BRILL
NIJHOFF

EUROPEAN JOURNAL OF MIGRATION
AND LAW 23 (2021) 457–484

European
Journal of
Migration
and Law

brill.com/emil

Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism

AQ 1

Niovi Vavoula
Lecturer in Migration and Security, Department~~?, Faculty?,~~ Queen Mary University of London, London, United Kingdom
n.vavoula@qmul.ac.uk

Abstract

Since the past three decades, an elaborate legal framework on the operation of EU-Schengen information systems has been developed, whereby in the near future a series of personal data concerning ~~effectively~~ all third-country nationals (TCNs) with an administrative or criminal law link with the EU/Schengen area will be monitored through at least one information system. This article provides a legal analysis on the embedment of Artificial Intelligence (AI) tools at the EU level in information systems for TCNs and critically examines the fundamental rights concerns that ensue from the use AI to manage and control migration. It discusses automated risk assessment and algorithmic profiling used to examine applications for travel authorisations and Schengen visas, the shift towards the processing of facial images of TCNs and the creation of future-proof information systems that anticipate the use of facial recognition technology. The contribution understands information systems as enabling the datafication of mobility and as security tools in an era whereby a foreigner is risky by default. It is argued that a violation of the right to respect for private life is merely the gateway for a series of other fundamental rights which are impacted, such as non-discrimination and right to effective remedies.

Keywords

fundamental rights – discrimination – migration management – borders – information systems – data protection

| DOI:10.1163/15718166-12340114

1 Introduction

The establishment of the Schengen area as a space without internal border controls has been accompanied by the gradual development of EU policies on, inter alia, the management of the external (Schengen) borders, a common visa policy and police cooperation. The rapid technological evolution has been an indispensable component of efforts to acquire – or regain – control over the movement of third-country nationals (TCNs). Technology has been the 'servant mistress of politics'[1] and has significantly upgraded the methods through which border controls are performed, leading to what Besters and Brom term as 'the digitalisation of the European migration policy'.[2] Modern technological advents, particularly the most controversial ones such as fingerprinting and travel surveillance, 'have been (and are still being) "tested" on migrants and refugees or otherwise legitimized at the border'.[3] This digitalisation constitutes part of a broader trend of techno-solutionism, which places a tremendous amount of trust in technological tools. ~~A p~~aradigmatic example in this context is the proliferation of information systems processing personal data of different categories of TCNs, initiatives to seize and analyse personal data from asylum seekers' phones,[4] as well as investments in e-gates, biometric ID cards, kiosks, unmanned drones for maritime surveillance.

In the era of techno-solutionism, the exponential increase in computational power coupled with the availability of large quantities of data has heightened the interest for Artificial Intelligence (AI). AI technology is increasingly used in public and private domains and enables computers to perform tasks that would otherwise require a large human workforce. AI could thus be described as a set of techniques used to train machines to approximate some aspects of human or animal cognition, such as algorithms to enable decision-making or systems recognising facial images and speech. In the field of migration, AI promises modernised migration, asylum and border controls through expedited and more efficient decision-making in relation to visa applications, residence permits, asylum applications or administrative detention by assessing the risk (security, public health or irregular immigration) a foreigner may

[1] Philippe Bonditti, 'From Territorial Spaces to Networks: A Foucauldian Approach to the Implementation of Biometry' (2004) 29 Alternatives: Global, Local, Political 465.

[2] Michiel Besters and Frans Brom, '"Greedy" Information Technology: The Digitalization of the European Migration Policy' (2010) 12(4) European Journal of Migration and Law 455.

[3] Ben Hayes, *NeoConOpticon: The EU Security-Industrial Complex* (Transnational Institute/ Statewatch 2009) 35.

[4] For example, in Germany there is ongoing litigation on this matter.

pose.[5] AI tools may also be used for more evidence-based policy-making, and even for predicting and preventing ~~a massive influx~~ of refugees and migrants.[6] In May 2020, the Commission published a report setting out the opportunities and challenges from embedding AI tools for immigration purposes and announced a portfolio with initiatives to be implemented within a 'roadmap' from 2021 to 2025.[7] In the meantime, the use of certain AI tools, in particular the devise of algorithms for profiling applications for Schengen visas and travel authorisations and the collection of facial images to pre-empt biometric identification at the borders is already embedded in the operation of information systems for TCNs. In April 2021, the Commission adopted a proposal for a Regulation laying down harmonised rules on AI, classifying initiatives related to immigration, asylum and border control management as 'high risk', thus acknowledging the potential for fundamental rights challenges.[8] The proposal added that 'AI systems used in migration, asylum and border control management affect people who are often in a particularly vulnerable position and who are dependent on the outcome of the action of the competent public authorities'.[9]

Whereas scholarly interest in AI is growing, legal scholarship on the challenges of AI regulation in the immigration, asylum and border control context is still in its infancy.[10] ~~Importantly, a~~ legal analysis on the embedment of AI tools at EU level in particular is currently missing.[11] This article aims to fill this literature gap, by exploring the extent to which AI tools are already embedded in the operationalisation of information systems and critically examining the fundamental rights concerns for TCNs. To that end, the article is organised as follows: Section 2 provides a concise synopsis of the legal landscape of EU information systems. Section 3 critically examines two examples ~~where~~ AI tools ~~are already embedded~~ in the legal framework of information

[5] Petra Molnar, 'Technology on the Margins: AI and Global Migration Management from a Human Rights Perspective' (2019) 8(2) Cambridge International Law Journal 305; Petra Molnar and Lex Gill, 'Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Asylum System' (University of Toronto, 2018).

[6] Ana Beduschi, 'International Migration Management in the Age of Artificial Intelligence' (2020).

[7] Commission, 'Opportunities and challenges for the use of artificial intelligence in border control, migration and security' (2020).

[8] Commission, COM(2021) 206final.

[9] Ibid Annex III.

[10] See Molnar (n 5); Beduschi (n 6).

[11] An analysis has been prepared by the European Parliament Research Service. See Costica Dumbrava, 'Artificial intelligence at EU borders – Overview of applications and key issues' (European Parliament Research Service, 2021).

systems. Automated risk assessments and algorithmic profiling are analysed in the context of examining applications for travel authorisations (ETIAS) and Schengen visas (VIS), viewed through the lens of the case law of the EU Court of Justice (CJEU) on automated processing of personal data. Section 4 highlights the shift towards processing facial images of ~~third-country nationals~~ by creating future-proofed information systems in anticipation of incorporation of facial recognition technology. Both AI applications are assessed in light of fundamental rights, focusing in particular on the rights to respect for private life (Article 7 of the EU Charter of Fundamental Rights), protection of personal data (Article 8 of the Charter) and the principle of non-discrimination (Article 21 of the Charter). The conclusion summarises the main findings of the analysis.

2 The Current Legal Landscape of EU (Schengen) Information Systems for ~~Third-Country Nationals~~

The AI-related developments in EU immigration law have predominantly taken place in the context of a network of highly sophisticated information systems for TCNs, some of which are currently operational (SIS, VIS, Eurodac), whereas others are under development (EES, ETIAS and ECRIS-TCN).[12]

Perhaps the most known EU information system is SIS. Operational since 1995, its overarching purpose is to ensure a high level of security in the Schengen area by facilitating both border control and police investigations. SIS registers alerts on various categories of persons and objects. In connection with each alert, it initially stored basic alphanumeric information – such as name, nationality, the type of alert and any specific objective physical characteristics.[13] In the first revision of the SIS legal framework in 2006, new functionalities were inserted into the system,[14] such as the interlinking of alerts involving different individuals or events registered under different legal bases[15] and the inclusion of biometric identifiers (photographs and fingerprints).[16] In 2018, the SIS legal

[12] For an overview see Niovi Vavoula, 'The "Puzzle" of EU Large-Scale Information Systems for Third-Country Nationals: Surveillance of Movement and Its Challenges for Privacy and Data Protection' (2020) 45(3) European Law Review 348.

