poderá indiretamente revelar a etnia desse indivíduo. Como tal, é possível incorrer indiretamente em discriminação dos titulares dessas características/dados

No espaço da União, ao ser permitido o uso de técnicas intrusivas com potencial limitador de direitos fundamentais aos imigrantes, o seu efeito poderá ser extensivo, tomando como exemplificativo a tentativa da criação de bases de dados europeias para centralizar os dados biométricos, nos termos da proposta 2018/0104/COD prévia ao Regulamento (EU) 2019/1157 relativo à documentação de identidade e residência, não tendo avançado. Ao referir este caso, também é possível verificar no Regulamento (UE) 2017/458 o aumento do controlo estendido aos cidadãos europeus nos casos previstos do mesmo.

Esta recolha abusiva poderá interpelar a padrões discriminatórios, quer pelos próprios serviços de fronteira, tomando sinais subjetivos, quer através do uso de ferramentas de aprendizagem automática, onde os dados carregados como dados históricos encontram-se enviesados, podendo discriminar a posição do migrante. É imprescindível perceber ainda que, ao aumentar o uso de sistemas de informação, aumenta-se inequivocamente a superfície de exposição dos dados, ou seja, a probabilidade desses dados dos imigrantes serem exfiltrados é maior.

Para nós, a articulação com as diversas bases de dados com este sistema da iBorderCtrl não salvaguarda os direitos fundamentais do migrante estritamente

tecnológicos, pelos fundamentos previamente elencados. Desta feita, respondendo à questão de partida: (P1) *Será que a posição dos imigrantes face às tecnologias de controlo dos fluxos migratórios tem vindo a ser acompanhado com medidas adequadas de segurança e privacidade, em particular nos sistemas de informação da UE, nomeadamente no projeto iBorderCtrl?*

Para nós, a resposta será negativa, pela circunstância deste sistema envolver uma quantidade de dados, por um lado, dados sensíveis que podem revelar traços únicos que identificam uma pessoa (e.g. como a condição clínica do próprio migrante), recolha de dados não visuais para a tomada de decisões sem a salvaguarda dos interesses do imigrante e, por outro lado, submete à avaliação discricionária do Guarda para atribuir certas regras nalguns módulos, no uso de ferramentas com tecnologias complexas, pouco transparentes na tomada de decisões, sem considerar as experiências do imigrante. Como tal, a (H2) *Não estão implementados os controlos de segurança e privacidade adequados nas ferramentas tecnológicas da UE, no sistema iBorderCtrl que salvaguardam a posição do imigrante*

Para que este sistema possa ser considerado admissível, os módulos a serem utilizados devem atender a uma ponderação da garantia dos direitos do imigrante ao longo do processo dos fluxos migratórios, compreendendo que o módulo de deteção de mentiras pode limitar direitos de um processo equitativo em prol da tonalidade (i.e. dificuldade em reconhecer tons escuros), das condições ambientais (i.e. focos de luz), a por desigualdade das posições, devendo ser nivelada com a possibilidade de recusar e exigir somente a presença humana do Guarda de Fronteiras.

Relativamente ao conjunto dos módulos que utilizam técnicas de aprendizagem profunda, que, pelas suas características são ocultas o processamento dentro das redes neuronais. É muito importante considerar que, no uso de qualquer modelo, deverá ser compreendido o código fonte, ou seja, supervisionar os erros, o modo de funcionamento deste sendo testado, compreender a entropia dos dados históricos que servem o modelo, garantindo que os elementos que são utilizados não sejam discriminatórios, que o input realizado a este modelo não seja tendencial para um determinado output, e, por fim, que as taxas de eficácia do modelo sejam consideráveis, devendo estabelecer parâmetros

aceitáveis na comunidade internacional. Neste sentido, devemos ainda de apelar ao conceito de legibilidade para o entendimento do imigrante na dimensão do funcionamento básico, bem como as consequências desse processamento.

Para próximos estudos nas áreas nos sistemas de informação da UE utilizados para o controlo dos fluxos migratórios, recomendamos certos tópicos indagados durante esta investigação, reconhecendo que as mesmas saiam do escopo do âmbito desta investigação, em particular o estudos dos variados sistemas de informação da UE para a vigilância marítima, o estudo dos diversos tipos de controlo fronteiriços automatizados, bem como o impacto das notícias falsas nos migrantes como dissuasores dos fluxos e potenciadores do discurso de ódio.

## **Bibliografia**

### Livros

AKKERMAN, M., 2018, *Expanding the Fortress: The policies, the profiteers and the people shaped by EU's border externalisation programme*, Transnational Institute and Stop Wapenhandel, pp. 22 e ss.

ALLINSON, K., 2018, *The right to be recognised as a person*, in Elspeth Guild, Stephanie Grant, CA Groenendijk (eds) *Human Rights of Migrants in the 21<sup>st</sup> Century*, pp. 16-20. Doi 10.4324/9781315145396

ANDRADE, P., G., 2015, *EU Cooperation with Third Countries In The Field Of Migration*, Technical Report, Study of the European Parliament, Policy Department of Citizens' rights and Constitutional Affairs, 2015/PE 536.469, [Migration Policy Centre] pp. 23 e ss.

ANES, J., M., 2015, *Criminalidade Organizada* in Enciclopédia de Direito e Segurança, Edições Almedina, Coimbra, pp. 89-94.