[13] Convention Implementing the Schengen Agreement (CISA) of 14 June 1985 [2000] O L239/19, art 94.

[14] Regulation (EC) No 1987/2006 [2006] OJ L381/4; Council Decision 2007/533/JHA [2007] OJ L205/63.

[15] Regulation 1987/2006, art 37; Decision 2007/533/JHA, art 52.

[16] Regulation 1987/2006, art 22; Decision 2007/533/JHA, art 22.

framework underwent another revision[17] and according to the current rules, SIS stores alerts for law enforcement purposes such as on persons wanted for arrest and extradition,[18] missing persons,[19] or persons or objects subject to discreet, inquiry or specific checks.[20] In addition, SIS stores alerts on ~~third-country nationals~~ subject to return procedures,[21] or to be refused entry or stay in the Schengen area.[22]

VIS stores a wide range of personal data (both biographical and biometric) on individuals applying for short-stay (Schengen) visas. VIS was set up by a series of instruments: Decision 2004/512/EC,[23] Regulation 767/2008[24] governing the use of the system for border control purposes, and Council Decision 2008/633/JHA[25] prescribing the modalities by which visa data are consulted by law enforcement authorities and Europol. VIS aims to improve the implementation of the common visa policy, but seven sub-purposes are envisaged, including the fight against fraud and visa shopping and the contribution to the prevention of threats to Member States' internal security. In July 2021, the VIS legal framework was revised to extend the scope to long-term visa holders and holders of residence permits and residence cards, lower the age threshold for fingerprinting (six years) and promote automation in the decision-making process.[26]

Eurodac processes primarily the fingerprints of asylum seekers as well as irregular migrants apprehended in connection with the irregular crossing of an external border or found illegally staying in a Member State.[27] Eurodac's purpose is to assist in the implementation of the hierarchical rules on the allocation of the Member State responsible to examine an application for

[17] Regulation (EU) 2018/1860 [2018] OJ L312/1; Regulation (EU) 2018/1861 [2018] OJ L312/14; Regulation (EU) 2018/1862 [2018] OJ L312/56.

[18] Regulation 2018/1862, arts 26–31.

[19] Regulation 2018/1862, arts 32–33.

[20] Regulation 2018/1862, arts 36–37.

[21] Regulation 2018/1860, art 3.

[22] Regulation 2018/1861, art 24. For a detailed overview of SIS see Evelien Brouwer, *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System* (Martinus Nijhoff 2008). For a more recent analysis see Evelien Brouwer, 'Schengen's Undesirable Aliens' in Paul Minderhoud, Sandra Mantu and Karin Zwaan (eds), *Caught in between Borders – Citizens, Migrants, Humans: Liber Amicorum in honour of prof. dr. Elspeth Guild* (Wolf Legal Publishers 2019).

[23] Council Decision 2004/512/EC [2004] OJ L213/5.

[24] Regulation (EC) 767/2008 [2009] OJ L243/1 (VIS Regulation).

[25] Council Decision 2008/633/JHA [2008] OJ L218/129.

[26] Regulation (EU) 2021/1134 [2021] OJ L248/11 (2021 VIS Regulation).

[27] Regulation 603/2013 [2013] OJ L180/1.

international protection.[28] Eurodac may also be accessed by national law enforcement authorities and Europol for the purposes of preventing, detecting and investigating terrorist offences and serious crimes.[29] Two recast proposals have been tabled, one in May 2016[30] and another one in September 2020.[31] The latter is currently negotiated, with the aim of expanding the purpose, scope and categories of personal data stored.

The new generation of information systems involves EES, scheduled to start its operations in 2022, that will register the border crossings, both at entry and exit, of almost all TCNs admitted for a short stay, irrespective of whether they are required to obtain a Schengen visa or not.[32] EES is a multi-purpose tool: it aims to enhance the efficiency and automation of border checks, assist in the identification of irregular migrants and overstayers, combat identity fraud and misuse of travel documents and strengthen internal security and the fight against terrorism by allowing law enforcement authorities access to travel history records.[33] EES will record the identities of TCNs, by storing alphanumeric data, four fingerprints and a facial image, along with details of their travel documents, which will be linked to electronic entry and exit records.[34]

The movement of visa-free travellers will also be monitored through ETIAS, also scheduled to launch ~~in 2023~~.[35] ETIAS will require them to apply online for travel authorisation prior to travelling to the Schengen area and disclosing a series of personal data including biographical data, travel arrangements, home and email address, phone number, level of education and current occupation.[36] Based on that information, ETIAS will operate as a pre-emptive control mechanism: travellers will get pre-vetted on the basis of background checks against information systems and databases, screening rules and a dedicated watchlist ~~so as~~ to determine whether their presence in the territory of the Member States would pose a security, irregular migration or high epidemic risk.[37]

The last addition to the EU information system family is ECRIS-TCN for the exchange of criminal records on convicted TCNs and stateless persons.[38]

[28] Regulation (EU) 604/2013 [2013] OJ L180/31.

[29] Regulation 603/2013, arts 19–22.

[30] Commission, COM(2016) 272final (2016 Eurodac proposal).

[31] Commission, COM(2020) 614final.

[32] EES Regulation, art 2(3).

[33] EES Regulation, art 6(1).

[34] Arts 14–20.

[35] Regulation (EU) 2018/1240 [2018] OJ L236/1 (ETIAS Regulation).

[36] Ibid art 17.

[37] Ibid, art 20.

[38] Regulation (EU) 2019/816 [2019] OJ L135/1.

ECRIS-TCN is meant to complement the already existing, decentralised ECRIS system through which information on the criminal records of EU nationals is exchanged among Member States.

SIS, VIS and Eurodac were originally envisaged to operate independently. Progressively, the need has emerged to provide technical and legal solutions that would enable EU information systems to complement each other. Interoperability Regulations 2019/817 and 2019/818 adopted on 20 May 2019 prescribe four main components to be implemented. First, a European Search Portal (ESP)~~,~~ will enable competent authorities to simultaneously query the underlying systems and the combined results will be displayed on a single screen. Second, a shared Biometric Matching Service (BMS) will generate and store templates from all biometric data recorded in SIS ~~II~~, VIS, Eurodac, EES and ECRIS-TCN. Third, a Common Identity Repository (CIR) will store an individual file for each person containing both biometric and biographical data, as well as a reference indicating the system from which the data were retrieved so as facilitate identity checks of TCNs, assist in the detection of individuals with multiple identities and streamline law enforcement access. Finally, a Multiple Identity Detector (MID)~~.~~[39] will ~~aim to~~ detect multiple identities, by creating links between identical data to indicate whether the individual is lawfully registered in more than one system or whether identity fraud is suspected.

3 Automated Risk Assessments and Algorithmic Profiling

The imminent completion of the 'puzzle' of information systems and the embedment of interoperability has increased the appetite for using the personal data stored in information systems beyond their specific context and purposes to assist more broadly in the operation of other databases. At the heart of these practices is the possibility of information systems to automatically be consulted ~~so as~~ to support human decision-making by sifting through the data provided in the applications and 'flagging' potentially risky individuals. Automated risk assessments also embrace algorithmic profiling, whereby TCNs' data are cross-checked against risk indicators to enable their classification as high risk or high priority individuals whose applications thus merit further review.[40]

At EU level, automated risk assessments and algorithmic profiling of TCNs will be carried out in the framework of ETIAS and the revised VIS – and they

[39] Regulation (EU) 2019/817 [2019] OJ L135/27; Regulation (EU) 2019/818 [2019] OJ L135/85.

[40] Molnar and Gill (n 5). For further explanation of these terms see below.

are also foreseen in the PNR Directive regarding information exchange of passengers more generally (albeit in the latter case the assessments ~~will~~ take place at national level). This section will unpack the relevant rules and explore key fundamental rights concerns raised by these novel methods of data processing.

3.1 *Databases as Automated Decision-Making Systems: The Cases of ETIAS and VIS*

A decisive step towards automated risk assessments of visa-free travellers has taken place in the development of ETIAS, which will require their pre-vetting as to whether they pose a security, irregular migration or high epidemic risk. In particular, the pre-screening will require automated risk assessment of each application based on three elements. First, ETIAS applications will be subject to background checks against data already present in immigration and law enforcement information systems – namely SIS, VIS, Eurodac, EES, ECRIS-TCN and ETIAS itself, as well as Europol data and certain Interpol databases, namely the Stolen and Lost Travel Document database (SLTD) and the Interpol Documents Associated with Notices databases (TDAWN).[41] Second, certain personal data will be compared against specific screening rules, enabling profiling on the basis of risk indicators.[42] Thus, ETIAS is a platform for mining and profiling ETIAS applicants. Profiling is defined pursuant to Article 4(4) of Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR) as

> any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.[43]

The ETIAS screening rules, which will be developed by the European Border and Coast Guard (Frontex), are meant to identify persons who are otherwise unknown to national competent authorities but are assumed to be of interest for immigration control or security purposes and therefore are likely to commit criminal offences in the future. These persons will be flagged not because of any specific actions they have engaged in but because they display particular

[41] In addition to Article 20, as mentioned earlier, see Regulation (EU) 2021/1152 [2021] OJ L249/15.

[42] ETIAS Regulation, arts 20(5) and 33.

[43] Regulation (EU) 2016/679 [2016] OJ L119/1.

category traits in a probabilistic logic devoid of concrete evidence.[44] Third, ETIAS applications will be cross-checked against a special watchlist of individuals suspected of having participated in terrorism or other serious crimes or in respect of whom there are factual indications or reasonable grounds to believe that they will commit such offences.[45]

Visa-free travellers will thus be subjected to an automated risk assessment to identify whether the applicant's data ~~is~~ listed in any of these information systems, watchlist or correspond to the screening rules for a reason that merits further attention and may justify the refusal of the travel authorisation (e.g. whether the applicant has been refused a short-stay visa, or is reported to SIS as subject to refusal of entry or stay). The automated comparison with data present in information systems will be facilitated by ~~one of the interoperability components,~~ ESP.[46] If automated processing reveals a hit, then Articles 21 and 22 of the ETIAS Regulation provide that the ETIAS Central Unit, to be established within Frontex, shall be consulted to verify the hit. If the hit is verified then the application will be processed manually by an ETIAS National Unit.[47] Otherwise, if no hit is reported, the travel authorisation will be automatically granted.[48]

The same approach has been followed in the revised VIS Regulation, under rules comparable to the ETIAS ones. However, there are some noticeable differences: ~~first~~, even if automated processing does not reveal any hits with other information systems or databases, the visa application will be processed manually by the national authorities and there is no automated positive decision-making. ~~Second, automated querying concerns all information systems and databases mentioned above but VIS itself, which is of course consulted under separate rules.~~ The purpose of automated querying is thus to assist human decision-making by flagging potentially risky individuals, the application of whom merits specific attention by the national authorities and thus conduct automated social sorting of potentially risky visa applicants. ~~Third~~, the verification of a hit (or hits) will take place by national authorities, with the VIS Regulation prescribing specific follow-up actions depending on the database or information system with which the data from the visa application matched.[49]

[44] Susie Alegre, Julien Jeandesboz and Niovi Vavoula, 'European Travel Information and Authorisation System (ETIAS): Border Management, Fundamental Rights and Data Protection' (Study for the LIBE Committee of the European Parliament, 2017) 23–26.

[45] ETIAS Regulation, art 34.

[46] Ibid art 11. See Regulation (EU) 2021/1151 [2021] OJ L249/7.

[47] ETIAS Regulation, arts 25–32.

[48] Ibid art 21.

[49] Ibid arts 9c–9g.

~~Fourth~~, whereas the watchlist consulted will be the same in both ETIAS and VIS, the risk indicators which will inform the screening rules will be devised separately ~~(see below)~~.

That said, the approach is one and the same: in an era where travel flows have been on the rise and post-COVID are expected to increase, the deployment of *automated* risk assessment and profiling of applications promises to further enact pre-emption in terms of reallocating screening resources to 'risky' individuals prior to their departure, while facilitating travel for low-risk profiles.[50]

For the sake of a holistic approach, similar rules are laid down in Directive 2016/681 on passenger name records (PNR Directive), which operates in the law enforcement context; nonetheless automated risk assessments of passengers are equally performed at EU borders.[51] The Directive obliges the Member States to collect and exchange passenger data to prevent, detect, investigate and prosecute terrorist offences and serious crimes. In order to identify unknown persons who may be risky, PNR data are compared through automated means against combinations of predetermined fact-based risk indicators developed by national passenger units assisted by the Europol Travel Intelligence Task Force, thus there are no harmonised risk indicators.

3.2 *Automated Processing of Personal Data under EU Law*

From the outset, automated processing of personal data must be distinguished from automated decision-making. The former informs and is pre-requisite of the latter. The Article 29 Working Party (now European Data Protection Board) has defined automated decision-making as 'the ability to make decisions by technological means without human involvement'.[52] Article 22 of the GDPR stipulates that:

> the data subject has the right not to be subject to a decision based solely on automated processing including profiling when it produces legal effects concerning him or her or at least it similarly significantly affects him or her.

[50] Matthias Leese, 'The New Profiling: Algorithms, Black Boxes, and the Failure of Anti-discriminatory Safeguards in the European Union' (2014) 45(5) Security Dialogue 494.

[51] Directive (EU) 2016/681 [2016] OJ L11/132. See also the contribution by Julien Jeandesboz in this special issue.

[52] Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (WP251, 2018) 8.

Guidance on the concept of automated processing is provided by two cases ~~by~~ the ~~European Court of Justice (~~CJEU~~)~~, albeit in the context of law enforcement. In Opinion 1/15 on the draft agreement between the EU and Canada on the transfer of PNR data to Canadian authorities, the CJEU considered the legality of automated processing of passengers' data in the context of Canada's border control pre-screening program, which involve~~s~~ automated cross-checking against various Canadian databases and analysis of information on the basis of pre-determined criteria about everyone who buys a flight ticket to Canada.[53] The premise of that automated processing is to identify supposedly high-risk travellers who would be subjected to secondary screening to be admitted to the country. The CJEU found that the proportionality of the automated processing of PNR data 'depends on the pre-established models and criteria and on the databases on which that type of data processing is based'.[54] In that respect, the Court developed a series of guidelines: (a) the pre-established models and criteria (algorithms), should be 'specific and reliable' to individuals who might be under a 'reasonable suspicion' of participation in terrorist offences or serious transnational crime and should be non-discriminatory; b) the databases cross-checked must be reliable and up to date; c) any hit following the automated processing of that data must be subject to an individual re-examination by non-automated means; d) the pre-established models and criteria and the databases used ~~are~~ not discriminatory and ~~are~~ limited to that which is strictly necessary; and (e) the reliability and topicality of those pre-established models and criteria as well as the use of databases should be subject to review, taking account of statistical data and results of international research.[55]

These considerations have been echoed in *La Quadrature du Net and Others* concerning algorithms to analyse traffic and location data of users of electronic communications services to detect suspicious patterns and behaviours in pursuance of safeguarding national security.[56] The CJEU has clarified that ~~such~~ automated analysis is in itself a limitation to the rights of privacy, personal data protection and confidentiality of communications and thus must be subject to a strict proportionality test. In addition to its pronouncements in Opinion 1/15, the CJEU added that the models or criteria to conduct an automated analysis cannot be based on sensitive data *in isolation*.[57] Furthermore, the Court acknowledged the need to regularly re-examine the algorithms

[53] Opinion 1/15, EU:C:2017:592.