APAP, J., RADJENOVIC, A., e DOBREVA, A., 2019, *A questão da migração* in Políticas da UE – Ao serviço dos cidadãos, EPRS - Serviço de Estudos do Parlamento Europeu, p. 10-14

ASCENSÃO, J. O. (2008). A dignidade da pessoa e o fundamento dos direitos humanos. *Revista Da Faculdade De Direito, Universidade De São Paulo*, 103, pp. 277-299. Disponível na hiperligação <http://www.revistas.usp.br/rfdusp/article/view/67806> [última consulta a 23 de novembro]

BEDUSCHI, A., 2020, *International migration management in the age of artificial intelligence*, Migration Studies, mnaa003 pp. 1-21, disponível na hiperligação <https://doi.org/10.1093/migration/mnaa003>

BENEDICTO, A., e BRUNET, P., 2018, *Building Walls: Fear and Securitization in the European Union*. Centre Delàs d'Estudis per la Pau. Report no. 35, September. pp. 1-58, disponível em [https://www.tni.org/files/publication-downloads/building\\_walls\\_-\\_full\\_report\\_-\\_english.pdf](https://www.tni.org/files/publication-downloads/building_walls_-_full_report_-_english.pdf). [última consulta a 23 de novembro]

BOSWORTH, M. (2016) Juxtaposed Border Controls and Penal Power on the French North Coast. Disponível em: <https://www.law.ox.ac.uk/research-subject-groups/centre-criminology/centreborder-criminologies/blog/2016/02/juxtaposed-border>. [última consulta a 23 de novembro]

BROUWER, E., 2011, *Legal Boundaries and the Use of Migration Technology* in: Dijstelbloem H., Meijer A. (eds) *Migration and the New Technological Borders of Europe* Migration, Minorities and Citizenship. Palgrave Macmillan, London. [https://doi.org/10.1057/9780230299382\\_6](https://doi.org/10.1057/9780230299382_6), pp. 134-169

BUSE, R. P., e WEIMER, W. R., 2009, Learning a metric for code readability. *IEEE Transactions on Software Engineering*, 36(4), 546-558.

CANTARERO, D. C., HERRERO, D. A. P., e MÉNDEZ, F. M., 2013, A multi-modal biometric fusion implementation for ABC systems in *2013 European Intelligence and Security Informatics Conference*, pp. 277-280, IEEE.

CARLOS-ROCA, L.R., TORRES, I.H., e TENA, C., 2018, *Facial recognition application for border control* in 2018 International Joint Conference on Neural Networks (IJCNN), pp. 1-7.

CARRETO, J., 2018, *A Política Europeia de Vizinhança*, in *Revista de Direito e Segurança* Ano VI, Número 12, FDUNL, pp. 81-101, disponível na hiperligação [http://cedis.fd.unl.pt/wp-content/uploads/2019/01/RDeS-nº-12-on-line\\_versão-sem-menção-projeto\\_comprimido.pdf](http://cedis.fd.unl.pt/wp-content/uploads/2019/01/RDeS-nº-12-on-line_versão-sem-menção-projeto_comprimido.pdf) [última consulta a 23 de novembro]

COLLIN, S., KARSENTI, T., e CALONNE, O., (2015). Migrants' Use of Technologies: An Overview of Research Objects in the Field. *Journal of Technologies and Human Usability*. 10, pp. 15-29. 10.18848/2381-9227/CGP/v10i3-4/56424.

COUTINHO, L., P., 2017, *A Realidade Internacional, Introdução à Teoria das Relações Internacionais*, 2ª edição, AAFDL Editora, pp. 109 e ss.;

D'ALFONSO, A., 2019, *External border control and asylum management as EU common goods: A budgetary perspective*, Robert Schuman Centre for Advanced Studies, European University Institute, p. 1-68. Disponível na hiperligação

[https://cadmus.eui.eu/bitstream/handle/1814/61044/RSCAS%202019\\_05rev.pdf?sequence=4&isAllowed=y](https://cadmus.eui.eu/bitstream/handle/1814/61044/RSCAS%202019_05rev.pdf?sequence=4&isAllowed=y) [última consulta a 23 de novembro]

DE GENOVA, N., 2017, *The Borders of “Europe”, Autonomy of Migration, Tactics of Bordering*. Durham; London: Duke University Press, pp. 1-376. doi:10.2307/j.ctv11smr05

DIJSTELBLOEM, H., MEIJER, A., e MICHIEL, B., 2011, The Migration Machine in: Dijnstelbloem H., Meijer A. (eds) *Migration and the New Technological Borders of Europe* Migration, Minorities and Citizenship. Palgrave Macmillan, London. pp. 1-21. Doi 10.1057/9780230299382

DOMINGUES, P., 2015, *O algoritmo mestre*, Como a busca pelo algoritmo de machine learning definitivo, Novatec, pp. 1-377;

EDWARDS, L., e VEALE, M. (2017). Slave to the algorithm: Why a right to an explanation is probably not the remedy you are looking for. *Duke L. & Tech. Rev.*, 16, 18, pp. 18-84. Disponível na hiperligação [https://discovery.ucl.ac.uk/id/eprint/1574817/1/Veale\\_slavetothealgorithm\\_published.pdf](https://discovery.ucl.ac.uk/id/eprint/1574817/1/Veale_slavetothealgorithm_published.pdf) [última consulta a 23 de novembro]

EULE, T., G., [et al.], 2019, *Decision-Making and the Role of Law* in: Eule, T. G., Borrelli, L. M., Lindberg, A., & Wyss, A. (2019). *Migrants Before the Law. Contested Migration Control in Europe*. Cham: Springer International Publishing, pp. 81-110. Doi 10.1007/978-3-319-98749-1

FERREIRA, A., F., 2018, *Profiling e algoritmos autónomos: um verdadeiro direito de não sujeição?* In *Anuário de Proteção de Dados 2018*, pp. 35-44