[54] Ibid para 172.

[55] Ibid paras 172–173.

[56] Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others v Premier Ministre and Others*, EU:C:2020:791.

[57] Ibid para 181. Emphasis added.

and the databases used to ensure that they are reliable, up-to-date and in practice non-discriminatory and limited to what is strictly necessary to achieve the intended purpose.[58] Lastly, the CJEU held that because of the margin of error that may result from the automated analysis, there has to be an individual non-automated re-examination of a positive result before adopting a measure that may have adverse effect on the person concerned.[59]

The aforementioned findings are crucial when assessing the ETIAS and VIS rules on automated processing of applicants' data and the next section will highlight how these guidelines are applied in this context.

3.3 *The Reliability and Relevance of Personal Data Used for Automated Risk Assessments*

A first issue is the extent to which automated comparisons will be taking place against 'reliable and up to date' systems. At the heart of this assessment is the quality of personal data stored. Data quality is a key principle of EU data protection law. Article 5(1)(d) of the GDPR prescribes that personal data should be 'accurate and, where necessary, kept up to date' and that 'every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay'.

Data quality has been a longstanding problem of the currently operational EU information systems. Spelling errors, lack of documentation, insufficient language skills, technical deficiencies, incorrect transcription of names into the Latin alphabet, recording of birth dates when the precise date is unknown and lack of training are only some of the reasons why EU information systems may record data that suffer in terms of quality.[60] ~~These findings are corroborated by immigration control officers who confirm that they have identified significant mistakes in the entries included in the data systems over the course of their work.~~ In November 2019, the European Court of Auditors highlighted the importance of the quality of personal data stored and stressed that eu-LISA performs automated monthly data quality checks on certain SIS alerts.[61] These checks generate a report listing the individual alerts with potential quality

[58] Ibid para 182.

[59] Ibid para 182.

[60] FRA, 'Fundamental Rights and the Interoperability of EU Information Systems: Borders and Security' (2017) 30; FRA, 'Under watchful eyes: biometrics, EU IT systems and fundamental rights' (2018) 81–94. The Commission refers to data quality issues in VIS. See Commission, COM(2016) 655final, 9–10, 12.

[61] European Court of Auditors, 'EU information systems supporting border control – a strong tool, but more focus needed on timely and complete data' (2019) 29–30.

issues and transmit it directly to the country concerned. The monthly reports show approximately three million warnings of potential data quality issues, which are not addressed sufficiently at the national level. Thus, their number is not significantly lower. The existence of incomplete records in SIS was also pointed out.[62] If the stored information is not of sufficient quality, any automated processing may lead to incorrect processing, irregularities and false hits, with significant repercussions for TCNs, whose applications may be denied, or delayed, or they may be required to provide additional information.

Furthermore, concerns are also raised in relation to certain alerts stored in SIS stemming from the discretion national authorities largely enjoy in recording alerts, which must be based on an individual assessment in accordance with the principle of proportionality.[63] An issue that has arisen in this respect involves the recording of alerts on individuals who should be subject to discreet checks or specific checks (or inquiry checks that will be registered in the future) in accordance with Articles 36–37 of Regulation 2018/1862. It has been reported that alerts on discreet checks are subject to variable practices by Member States. For example, in France alerts on discreet checks were registered 'en masse' as a response to terrorist events.[64] The varied application of the proportionality assessment by national authorities and the registration of SIS alerts may have indirect repercussions in the automated processing of ETIAS and VIS application files, as the same conduct may not warrant a SIS alert in all Member States.

Similar reliability issues have also been raised in relation to the operation of the Interpol database TDAWN. The latter contains travel documents related to notices circulated by states, which are international requests for cooperation or alerts allowing police in member countries to share critical crime-related information concerning individuals wanted for serious crimes, missing persons, unidentified bodies, possible threats, prison escapes and criminal *modi operandi*.[65] Recent reports have unearthed the abuse of these notices by some states in the pursuit of political objectives, repressing the freedom of expression or persecuting members of the political opposition beyond their

[62] Ibid 31.

[63] Regulation 2018/1861, art 21.

[64] 'Inaccurate data in Schengen system "threatens rights"' (*euobserver*, 8 January 2018) <https://euobserver.com/tickers/140468> accessed 10 August 2021. Even if these practices have stopped, the alerts are retained for at least three years and may be renewed. See Regulation 2018/1862, art 53(3).

[65] Mario Savino, 'Global Administrative Law Meets Soft Powers: The Uncomfortable Case of Interpol Red Notices' (2011) 43 New York University Journal of International Law and Politics 263.

borders.[66] These issues, which are of grave concern are bound to preoccupy, as at the time of writing, the negotiations for a cooperation agreement between the EU and Interpol will start shortly.[67]

Finally, the establishment of ECRIS-TCN questions not only the reliability, but also the relevance of information systems. At the heart of the problem is the extent to which comparison against ECRIS-TCN will be necessary in view of SIS, the purpose of which is precisely to prevent the entry among others of convicted third-country nationals.[68] Article 24 of Regulation 2018/1861 allows Member States to record alerts concerning TCNs who are unwelcome to enter or stay on national territory because they have been convicted in a Member State of an offence carrying a penalty involving the deprivation of liberty of at least one year. Although, Member States must determine whether the case is 'adequate, relevant and important enough to warrant an alert in SIS', terrorist offences are excluded from a proportionality assessment (Article 21(2) Regulation 2018/1861). In practice, in relation to terrorist offences, the overlap between ECRIS-TCN and SIS would be complete. As for serious offences, the extent of that overlap is opaque. However, since the purpose of these alerts is precisely to prevent the entry of unwelcome TCNs, cases that deserve an alert in SIS for refusal of entry and stay are and will be recorded. This is all the more because the scope of Article 24 of Regulation 2018/1861 is wider than the scope of comparison against ECRIS-TCN which concerns serious offences only. Regrettably, the final text does not provide rules on the treatment of applications in cases where automated processing reveals a hit in SIS without a corresponding a record in ECRIS-TCN (for instance if the Member State has forgotten to delete an alert) or where there is a hit in ECRIS-TCN without a corresponding alert for refusal of entry or stay in SIS by the convicting Member State.[69]

3.4 *Algorithmic Profiling and the Risk of Discrimination*

In the configuration of the screening rules based on risk indicators further fundamental rights challenges are evident. Article 33 of the ETIAS Regulation

[66] See Rasmus Wandall et al, 'Misuse of Interpol's Red Notices and impact on human rights – recent developments' (Study for the DROI Committee of the European Parliament, 2019).

[67] The green light has been given for the Council to adopt a Decision authorising the opening of negotiations for a cooperation agreement with Interpol. See Council, Document 10407/21 (6 July 2021).

[68] For further analysis see Niovi Vavoula, 'The Commission Package for ETIAS Consequential Amendments – Substitute Impact Assessment' (2020) 20–30.