FRA, 2017, *Fundamental Rights and the interoperability of EU Information systems: borders and security*, pp. 1-56. Disponível na hiperligação [https://fra.europa.eu/sites/default/files/fra\\_uploads/fra-2017-interoperability-eu-information-systems\\_en-1.pdf](https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-interoperability-eu-information-systems_en-1.pdf)

FRA, 2018a, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, p. 1-135. Disponível na hiperligação <https://fra.europa.eu/en/publication/2018/under->

[watchful-eyes-biometrics-eu-it-systems-and-fundamental-rights](#) [última consulta a 23 de novembro]

FRA, 2018b, *How eurosur regulation affects fundamental rights*, pp. 1-32. Disponível na hiperligação [https://fra.europa.eu/sites/default/files/fra\\_uploads/fra-2018-eurosur-regulation-fundamental-rights-impact\\_en.pdf](https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-eurosur-regulation-fundamental-rights-impact_en.pdf) [última consulta a 23 de novembro]

FRA, 2018c, *Preventing unlawful profiling today and in the future: a guide*, pp. 1-138. Disponível na hiperligação <https://fra.europa.eu/en/publication/2018/preventing-unlawful-profiling-today-and-future-guide> [última consulta a 23 de novembro]

FREITAS, V., 2020, *A Regulação Jurídica do Ciberespaço – Mutação do paradigma à luz do Acórdão James Elliot do TJUE*, Revista de Cyberlaw do CIJIC, n.º 9, março de 2020 pp. 1-36

GERARDS, J., 2019, *The Fundamental rights challenges of algorithms*, Netherlands Quarterly of Human Rights, 37(3), pp. 205-209. DOI: <https://doi.org/10.1177/0924051919861773>

GIL, A., R., 2016, *A proteção derivada de direitos fundamentais de imigração*, Tese de Doutoramento em Direito Público, Faculdade de Direito da Universidade Nova de Lisboa, Portugal, pp. 100 e ss. Disponível em <http://hdl.handle.net/10362/19078> [última consulta a 23 de novembro]

GIL, A., R., 2017, Imigrante in Enciclopédia de Direito da União, Petrony

GIL, A., R., 2018, *O Direito das Migrações como um "novo" Ramo do Direito Público* in Ana Gouveia Martins, Anabela Leão, Benedita Mac Crorie, Patrícia Fragoso Martins (org.) AA.VV., Atas do XI Encontro de Professores de Direito Público - Direito Público e Direitos Públicos: Pontes, Diálogos e Encruzilhadas, Universidade do Porto, pp. 207-222

GORODNICHY, D., YANUSHKEVICH, S., e SHMERKO, V., (2014), Automated border control: Problem formalization, *2014 IEEE Symposium on Computational Intelligence in Biometrics and Identity Management (CIBIM)*, Orlando, FL, 2014, pp. 118-125. DOI: 10.1109/CIBIM.2014.7015452.

GOUVEIA, J., B., 2015a, *Direito Internacional da Segurança*, Edições Almedina, Coimbra, pp. 1-171

GOUVEIA, J., B., 2015b, *Direitos Fundamentais* in *Enciclopédia de Direito e Segurança*, Edições Almedina, Coimbra, pp. 161-165

GOUVEIA, J., B., 2018, *Direito da Segurança, Cidadania, Soberania e Cosmopolitismo*, (1 ed.) Almedina, pp. 970 e ss.

GRUPO DE TRABALHO DO ARTIGO 29.º, 2018, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP251rev.01, adotadas a 3 de outubro de 2017, revista a 2018, p. 1-37

HAN, J., KAMBER, M. e PEI, J., 2011, *Data Mining: Concepts and Techniques*, 3rd Edition. Morgan Kaufmann Publishers, Waltham pp. 1-39 e 393-442. DOI: 10.1016/C2009-0-61819-5

HAYES, B., 2017, Migration and data protection: Doing no harm in an age of mass displacement, mass surveillance and “big data”. *International Review of the Red Cross*, 99(904), pp. 179-209. DOI: 10.1017/S1816383117000637

HECKMANN, F., HONECOPP, E., e CURRLE, E., 2009, *Guest worker programs and circular migration: what works*, Immigration Paper Series, 9, pp. 1-17

HELLER, C., e PEZZANI, L., 2017, *Liquid Traces: Investigating the Deaths of Migrants at the EU's Maritime Frontier* in *The Borders of “Europe” Autonomy of Migration, Tactics of Bordering*, pp. 101 e ss. Disponível na hiperligação <https://doi.org/10.1215/9780822372660-004>

IBORDERCTRL, 2016a, First version of tech tools and subsystems redacted, disponível na hiperligação <https://www.asktheeu.org/de/request/6087/response/19711/attach/html/4/8%20D3%202%20First%20version%20of%20tech%20tools%20and%20subsystems%20redacted.pdf.html> [última consulta a 23 de novembro]

IBORDERCTRL, 2016b, 2nd version of all tech tools and subsystems for integration redacted, disponível na hiperligação

<https://www.asktheeu.org/de/request/6087/response/19711/attach/html/3/9%20D3%203%202nd%20version%20of%20all%20tech%20tools%20and%20subsystems%20for%20integration%20redacted.pdf.html> [última consulta a 23 de novembro]

IBORDERCTRL, 2016c, Data Collection Devices specifications redacted, disponível na hiperligação <https://www.asktheeu.org/de/request/6087/response/19711/attach/html/2/7%20D3%201%20Data%20Collection%20Devices%20specifications%20redacted.pdf.html> [última consulta a 23 de novembro]

IBORDERCTRL, 2016d, Yearly communication report including communication material, disponível na hiperligação <https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5be014692&appId=PPGMS> [última consulta a 23 de novembro]

IBORDERCTRL, 2016e, Yearly report of the communication plan and material 2, disponível na hiperligação <https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c719c0b8&appId=PPGMS> [última consulta a 23 de novembro]

JONES, C., 2019, *Monitoring “secondary movements” and “hotspots”*: Frontex is now an internal surveillance agency, Statewatch Analysis, Volume 21, Number 11, pp. 1-8. Disponível na hiperligação <https://www.statewatch.org/analyses/2019/monitoring-secondary-movements-and-hotspots-frontex-is-now-an-internal-surveillance-agency/> [última consulta a 23 de novembro]

JONES, C., 2020, *Automated Suspicion*, EU Travel Data-Gathering/Surveillance Plans - How Will They Affect Me?, Biometric Europe: imposing digital identities in the name of security’ Statewatch p. 1-38

KALPOKAS, 2019, *Algorithmic Governance*, Politics and Law in the Post-Human Era, Palgrave Pivot p. 1-48. Doi: 10.1007/978-3-030-31922-9

KANT, E., 1995, *A Paz Perpétua e Outros Opúsculos*, traduzido por Artur Morão, Edições 70, Lisboa, pp. 1-55. Disponível na hiperligação

<https://www.marxists.org/portugues/kant/1795/mes/paz.pdf> [última consulta a 23 de novembro]

KARAMANIDOU, L. (2015). The securitisation of European migration policies: perceptions of threat and management of risk. In G. Lazaridis, & K. Wadia (Eds.), *The Securitisation of migration in the EU: Debates since 9/11*, The European Union in International Affairs Palgrave Macmillan, pp. 37-61. disponível na hiperligação [https://doi.org/10.1057%2F9781137480583\\_3](https://doi.org/10.1057%2F9781137480583_3)

KEHL, D., [et al.], 2017, *Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing*, Responsive Communities Initiative, Berkman Klein Center for Internet & Society, Harvard Law School, pp. 1-36. Disponível na hiperligação <http://nrs.harvard.edu/urn-3:HUL.InstRepos:33746041> [última consulta a 23 de novembro]

KING, R., 2012, *Theories and Typologies of Migration: An Overview and A Primer*. Willy Brandt Series of Working Papers in International Migration and Ethnic Relations. 12. 1-43.

KLUG, A., E HOWE, T., 2010, *The Concept of State Jurisdiction and the Applicability of the Non-Refoulement Principle to Extraterritorial Interception Measures*, in *Extraterritorial Immigration Control*, pp. 69-101.

KOKA, E., E VESHI, V., 2019, *Irregular Migration by Sea: Interception and Rescue Interventions in Light of International Law and the EU Sea Borders Regulation*, *European Journal of Migration and Law*, 21(1), pp. 26-52. Doi: <https://doi.org/10.1163/15718166-12340041>

LA DIEGA, G., 2018, *Against the Dehumanisation of Decision-Making Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information*, pp. 3-34

LAUC, D., 2020, *Machine Learning and the Philosophical Problems of Induction* in: Skansi S. (eds), *Guide to Deep Learning Basics, Logical, Historical and Philosophical Perspectives* Springer, Cham, p. 93-106. Doi: [https://doi.org/10.1007/978-3-030-37591-](https://doi.org/10.1007/978-3-030-37591-1)

1

MACNISH, K., [et al.], 2020, *Predictive Policing in 2025: A Scenario*, in *Policing in the Era of AI and Smart Societies*, Advanced sciences and technologies for security applications . Cham, Switzerland, Online pp. 199-215. Doi: 10.1007/978-3-030-50613-1

MAGGIOLINO, M., 2019, *EU Trade Secrets Law and Algorithmic Transparency*, in Aida. *Annali Italiani Del Diritto D'autore, Della Cultura e Dello Spettacolo* pp. 1-16. Disponível na hiperligação <http://hdl.handle.net/11565/4013803> [última consulta a 23 de novembro]

MALGIERI, G., 2019, *Automated decision-making in the EU Member States: The right to explanation and other “suitable safeguards” in the national legislations*, *Computer Law & Security Review*, Volume 35, Issue 5, pp. 1-26

MITSOLEGAS, V., 2014 *The Criminalisation of Migration in Europe, Challenges for Human Rights and the Rule of Law*, Springer International Publishing, DOI 10.1007/978-3-319-12658-6, pp. 1-110.

MOLEIRINHO, P., 2014, *Partilha de intelligence – limites e interferências* in *Revista de Direito e Segurança*, Ano III, número 5, p. 247-271. Disponível na hiperligação <http://cedis.fd.unl.pt/wp-content/uploads/2017/06/REVISTA-RDeS-nº-5.pdf>

MOLNAR, P., 2019, *New technologies in migration: human rights impacts in: Forced Migration Review*, n.º 61, University of Oxford, pp. 7-9. Disponível na hiperligação <https://www.fmreview.org/ethics>

MOLNAR, P., 2020, *AI and Migration Management in: Dubber, M., D., Pasquale, F., e Das, S. (eds.) The Oxford Handbook of Ethics of AI*, Oxford University Press, pp. 769-788. DOI: 10.1093/oxfordhb/9780190067397.013.49

MORENO-LAX, V., 2014, *Life After Lisbon: EU Asylum Policy as a Factor of Migration Control In: D.A. Arcarazo & C.C. Murphy (Eds.). EU Security and Justice Law: After Lisbon and Stockholm.*, London: Hart Publishing Ltd, pp. 146–167, disponível na hiperligação <http://dx.doi.org/10.5040/9781474201179.ch-009> [última consulta a 23 de novembro]

MÜLLER, P., E SLOMINSKI, P., 2020, *Breaking the legal link but not the law? The externalization of EU migration control through orchestration in the Central Mediterranean*, Journal of European Public Policy, pp. 1-20; Doi 10.1080/13501763.2020.1751243

O'SHEA, J., CROCKETT, K., KHAN, W., KINDYNIS, P., ANTONIADES, A., & BOULTADAKIS, G. (2018, July). Intelligent deception detection through machine based interviewing. In 2018 International Joint Conference on Neural Networks (IJCNN), pp. 1-8. IEEE.