[69] Instead, statistical data will be collected on the overlap between SIS and ECRIS-TCN to establish whether it is necessary to address the aforementioned issues.

prescribes that specific ETIAS screening rules will be built in an algorithm, enabling profiling, so as to sift unknown TCNs that fit pre-defined risk profiles and may constitute immigration, security or public health risks. It is the Commission that ~~shall further~~ define, ~~via a delegated act, what must be regarded as such~~ risks, taking into account various factors, in particular: a) EES statistics indicating abnormal rates of overstaying and refusals of entry, b) ETIAS statistics on abnormal rates of refusal of travel authorisations, c) ETIAS statistics on correlations between data and overstaying by travellers or refusals of entry, d) 'information substantiated by factual and evidence-based elements' provided by Member States on specific security risk indicators or threats; e) information substantiated by factual and evidence-based elements provided by Member States concerning abnormal rates of overstaying and refusals of entry and f) information concerning specific high epidemic risks provided by Member States as well as epidemiological surveillance information and risk assessments by the ECDC and disease outbreaks reported by the World Health Organization.[70] Similar rules are envisaged in the revised VIS Regulation, with few tweaks, for example, instead of using ETIAS statistics, the screening rules will take into consideration VIS statistics.[71]

In assessing the risk for discriminatory profiling, there are three considerations that must be taken into account regarding the reliability of the statistical data and information on the basis of which the risks will be determined. First, with respect to EES, the reliability of its statistics on overstayers may be called into question, as the system will automatically detect individuals who may have not been entered.[72] Arguably, statistical data will be based on large amounts of records and therefore even though it will have a margin of error, the risks drawn could still remain correct. Second, it is premature to employ information systems that have not even started their operations yet and will thus be evaluated in terms of data quality and possible malfunctions in the future~~ for supporting the operation of other systems~~. This disregards the mounting and unresolved data quality issues that operational systems experience. The experience of the existing operational information systems shows that such issues regularly arise and, more importantly, have spill over effects. Third, there are doubts as regards the reliability of the information provided

[70] ETIAS Regulation, art 33(2).

[71] 2021 VIS Regulation, art 9j(2).

[72] For criticism on the reliability of EES entry/exit records see Standing Committee of Experts on International Immigration, Refugee and Criminal Law (Meijers Committee), 'Note on the Smart Borders proposals (COM(2013) 95 final, COM(2013) 96 final and COM (2013) 97 final' (CM1307, 2013); Ben Hayes and Mathias Vermeulen, 'Borderline – The EU's New Border Surveillance Initiatives' (Heinrich Böll Stiftung 2012).

by the Member States. Both Regulations require that the information provided be based on facts and evidence-based elements, but the extent to which this can be checked and validated remains to be seen. As with the registration of SIS and Interpol alerts, Member States may have very different understandings of security risks and may abuse this possibility to promote highly securitised agendas. After defining the risks based on the information mentioned above, the Commission will also adopt an implementing act detailing those risks on which the specific risk indicators will be based. The ETIAS risk indicators shall consist of a combination of data including one or several of these categories of data: a) age range, sex, nationality; b) country and city of residence; c) level of education; d) current occupation.[73] In the case of VIS, the measures for screening under a), b) and d) will be used for developing the VIS risk indicators along with data on the Member States of destinations, the Member State of first entry and the purpose of travel.[74]

As with all algorithmic tools, given they are trained on pre-existing data and past decision-making, they run the danger to replicate all of the implicit and inherent biases of those earlier decisions.[75] In recognition that the aforementioned list of risk indicators contains a series of grounds of prohibited discrimination under the UN Convention for the elimination of all forms of racial discrimination 1965[76] and the Charter, both Regulations note that the indicators shall be 'targeted and proportionate'. Going beyond the requirements of Opinion 1/15 and *La Quadrature du Net and Others*,[77] risk indicators are to be used 'based solely on a person's sex or age',[78] which leaves it open as to whether permissible risk factors could be based on a combination of gender and age (e.g. 'women below the age of x').[79] Furthermore, in line with these

[73] ETIAS Regulation, art 33(4).

[74] 2021 VIS Regulation, art 9j(4).

[75] For example, the UK Home Secretary decided to withdraw an algorithm used to filter visa applications similar to that prescribed by the revised VIS Regulation after being called out as racially discriminatory. Home Office to scrap 'racist algorithm' for UK visa applicants' (*The Guardian*, 4 August 2020) <https://www.theguardian.com/uk-news/2020/aug/04/home-office-to-scrap-racist-algorithm-for-uk-visa-applicants> accessed 10 August 2021.

[76] International Convention on the Elimination of All Forms of Racial Discrimination of 21 December 1965.

[77] Opinion 1/15 (n 53) para 165; *La Quadrature du Net and Others* (n 56) para 181.

[78] ETIAS Regulation, art 33(5); revised VIS Regulation, art 9j(5). González Fuster correctly notes that gender is not covered as sensitive data by Article 9(1) of the GDPR, therefore this addition is particularly welcome. See Gloria Gonzalez Fuster, 'Artificial Intelligence and Law Enforcement – Impact on Fundamental Rights' (Study for the LIBE Committee of the European Parliament, 2020) 42.

[79] González Fuster (n 78) 34.

judgments, the ETIAS and VIS Regulations state that the risk indicators should in no circumstances be based on information revealing a person's colour, race, ethnic or social origin, genetic features, language, political or any other opinion, religion or philosophical belief, trade union membership, membership of a national minority, property, birth, disability, or sexual orientation.[80] However, designating sex may often indicate sexual orientation, city of residence ~~will often~~ reveal ethnicity and colour, level of education – in the case of ETIAS only – and current occupation will often be an indicator of property and trade union membership.[81] Nationality may be a proxy for race, ethnic origin, or religion; differences of treatment on grounds of nationality can turn into discrimination on prohibited grounds. Furthermore, algorithms based on level of education or job group have the potential for undue and unlawful discriminatory profiling.[82] For example, the combination of data on occupation, level of education along with previous criminal convictions could 'weave' people from a specific trade union group, due to the specific policy of a single state on demonstrations or on access to occupation and education. Overall, it has been found that algorithms may still lead to indirect discrimination where it may not be done by reference to a protected characteristic, but nonetheless has a discriminatory effect on group of people sharing the same protected characteristics if nevertheless puts them at a particular disadvantage.[83] The establishment of the ETIAS and VIS Fundamental Rights Guidance Boards[84] to enable checks and balances in the configuration of algorithms is welcome, but more specific commitments about the evaluation and possible revision of the algorithms could have been spelled out.

These rules should be read in conjunction with the Commission proposal for an AI Regulation, which, as mentioned earlier, considers AI for

[80] ETIAS Regulation, art 33(5); 2021 VIS Regulation, art 9j(5).

[81] Elspeth Guild and Niovi Vavoula, 'Travel authorization in the EU: automated processing and profiling' (*openDemocracy*, 12 October 2020) <https://www.opendemocracy.net/en/can-europe-make-it/travel-authorization-eu-automated-processing-and-profiling/> accessed 10 August 2021.

[82] Fondazione Giacomo Brodolini, 'Fundamental rights review of EU data collection instruments and programmes' (2019) 39.

[83] Andrea Romei and Salvatore Ruggieri, 'Discrimination Data Analysis: A Multi-disciplinary Bibliography' in Bart Custers et al. (eds), *Discrimination and Privacy in the Information Society – Data Mining and Profiling in Large Databases* (Springer 2013) 109. *La Quadrature du Net and Others* blurs this issue of indirect discrimination. For a critical analysis see Elspeth Guild, Eliz Mendos Kuşkonmaz, Valsamis Mitsilegas and Niovi Vavoula, 'Data Retention and the Future of Large-Scale Surveillance: The Evolution and Contestation of Judicial Benchmarks' (European Law Journal, forthcoming 2021).