OMEZI, N., [et al.], 2020, Jahankhani, H., Akhgar, B., Cochrane, P., Dastbaz, M. (Eds.) Policing in the era of ai and smart societies: austerity; legitimacy and blurring the line of consent. In: Policing in the era of ai and smart societies. Advanced sciences and technologies for security applications . Cham, Switzerland, Online pp. 231-265. Doi: 10.1007/978-3-030-50613-1

PALM, E. (2020), Externalized Migration Governance and the Limits of Sovereignty: The Case of Partnership Agreements between EU and Libya. *Theoria*, 86, pp. 9-27. DOI: <https://doi.org/10.1111/theo.12224>

PALMERINI, E., 2013, *The interplay between law and technology, or the RoboLaw project in context*, in: E. Palmerini and E. Stradella (eds), *Law and Technology. The Challenge of Regulating Technological Development*, Pisa: Pisa University Press, p. 7-19

PIJNENBURG, A., 2020, *Containment Instead of Refoulement: Shifting State Responsibility in the Age of Cooperative Migration Control?*, *Human Rights Law Review*, Volume 20, Issue 2, pp. 306-332. Disponível na hiperligação <https://doi.org/10.1093/hrlr/ngaa011>

PINA DELGADO, J., E TIUJO DELGADO, L., 2015, *Criminalidade Organizada* in *Enciclopédia de Direito e Segurança*, Edições Almedina, Coimbra pp. 472-476

PLOEG, [et al.], 2011, *Migration and the Machine-Readable Body* in *Migration and the New Technological Borders of Europe* in: Dijstelbloem, H., Meijer, A. (Eds.), *Migration and the New Technological Borders of Europe*, pp. 68-104

PORTER, S., E TEM BRINKE, L., 2008, *Reading between the lies: identifying concealed and falsified emotions in universal facial expressions*, Psychological science, 19(5), pp. 508-514. DOI: <https://doi.org/10.1111/j.1467-9280.2008.02116.x>

RESTOVIC, I., 2020, Why Not Fuzzy Logic? in: Skansi S. (eds), *Guide to Deep Learning Basics, Logical, Historical and Philosophical Perspectives* Springer, Cham, p. 29-40. DOI: <https://doi.org/10.1007/978-3-030-37591-1>

RUGGIU, D., 2018. *Human Rights and Emerging Technologies*, Analysis and Perspectives in Europe, New York: Jenny Stanford Publishing, pp. 10 e ss. DOI: <https://doi.org/10.1201/9780429490590>

RYAN, B., & MITSILEGAS, V. (Eds.), 2010, *Extraterritorial Immigration Control*, volume 21, *Immigration and Asylum Law and Policy in Europe*, Leiden, The Netherlands: Brill Nijhoff ; pp. 1-340

SANCHÉZ-MONEDERO, J., E DENCİK, L., 2020, The politics of deceptive borders: ‘biomarkers of deceit’ and the case of iBorderCtrl, *Information, Communication & Society* pp. 1-18. DOI: 10.1080/1369118X.2020.1792530

SHACHAR, A. (2019). *Bordering migration/migrating borders*. *Berkeley Journal of International Law*, 37(1), 93-147. doi:10.15779/Z38696ZZ3M, disponível em <http://hdl.handle.net/21.11116/0000-0006-CA94-F> [última consulta a 23 de novembro]

SHETH A.P. (1999) *Changing Focus on Interoperability in Information Systems: From System, Syntax, Structure to Semantics* In: Goodchild M., Egenhofer M., Fegeas R., Kottman C. (eds) *Interoperating Geographic Information Systems*. The Springer International Series in Engineering and Computer Science, vol 495. Springer, Boston, MA., pp. 1-25. DOI: [https://doi.org/10.1007/978-1-4615-5189-8\\_2](https://doi.org/10.1007/978-1-4615-5189-8_2) -

SKELAC, I., E JANDRIĆ, A., 2020, *Meaning as Use: From Wittgenstein to Google's Word2vec* In: Skansi S. (eds) *Guide to Deep Learning Basics*. Springer, Cham, p. 41-53. DOI: 10.1007/978-3-030-37591-1\_5

SPIJKERBOER, T., 2018, The Global Mobility Infrastructure: Reconceptualising the Externalisation of Migration Control in *European Journal of Migration and Law*, 20(4), 452-469. DOI: <https://doi.org/10.1163/15718166-12340038>

STATEWATCH, 2020, *Mediterranean: As the fiction of a Libyan search and rescue zone begins to crumble, EU states use the coronavirus pandemic to declare themselves unsafe*, pp. 1-13. disponível na hiperligação : <https://www.statewatch.org/media/documents/analyses/no-360-malta-italyeu-libya-pushbacks.pdf> [última consulta a 23 de novembro]

TOPRAKSEVEN C., M., 2018, *Migrant Rights at the border* in Elspeth Guild, Stephanie Grant, CA Groenendijk (eds) *Human Rights of Migrants in the 21<sup>st</sup> Century*, pp. 21-26 DOI: 10.4324/9781315145396

TRIANDAFYLLIDOU, A., E BARTOLINI, L., 2020, *Understanding Irregularity* in Spencer, S., & Triandafyllidou, A. (eds) *Migrants with Irregular Status in Europe Evolving Conceptual and Policy Challenges*, Springer International Publishing pp. 11-31. DOI: 10.1007/978-3-030-34324-8

VALENTE, I. M. F., & GUIA, M. J., 2016, *As políticas europeias para a imigração e asilo: o caso português*. Anos 90: Revista do Programa de Pós-Graduação em História da Universidade Federal do Rio Grande do Sul, 23(43), pp. 39-65.

WATSON, H, 2020, iBorderCtrl: Exploring the Issue of Algorithmic Bias in Global Governance in: CGC *New Technologies and Global Governance: Challenge or Opportunity?*, Junior Scholar Working Paper Series, Vol. 4, no. 1, The Centre for Global Constitutionalism, University of St Andrews, pp. 1-12. ISSN 2514-5819

ZAVRŠNIK, A., 2020, *Criminal justice, artificial intelligence systems, and human rights*, ERA Forum, pp. 567-583. DOI: 10.1007/s12027-020-00602-0

## Diplomas

Carta dos Direitos Fundamentais da União Europeia (JO C 202 de 7.6.2016, p. 389-405)  
Proclamada solenemente pelo Parlamento Europeu, Conselho e Comissão Europeia em Nice, a 7 de Dezembro de 2000.

CEPOL, aprovado pelo Regulamento (UE) 2015/2219 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, sobre a Agência da União Europeia para a Formação Policial (CEPOL) e que substitui e revoga a Decisão 2005/681/JAI do Conselho

Código das Fronteiras Schengen, aprovado por 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), com posteriores alterações.

Comunicação da Comissão ao Parlamento Europeu e ao Conselho sobre o Reforço da cooperação entre as autoridades responsáveis pela vigilância marítima tendo em vista um melhor conhecimento das situações: próximas medidas no quadro do Ambiente Comum de Partilha da Informação no domínio marítimo da UE (COM/2014/0451 final)

Convenção Europeia dos Direitos do Homem, assinada em Roma em 4 de Novembro de 1950 como a Convenção Europeia para a Protecção dos Direitos Humanos e Liberdades Fundamentais, emendado pelos protocolos n.º 11 e 14

Convenção Internacional sobre a Protecção dos Direitos de Todos os Trabalhadores Imigrantes e dos Membros das suas famílias. Adotada pela Assembleia Geral das Nações Unidas na sua resolução 45/158, de 18 de dezembro de 1990. Entrada em vigor na ordem internacional: 1 de julho de 2003, em conformidade com o artigo 87.º, n.º 1.

Convenção sobre os Direitos da Criança e Protocolos Facultativos, adotado e aberto para assinatura, ratificação e adotada pela resolução da Assembleia Geral 44/25 de 20 de novembro de 1989, entrando em vigor a 2 de setembro de 1990, em concordância com o artigo 49.º

Declaração Universal dos Direitos Humanos, adoptada e proclamada em 10 de Dezembro de 1948, publicada em Portugal no Diário da República, I Série A, n.º 57/78, de 9 de Março de 1978. Convenção de Genebra de 1951

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

Diretiva do Retorno, aprovada pela Diretiva 2008/115/CE do Parlamento Europeu e do Conselho, de 16 de Dezembro de 2008, relativa a normas e procedimentos comuns nos Estados-Membros para o regresso de nacionais de países terceiros em situação irregular

ECRIS-TCN, aprovado por Regulamento (UE) 2019/816 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, que cria um sistema centralizado para a determinação dos Estados-Membros que possuem informações sobre condenações de nacionais de países terceiros e de apátridas (ECRIS-TCN) tendo em vista completar o Sistema Europeu de Informação sobre Registos Criminais e que altera o Regulamento (UE) 2018/1726

EES, aprovado por Regulamento (UE) 2017/2226 do Parlamento Europeu e do Conselho, de 30 de novembro de 2017, que estabelece o Sistema de Entrada/Saída (SES) para registo dos dados das entradas e saídas e dos dados das recusas de entrada dos nacionais de países terceiros aquando da passagem das fronteiras externas dos Estados-Membros, que determina as condições de acesso ao SES para efeitos de aplicação da lei, e que altera a Convenção de Aplicação do Acordo de Schengen e os Regulamentos (CE) n.º 767/2008 e (UE) n.º 1077/2011

eIDAS, aprovado por Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE

ETIAS, aprovado pelo 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

eu-LISA, aprovado pelo Regulamento (UE) 2018/1726 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, relativo à Agência da União Europeia para a Gestão Operacional de Sistemas Informáticos de Grande Escala no Espaço de Liberdade, Segurança e Justiça (eu-LISA), que altera o Regulamento (CE) n.º 1987/2006 e a Decisão 2007/533/JAI do Conselho, e que revoga o Regulamento (UE) n.º 1077/2011, com posteriores alterações

Eurodac, aprovado Regulamento (UE) n.º 603/2013 do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativo à criação do sistema «Eurodac» de comparação de impressões digitais para efeitos da aplicação efetiva do Regulamento (UE) n.º 604/2013, que estabelece os critérios e mecanismos de determinação do Estado-Membro responsável pela análise de um pedido de proteção internacional apresentado num dos Estados-Membros por um nacional de um país terceiro ou um apátrida, e de pedidos de comparação com os dados Eurodac apresentados pelas autoridades responsáveis dos Estados-Membros e pela Europol para fins de aplicação da lei e que altera o Regulamento (UE) n.º 1077/2011 que cria uma Agência europeia para a gestão operacional de sistemas informáticos de grande escala no espaço de liberdade, segurança e justiça

Europol, aprovado pelo Regulamento (UE) 2016/794 do Parlamento Europeu e do Conselho, de 11 de maio de 2016, que cria a Agência da União Europeia para a Cooperação Policial (Europol) e que substitui e revoga as Decisões 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI e 2009/968/JAI do Conselho