[84] ETIAS Regulation, art 10; 2021 VIS Regulation art 9l.

immigration-related purposes as high risk. Regrettably, Article 83 of the AI Regulation proposal explicitly excludes the legal instruments concerning information systems from its scope 'unless the replacement or amendment of those legal acts leads to a significant change in the design or intended purpose of the AI system or AI systems concerned'. Thus, a forthcoming AI Regulation will not be the *lex generalis*. However, its requirements shall be taken into account, *where applicable*, in the evaluation of each database. This rule is disappointing, not only because the application of the safeguards of the Proposal is dependent on future developments, but also because the actual impact of the safeguards on the operation of information systems based on AI tools cannot be determined.

Th~~e~~ analysis~~ in this and the previous section~~ aimed to highlight key privacy, data protection and discrimination concerns posed by automated risk assessments, which may lead to automatic decision-making, based on automated queries of information systems and databases and algorithmic profiling as novel AI tools. These challenges stem from the lack of reliability of data feeding automated comparisons or training/feeding the algorithms. The lack of impact assessments when introducing automated queries and algorithmic profiling is also noteworthy. ETIAS was only subjected to a feasibility study,[85] whereas the legal assessment on the VIS revision focused predominantly on the expansion of its scope to holders of long-stay visas, residence permits and residence cards.[86] A counter argument to the analysis is that following flagging, each request for travel authorisation or Schengen visa will be assessed individually. In view of the trust placed on modern technologies and conversely the inherent distrust towards TCNs, it is highly probable that individuals singled out through automated processing of their applications will be at a disadvantage. These challenges, stemming from so-called automation bias, are magnified when considering that the targeted individuals, third-country nationals, may also be vulnerable~~,~~ and in any case are *by default* in a rather weak position to exercise their rights to an effective remedy.[87] These tools will operate extraterritorially and the logic/process under which the decisions will be taken is altered, thus potentially hindering individuals to seek clarifications on automated processing of their personal data and effective review.

[85] PWC, 'Feasibility Study for a European Travel Information and Authorisation System (ETIAS)' (2016).

[86] Commission, 'Legal analysis on the necessity and proportionality of extending the scope of the Visa Information System (VIS) to include data on long stay visas and residence documents' (2018).

[87] See the contribution by Eveli~~ne~~ Brouwer in this special issue.

4 Biometric Identification through Facial Images: The Move towards Facial Recognition Technology

Another AI-based tool intertwined with the operation of EU information systems is facial recognition, enabled by the collection and further processing of facial images ~~of different categories of TCNs~~. Facial recognition technology allows the automatic authentication/verification (one-to-one comparison), for example at Automated Border Control gates, identification (one-to-many comparison) or categorisation, for instance face analysis – the deduction of whether an individual belongs to a specific group based on their characteristics.[88] Facial recognition technology is based on deep learning, whereby a face is typically detected, the image is normalised (localising face landmarks), and then facial features are extracted for comparison against one or many reference faces. At EU level, facial recognition technology gained attention since 2014 due to the availability of increased computational power, massive amounts of data and the use of modern machine learning algorithms.[89] This section aims to highlight how information systems are future-proofed to accommodate facial recognition technology as part of immigration management.

4.1 *The Anticipation of Facial Recognition Technology in the Operationalisation of Information Systems*

With the exception of ETIAS, information systems process different types of biometric identifiers, with emphasis ~~over the past years~~ on verification and identification first through fingerprints and growingly via facial images. The preference for digitally tagging individuals using their biological characteristics is attributed to a number of qualities that they carry, such as their universality, distinctiveness and permanence.[90] Biometrics create an 'anchor' for identity in the human body, to which information can be fixed,[91] resulting in its 'informatisation'.[92] Under EU data protection law, biometric data constitute a special category of personal data[93] and are defined as 'personal data resulting

[88] FRA, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (2019) 7–8.

[89] See Patrick Grother et al, 'Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification' NISTIR 8238.

[90] Anil Jain, Ruud Bolle and Sharath Pankanti, *Personal Identification in Networked Society* (Kluwer 1999). For an analysis on implementing biometrics at the borders see Commission, 'Biometrics at the frontiers: Assessing the impact on society' (2005).

[91] Surveillance Studies Network, 'A Report on the Surveillance Society' (2006) 23.

[92] Irma van der Ploeg, 'Biometric Identification Technologies: Ethical Implications of the Informatization of the Body' (No 1, Biometric Technology & Ethics 2005).

[93] GDPR, art 9. See Directive (EU) 2016/680 [2016] OJ L119/89, art 10.

from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person'.[94] Furthermore, facial images fall within the remit of Article 8 ECHR.[95] Facial images constitute biometric data: they are largely unique, they cannot be changed by individuals (e.g. destroying) and in comparison to fingerprints they can easily be captured; individuals are unable to prevent the capture of their facial images.[96]

In the early days of information systems, Eurodac only processed fingerprint data (and at the time of writing this is still the case), whereas VIS and SIS required the collection of both fingerprints and 'photographs', but not 'facial images'.[97] The difference is significant. Recital 51 of the GDPR notes that there is a distinction between photographs and facial images, with the definition of biometric data applying to photographs only when these are processed through specific technical means allowing the unique identification or authentication of a natural person.

At the time of writing, facial recognition technology is not applied by any operational EU information system, but in the near future all systems except for ETIAS will process facial images for the purpose of verification and/or identification. This will be facilitated by the BMS and CIR ~~interoperability components~~. The first step towards the insertion of facial images in information systems took place in the setting up of EES. The Commission's 2013 EES proposal originally foresaw the collection and storage of a full set of fingerprints only.[98] However, as the capture of 10 fingerprints stumbled across practical and proportionality issues, the EES Regulation introduced two types of biometric identifiers – four fingerprints and a facial image – and has provided for the use of facial recognition technology for verification purposes at the border[99] and on national territory.[100] EES will rely on machine learning techniques for biometric matching.[101] Facial images may also be used *in combination with fingerprints* to identify individuals and border authorities or immigration authorities

[94] GDPR, art 3(13).

[95] See *Peck v UK* (2003) 36 EHRR 41; *Gaughran v UK*, Appl no 45245/15, Judgment of 13 February 2020.

[96] GDPR, art 4(14).

[97] SIS II Regulation, art 20(2)(e). See also Regulation 810/2009, art 13.

[98] Commission, COM(2013) 95final.

[99] EES Regulation, art 23(2).

[100] Ibid art 26. Also according to Articles 24 and 25, facial images may be used as search keys to conduct searches in EES for the purposes of examining a visa application or having access to facilitation programmes.

[101] eu-LISA, 'Artificial Intelligence in the Operational Management of Large-scale IT Systems' (2020).

shall have access to search with the fingerprint data or the fingerprint data combined with the facial image, for the sole purpose of identifying any TCN who may have been registered previously in EES under a different identity or who does not fulfil or no longer fulfils the conditions for entry to, or for stay on, the territory of the Member States.

Furthermore, Articles 22–23 of the 2018 SIS framework regulate the processing of photographs, facial images and dactyloscopic data that fulfil minimum data quality standards and technical specifications and must be processed following a data quality check.[102] In rules almost identical to those envisaged in the SIS II Regulation of 2006 that first required the recording of fingerprints in SIS,[103] facial images will not only be used to confirm the identity of a person, but also 'as soon as it becomes technically possible, and while ensuring a high degree of reliability of identification' facial images may be used to identify a person in the context of regular border crossing points.[104] Before the implementation of this functionality, the Commission shall present a report on the availability, readiness and reliability of the required technology. The Parliament shall be consulted on the report. In delegated acts, the Commission will also determine 'other circumstances in which photographs and facial images may be used to identify persons'.[105] The wording of these provisions is vague, particularly the last part which leaves the door open to the Commission to enable live facial recognition technology ~~at the borders~~ without the knowledge of the persons affected. The Parliament's limited role in ensuring democratic scrutiny is problematic even more so since the introduction of facial images – and generally the adoption of the revised SIS framework – was not accompanied by an impact assessment evaluating the necessity and proportionality of this new functionality. The impetus towards the incorporation of facial images in SIS is high. The Joint Research Centre of the Commission conducted a study in this respect noting that 30% of alerts in SIS contain facial images already (out of the 965,000 alerts on persons stored in SIS)[106] and concluding that facial recognition technology could be integrated in SIS, listing 19 recommendations for the rollout of the technology, including different measures to ensure the highest possible quality of the stored data.[107]

[102] The Commission will adopt those standards and specifications. See Regulation 2018/1861, art 32(4). Also see Regulation 2018/1860, art 4.

[103] Compare with 2006 SIS Regulation, art 22.

[104] Regulation 2018/1861, art 33(4).

[105] Ibid.

[106] eu-LISA, 'SIS II – 2020 statistics' (March 2021).

[107] Javier Galbally Herrerro et al, 'Study on Face Identification Technology for its Implementation in the Schengen Information System' (2019) 9.

Similarly, with respect to ECRIS-TCN, which will also be used for border management purposes, Article 6 of the ECRIS-TCN Regulation foresees that in the first stage, facial images may be used only to confirm the identity of a TCN who has been identified as a result of an alphanumeric search or a search using fingerprint data. In the second stage and following a Commission delegated act, facial images will be used for the purpose of identifying TCNs in order to determine the Member States holding information on previous convictions concerning such persons.

As regards Eurodac, the 2016 proposal foresaw the inclusion of additional alphanumeric data and facial images to 'prime the system for searches to be made with facial recognition software in the future'.[108] The rules on facial images were agreed by the co-legislators prior to the adoption of the 2020 proposal. According to the interinstitutional agreement, facial images will be included to enable comparisons on that basis.[109]

Finally, in the revised VIS Regulation, the collection of live facial images is foreseen during the application process to enable biometric matching using facial recognition technology.[110] Furthermore, in rules mirroring the EES Regulation, facial images will be used to verify the identity of a visa holder at the borders[111] or to identify them in combination with their fingerprints.[112] However, it is explicitly stated that facial images shall not be the only search criterion.[113]

4.2 *The Challenges of Facial Recognition: The Reliability and Accuracy of Facial Images, Algorithmic Bias and Lurking Surveillance*

Facial recognition technology has the potential to identify individuals at a distance, in real-time or ex post, even without the knowledge and with limited interaction and inconvenience of the individual involved. Though facial recognition technology has progressed in the past years, it 'remains far more prone to errors than other biometrics'.[114] The risks associated to facial recognition

[108] Commission, '2016 Eurodac proposal' (n 30) 13.

[109] Ibid art 2(1). A reference that comparisons will be allowed solely on the basis of facial images, as a last resort, in circumstances where an individual's fingertips are too damaged to ensure a high level of accuracy or the individual concerned would refuse to provide fingerprints was deleted. See ibid arts 16(1). Compare with Council, Document 12816/16 (5 October 2016) 7.

[110] 2021 VIS Regulation, art 22a(1)(j).

[111] Ibid art 18.

[112] Ibid art 20.

[113] Idem.

[114] Tamir Israel, 'Facial Recognition at a Crossroads: Transformation at our Borders and Beyond' (Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic, 2020).

technology are recognised in the Commission AI proposal, which has classified as *high-level risk* AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons.[115]

The fundamental rights challenges of facial images are directly associated with their future use for facial recognition purposes. In particular, the degree of accuracy in facial recognition technology is vital to minimise the risk of false positive matches, namely results that may be unrelated to the individual, or false negative results, when the facial recognition algorithm fails to identify correct matches. Therefore, depending on the task, purpose and context of the use of facial images (verification or identification) the errors may be significantly different as well as the consequences for individuals affected. When applying this technology in public spaces for identification purposes in particular, even a relatively small proportion of errors (for example, 0,01%) still signifies that hundreds of people may be wrongly flagged. This is crucial, as facial recognition technology will be used for identification purposes, thus searches on the basis of a facial image (a portrait type picture or a probe retrieved from a camera from video surveillance) against the full content of information systems – crucially the BMS that will store all templates. False positive matches in particular may have important consequences for individuals, who may be flagged for secondary checks because of incorrect matching, or be identified as potential security risks based on SIS alerts and even be subject to discriminatory practices by national authorities.

Accuracy will be dependent on the quality of facial images. Ensuring high quality of facial images needs to respect Article 5(1)(d) of the GDPR and the underlying requirements of each information system on data quality.[116] However, as stressed above, the data quality issues experienced in the operation of information systems will backfire in this context as well. In the case of VIS, it has been found that biometrics were attached to the wrong application file, resulting in false matches.[117] As a result, the move towards facial recognition technology at the borders will be affected. The duties imposed on Member States on data quality may be insufficient, particularly in the near future with six massive, interoperable information systems that already experience data quality issues and whose records will exponentially grow. As a result, enabling eu-LISA to conduct automated quality checks to highlight potential data quality issues is not sufficient[118] unless coupled ~~to~~ specific obligations for the

[115] Commission, 'AI Proposal' (n 8) Annex III.

[116] See Regulation 2018/1861, art 44; 2021 VIS Regulation, art 29; EES Regulation, art 39.

[117] FRA, 'Under watchful eyes – biometrics, EU IT-systems and fundamental rights' (2018) 16.

[118] As is currently the case. See Regulation (EU) 2018/1726 [2018] OJ L295/99, art 12.

Member States to follow-up, by rectifying or deleting the flagged data within specific and tight deadlines and notify eu-LISA about their actions. Penalties for persistent violations are another option to consider.

In order to ensure a minimum level of accuracy across Member States, facial images must be of as high quality as possible. A portrait-style image for example, which is subject to certain quality standards and taken under controlled circumstances with appropriate lighting, will ensure high confidence matching. Probe images (taken at e-gates or through a CCTV camera under variable environmental conditions) will be of lower quality and may result in less accurate results. In relation to SIS, the Joint Research Council study on the introduction of face identification technology recommended to ~~always~~ use a live picture of the traveller and avoid using the face image stored in the passport chip because its low resolution reduces accuracy.[119] However, the EES Regulation allows operators using the system to exceptionally extract facial images from the chip of the electronic machine-readable travel document, provided that the image has 'sufficient image resolution and quality to be used in automated biometric matching'.[120] The study on SIS further ~~recommended~~ to store 'additional off-angle (yaw) images' for 'future potential uses, such as consultation using images acquired in unconstrained environments, essentially *video surveillance footage*.[121] These recommendations pose a series of privacy and data protection challenges: the principles of purpose limitation will be affected as well as the rights of the individuals whose personal data will be collected and stored for future undefined uses. Besides, the quality of images extracted from video footage may be insufficient to produce accurate matches using facial recognition technology, resulting in higher error rates.[122]

The size of the information system will also impact accurate identification since the higher the number of images which may be of insufficient quality, the higher the possibility of false matches. Another relevant factor is the age of the facial image. There is gradual increase in the possibility of a false match as the years since its capturing pass by. This will be particularly relevant in cases of children whose physical appearance and facial shape will be subject to change. A 'considerable degradation in performance' for face recognition algorithms on children has been found in comparison to the performance

[119] Galbally Herrerro et al (n 107).

[120] EES Regulation, art 15.

[121] Galbally Herrerro et al (n 10~~6~~) 113.