Eurosur, aprovado pelo Regulamento (UE) n.º 1052/2013 do Parlamento Europeu e do Conselho, de 22 de outubro de 2013, que cria o Sistema Europeu de Vigilância das Fronteiras (Eurosur)

FAMI, aprovado pelo Regulamento (UE) n. ° 516/2014 do Parlamento Europeu e do Conselho, de 16 de abril de 2014 , que cria o Fundo para o Asilo, a Migração e a Integração, que altera a Decisão 2008/381/CE do Conselho e que revoga as Decisões n. ° 573/2007/CE e n. ° 575/2007/CE do Parlamento Europeu e do Conselho e a Decisão 2007/435/CE do Conselho, com posteriores alterações

FEDER, aprovado pelo Regulamento (UE) n.o 437/2010 do Parlamento Europeu e do Conselho, de 19 de maio de 2010, que altera o Regulamento (CE) n.o 1080/2006 relativo ao Fundo Europeu de Desenvolvimento Regional no que diz respeito à elegibilidade de intervenções habitacionais a favor de comunidades marginalizadas

FSI, aprovado pelo Regulamento (UE) n. ° 515/2014 do Parlamento Europeu e do Conselho, de 16 de abril de 2014 , que cria, no âmbito do Fundo para a Segurança Interna, um instrumento de apoio financeiro em matéria de fronteiras externas e de vistos e que revoga a Decisão n. ° 574/2007/CE

Fundo de apoio a emergência na União, aprovado pelo Regulamento (UE) 2016/369 do Conselho, de 15 de março de 2016, relativo à prestação de apoio de emergência na União

Guarda Europeia de Fronteiras e Costeira, aprovada pelo Regulamento (UE) 2019/1896 do Parlamento Europeu e do Conselho, de 13 de novembro de 2019, relativo à Guarda Europeia de Fronteiras e Costeira, que revoga os Regulamentos (UE) n.º 1052/2013 e (UE) 2016/1624

Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social.

Livre circulação dos cidadãos da União, aprovado pela Diretiva 2004/38/CE relativa ao direito de livre circulação e residência dos cidadãos da União e dos membros das suas famílias no território dos Estados-Membros

Manual prático para os guardas de fronteiras, aprovado por Recomendação da Comissão de 8.10.2019 que estabelece um «Manual prático para os guardas de fronteira» a utilizar pelas autoridades competentes dos Estados-Membros quando procedem ao controlo de pessoas nas fronteiras e que substitui a Recomendação C(2006) 5186 da Comissão, de 6 de novembro de 2006, C(2019) 7131 final

Mecanismo de Proteção Civil da União, aprovado pela Decisão n.º 1313/2013/UE do Parlamento Europeu e do Conselho, de 17 de dezembro de 2013, relativa a um Mecanismo de Proteção Civil da União Europeia Texto relevante para efeitos do EEE

Obrigação de comunicação de dados pelas transportadoras, aprovada pela Diretiva 2004/82/CE do Conselho, de 29 de Abril de 2004, relativa à obrigação de comunicação de dados dos passageiros pelas transportadoras

Obrigações às transportadoras, aprovada pela Diretiva 2001/51/CE do Conselho, de 28 de Junho de 2001, que completa as disposições do artigo 26.º da Convenção de Aplicação do Acordo de Schengen de 14 de Junho de 1985

Pacto Internacional sobre os Direitos Civis e Políticos, adotado e aberto à assinatura a 16 de dezembro de 1966. Entrada em vigor na ordem internacional: 23 de março de 1976, em conformidade com o artigo 49.º.

Parecer da Autoridade Europeia para a Proteção de Dados sobre a Proposta de um Regulamento que estabelece um Sistema de Entrada/Saída (EES) e de um Regulamento que estabelece um Programa de Viajantes Registados (RTP)

PNR, aprovado pela 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

Proposta de Regulamento do Parlamento Europeu e do Conselho relativo às ordens europeias de entrega ou de conservação de provas eletrónicas em matéria penal COM/2018/225 final - 2018/0108 (COD)

Protocolo Adicional contra o Tráfico Ilícito de Imigrantes por Via Terrestre, Marítima e Aérea à Convenção das Nações Unidas contra a Criminalidade Organizada Transnacional, de 2000

Regime Comunitário de Controlo, aprovado pelo Regulamento (CE) n.º 1224/2009 do Conselho, de 20 de Novembro de 2009, que institui um regime comunitário de controlo a fim de assegurar o cumprimento das regras da Política Comum das Pescas, altera os

Regulamentos (CE) n. o 847/96, (CE) n. o 2371/2002, (CE) n. o 811/2004, (CE) n. o 768/2005, (CE) n. o 2115/2005, (CE) n. o 2166/2005, (CE) n. o 388/2006, (CE) n. o 509/2007, (CE) n. o 676/2007, (CE) n. o 1098/2007, (CE) n. o 1300/2008, (CE) n. o 1342/2008, e revoga os Regulamentos (CEE) n. o 2847/93, (CE) n. o 1627/94 e (CE) e n. o 1966/2006, com posteriores alterações

Registos de identificação dos passageiros (PNR) — Unidades de informações de passageiros — Lista das unidades de informações de passageiros referidas no artigo 4.º da Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho 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 (2018/C 230/05)

SIS II – Controlo Fronteiriço, aprovado por Regulamento (UE) 2018/1861 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio dos controlos de fronteira, e que altera a Convenção de Aplicação do Acordo de Schengen e altera e revoga o Regulamento (CE) n.º 1987/2006

SIS II – Polícia, aprovado por Regulamento (UE) 2018/1862 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio da cooperação policial e da cooperação judiciária em matéria penal, e que altera e revoga a Decisão 2007/533/JAI do Conselho e revoga o Regulamento (CE) n.º 1986/2006 do Parlamento Europeu e do Conselho e a Decisão 2010/261/UE da Comissão

SIS II – Retorno, aprovado por Regulamento (UE) 2018/1860 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo à utilização do Sistema de Informação de Schengen para efeitos de regresso dos nacionais de países terceiros em situação irregular

Sistema comunitário de acompanhamento e de informação do tráfego de navios, aprovado pela Diretiva 2014/100/UE da Comissão, de 28 de outubro de 2014, que altera a Diretiva 2002/59/CE do Parlamento Europeu e do Conselho relativa à instituição de

um sistema comunitário de acompanhamento e de informação do tráfego de navios  
Texto relevante para efeitos do EEE

Tratado da União Europeia, de 13 de dezembro de 2007 — versão consolidada (JO C 202 de 7.6.2016, p. 13-46)

Tratado sobre o Funcionamento da União Europeia, de 13 de dezembro de 2007 — versão consolidada (JO C 202 de 7.6.2016, p. 47-360)

VIS, aprovado pelo Regulamento (CE) n.º 767/2008 do Parlamento Europeu e do Conselho, de 9 de Julho de 2008, relativo ao Sistema de Informação sobre Vistos (VIS) e ao intercâmbio de dados entre os Estados-Membros sobre os vistos de curta duração (Regulamento VIS)

## Jurisprudência

- Acórdão de 15 de dezembro de 2011, Al-Khawaja e Tahery c. Reino Unido, n.º 26766/05 e 22228/06 (TEDH)
- Acórdão de 23 de fevereiro de 2012, Hirsi Jamaa e outros c. Itália, n.º 27765/09 (TEDH)
- Acórdão de 7 de julho de 2011, Al-Skeini c. Reino Unido, n.º 55721/07 (TEDH)
- Acórdão de 29 de março de 2010, Medvedyev e outros c. France, n.º 3394/03 (TEDH)
- Acórdão de 13 de fevereiro, N.D. e N.T. c. Espanha, n.º 8675/15 e 8697/15 (TEDH)
- Acórdão de 16 de dezembro de 2008, Heinz Huber v. Bundesrepublik Deutschland, C-524/06, (TJUE)
- Acórdão de 2 de abril de 2020, Comissão c. Polónia, C 715/17 (TJUE)
- Acórdão de 2 de abril de 2020, Comissão c. Hungria C718/17 (TJUE)
- Acórdão de 2 de abril de 2020, Comissão c. República Checa, C719/17 (TJUE)

## Sítios web

- CISE  
[https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/cise-ia-study-part1-individual-analysis-final\\_en.pdf](https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/cise-ia-study-part1-individual-analysis-final_en.pdf)
- EMSA  
<http://www.emsa.europa.eu/operations/maritime-monitoring.html>.
- Guia da AEPD (2019) para avaliar a proporcionalidade das medidas que limitam direitos fundamentais da privacidade e da proteção de dados  
[https://edps.europa.eu/sites/edp/files/publication/19-12-19\\_edps\\_proportionality\\_guidelines2\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf)
- Horizonte 2020  
[https://ec.europa.eu/programmes/horizon2020/sites/horizon2020/files/H2020\\_PT\\_KI0213413PTN.pdf](https://ec.europa.eu/programmes/horizon2020/sites/horizon2020/files/H2020_PT_KI0213413PTN.pdf),
- Linguagem Corporal

- <http://index-of.co.uk/Social-Interactions/The%20Definitive%20Book%20of%20BODY%20LANGUAGE%20-%20Barbara%20Pease.pdf>
- Manual prático para os guardas de fronteira  
<https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/borders-and-visas/schengen/docs/c2019-7131-annex.pdf>.
  - Melhores práticas para os sistemas de controlo fronteiriço automatizado  
<https://euagenda.eu/upload/publications/untitled-6349-ea.pdf>
  - Pacote legislativo relativo às fronteiras inteligentes  
[https://www.europarl.europa.eu/legislative-train/theme-towards-a-new-policy-on-migration/file-registered-traveller-programme-\(2013-smart-borders-package\)](https://www.europarl.europa.eu/legislative-train/theme-towards-a-new-policy-on-migration/file-registered-traveller-programme-(2013-smart-borders-package))
  - Parecer da AEPD relativo à Decisão de Execução da Comissão no SIS  
[https://edps.europa.eu/sites/edp/files/publication/20-08-26\\_edps\\_comments\\_on\\_draft\\_commission\\_implementing\\_decisions\\_on\\_minimum\\_standards\\_and\\_technicalities\\_for\\_biometric\\_data\\_in\\_sis\\_in\\_field\\_of\\_border\\_checks\\_and\\_return\\_and\\_police\\_and\\_judicial\\_cooperation\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/20-08-26_edps_comments_on_draft_commission_implementing_decisions_on_minimum_standards_and_technicalities_for_biometric_data_in_sis_in_field_of_border_checks_and_return_and_police_and_judicial_cooperation_en.pdf)
  - Projeto do IBorderCtrl  
<https://cordis.europa.eu/project/id/700626>
  - Projetos de sistemas de controlo fronteiriço automatizado  
<http://www.projectprotect.eu/about/related-projects>
  - Relatório da IOM de 2019  
<https://migration.iom.int/reports/europe-%E2%80%94-mixed-migration-flows-europe-monthly-overview-december-2019>,
  - Silent Talker  
<https://www.silent-talker.com>
  - Vigilância marítima (Marsur)  
[https://www.eda.europa.eu/what-we-do/activities/activities-search/maritime-surveillance-\(marsur\)](https://www.eda.europa.eu/what-we-do/activities/activities-search/maritime-surveillance-(marsur))