[122] National Institute for Standards and Technology (NIST), 'Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects' (2019).

obtained on adults.[123] With the revised rules on Eurodac and VIS lowering the threshold for capturing biometric identifiers to the age of six, these concerns are significantly heightened. Besides, as regards SIS, EES and ECRIS-TCN such threshold for capturing facial images does not exist. Finally, the fact that there are different ways to calculate and interpret error rates, which must be defined in advance, must also be taken into account.[124] In its Implementing Decision specifying data quality standards as regards EES, the maximum false positive identification rate is 0,1% and a false negative identification rate is 1%.[125] These rates may seem quite low, but considering the aforementioned factors, particularly the size of the system that is expected to process more than 50 million records, the false positive rate will result in a large number of TCNs being affected.[126]

Even if perfectly accurate and reliable facial recognition technology could be designed, the potential for public surveillance through 'covert, remote and mass capture and identification of images'[127] must also be addressed, as it may lead to a transformation of the way people understand and experience public space. It has been eloquently argued that 'facial recognition technologies are transforming ports of entry and exit into true panopticons, tracking and identifying travellers at numerous points throughout their border control journey and linking identification points that were previously distinct'.[128] Indeed, facial recognition technology employed *en masse* will further deepen and systematise the cloak of suspicion with which TCNs and generally people on the move are viewed.[129] The potential of extending the technologies adopted at the borders to other contexts, resulting in surveillance creep, cannot be overruled. As mentioned earlier, the ~~JRC~~ ~~report~~ on SIS mentioned the potential of collecting additional facial images for further additional and future uses.

Finally, the inherent limitations of facial recognition should be underlined. As research ~~by NIST~~ demonstrates,[130] the algorithms embedded in facial recognition systems produce higher false positive matches in cases of black people and women, particularly of black women. In that regard, ~~NIST~~ test~~ed~~ 189 facial

[123] Nisha Srinivas et al, 'Face Recognition Algorithm Bias: Performance Differences on Images of Children and Adults' (Proceedings of the IEEE/CVF Conference on Computer Vision and Patter Recognition Workshops, 2019).

[124] On evaluation metrics see Grother et al (n 8~~8~~); Galbally Herrerro et al (n 10~~6~~).

[125] Commission Implementing Decision (EU) 2019/329 [2019] OJ L57/18.

[126] Dumbrava (n 11) 25.

[127] Jennifer Lynch, 'Face off report – Law enforcement use of facial recognition technology' (Electronic Frontier Foundation, 2020) 7.

[128] Israel (n 114).

[129] See Statewatch, 'Automated suspicion: The EU's new travel surveillance initiatives' (2020).

[130] NIST (n 122).

recognition algorithms ~~and found~~ that most of them displayed bias. This finding is corroborated by another study that concluded that demographic factors may significantly influence various biometric algorithms and that current technology shows some degree of bias towards certain demographic groups.[131] Translated in the context of EU information systems for TCNs, it may be the case that people of colour may find themselves wrongly flagged by the systems in far more cases than white people, due to algorithmic bias. The consequences could range from secondary checks at the borders and on national territory to discriminatory practices, such as refusals of entry or degrading treatment. Such bias may be attributed to the training of the algorithms, which could be based on insufficient or flawed data or because algorithms replicate and reflect the biases and prejudices of those developing them. In order to address this challenge, eu-LISA has proposed either the use of representative datasets for training algorithms or the creation of synthetic datasets with the characteristics that are representative of that population.[132] However, neither solution is satisfactory; the former could pose data protection risks, particularly regarding purpose limitation and potentially data minimisation depending on how large are the datasets used for training the algorithms. The latter solution could entail higher error rates associated with the use of synthetic data.[133] Therefore, not only human intervention in establishing a hit must be ensured at all times, but also any automated exchange of data based on image matching should not be allowed. Importantly, the maturity of facial recognition technology must be carefully monitored prior and after its implementation so that these challenges are prevented as much as possible.

5 Conclusion

This article aimed to critically examine the fundamental rights implications in relation to privacy, data protection and non-discrimination stemming from the introduction of AI tools in the operation of information systems for TCNs. In immigration systems suffering from backlogs, lengthy delays and uncertain outcomes, the deployment of AI technology, such as automated, algorithmic risk assessments, appears as a panacea for treating pathogenic practices and promoting superficial neutrality in decision-making of applications for travel

[131] Pawel Drozdowski et al, 'Demographic Bias in Biometrics: A Survey on an Emerging Challenge' (2020) 1(2) IEEE Transactions on Technology and Society 89, 98.

[132] eu-LISA, 'Artificial Intelligence' (n 10~~0~~).

[133] Dumbrava (n 11) 27.

authorisations, visas (or even asylum applications). Furthermore, AI could also, more broadly, improve adaptation to a fast-paced geopolitical and security environment. In the White Paper on AI, the Commission stresses that 'as digital technology becomes an ever more central part of every aspect of people's lives, people should be able to trust it.'[134] The analysis has shown that such trust cannot be substantiated yet: automated comparisons of data present in information systems and databases capitalise on data collection but could be based on unreliable information – poor quality of data are destined to produce equally poor outcomes. Importantly, algorithmic profiling may reinforce existing non-entrée policies, by transforming discriminatory practices in the decision-making on travel authorisations and visas into discriminatory algorithms.

In supporting decision-making by flagging potentially risky individuals, such techniques essentially take advantage of the weak position of TCNs at the borders, who will find it extremely hard to contest the technological fixes. Facial recognition technology is equally problematic, with algorithmic bias being a significant risk, as AI is known for discriminating on the grounds of race or gender. Thus, the potential for social sorting of foreigners depending on whether they originate from specific countries is more than a rhetoric. As a minimum the reinforcement of effective remedies for TCNs affected and raising awareness about their existence are central. Accountability, transparency, close monitoring in the development of algorithms and clear obligations on Member States to maintain high data quality in information systems are also vital.

These developments have been introduced in existing legal instruments without prior scrutiny or impact assessments of the fundamental rights implications that they entail, but with the future development of EU border management in mind. Thus, information systems have been future-proofed by incorporating AI tools in anticipation of the further development of digital technologies, but excluding them from the safeguards of a forthcoming AI Regulation. These efforts are also in striking contrast to calls by the UN Special Rapporteur for on contemporary forms of racism, racial discrimination, xenophobia and related intolerance rightly called for a moratorium on or an immediate moratorium on the sale, transfer and use of surveillance technology, until robust human rights safeguards are in place to regulate such practices.[135]

[134] Commission, COM(2020) 65 final.

[135] UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, 'Racial discrimination and emerging digital technologies: a human rights analysis' (2020).

Interoperability is also showing its true colours; both automated comparisons and facial recognition technology will become possible through interoperability components. Under this technology-driven approach TCNs continue to be used as test beds ~~or experimentation grounds~~ for emerging technologies, as it has been the case with fingerprinting in the past.

Data is the foundation of AI. Without the proliferation of information systems to collect personal data of almost the entire non-EU population with an administrative or criminal law link to the EU, the transition to AI to assist in 'sieving' the data and identify the unknown, risky foreigner would not have been possible. With more intrusive and highly controversial AI tools contemplated and tested, for example emotion detection,[136] chatbots and virtual assistants, or risk assessment and application triaging in the context of the visa process,[137] it remains to be seen whether, when and how the digital experiment on TCNs will evolve.

AQ 2

Acknowledgements

I am grateful to the editor of this special issue and to Valsamis Mitsilegas, Merve Hickok and Alexandra Karaiskou for their insightful comments in earlier drafts of this article. Any errors remain, of course, my own.

[136] Developed through the iBorderCtrl project. See Javier Sánchez-Monedero & Lina Dencik, 'The Politics of Deceptive Borders: "Biomarkers of Deceit" and the Case of iBorderCtrl' (2020) Information, Communication & Society 1.

[137] See Commission (n 7). A Commission Proposal on the digitalisation of the visa procedure is expected in late 2021.

AQ 1: Please provide complete affiliation details and ORCID if you have one

AQ 2: Converted asterisk note to Acknowledgements, please check if correct