Analysis

Disproportionate and discriminatory: the European Criminal Records Information System on Third-Country Nationals (ECRIS-TCN)

- **The ECRIS-TCN, which will hold the personal data of non-EU citizens convicted in EU Member States, is designed to 'complement' the existing ECRIS for EU nationals**
- **The EU's 'interoperability' agenda propelled the choice of a more privacy-intrusive centralised, rather than decentralised, system**
- **Dual nationals will also have their personal data included in the system, violating the right to non-discrimination by creating two 'tiers' of EU citizens**

Chris Jones
February 2019

1. Introduction

The EU will soon have another new biometric database to add to its growing collection – the European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN), designed to make it easier for the EU's national authorities to obtain the criminal records of non-EU nationals who have been convicted in another Member State.

The text of the Regulation governing the ECRIS-TCN has been informally agreed between the European Parliament and the Council of the EU and is now awaiting formal adoption by both institutions. ECRIS-TCN will be a centralised database, managed by the European Agency for Large-Scale IT Systems (eu-Lisa), with connections to a national central access point in each Member State. It will hold "identity information" (biographic data, fingerprints and potentially facial images) that will be accessed by national authorities to ascertain whether people holding citizenship of a non-EU state ("third-country nationals") or stateless persons have a criminal record in any other EU Member State. If a search in the ECRIS-TCN returns a "hit", the authorities will have to use the existing ECRIS (in operation since 2012) to obtain further information.

Member States' authorities will be able to use the system to request information for use in both criminal and non-criminal proceedings. Regarding the latter, the agreed text sets out seven possible non-criminal proceedings for which requests can be made (in Article 7(1)),[1] although Member States can also decide upon their own purposes, "if provided under and in accordance with national law." In this case, they will have to notify the European Commission of these other purposes so that they can be published in the Official Journal of the EU. Three EU agencies – Europol, Eurojust and the European Public Prosecutor's Office (EPPO) will also be afforded direct access to the system, for various reasons (set out in the annex to this report).

The final text of the Regulation raises a number of concerns regarding the rights to privacy, data protection and non-discrimination. Firstly, it is not clear that the establishment of a centralised database was necessary to achieve the intended policy goal. Secondly, the Regulation imposes a new fingerprinting requirement in some Member States. Thirdly, it discriminates in general against dual nationals (those holding EU and non-EU citizenship) and because of this may well lead to specific instances of discrimination against non-white EU citizens. Before examining these issues, however, an explanation of the system and its context is necessary.

2. Exchanging criminal records

The European Criminal Records Information System (ECRIS) was established in 2009[2] and began functioning in 2012. It is used for transferring, between EU Member States, information

[1] Checking person's own criminal record at their request; security clearances; obtaining a license or permit; employment vetting; vetting for voluntary activities involving direct and regular contacts with children or vulnerable persons; visa, acquisition of citizenship and migration procedures, including asylum procedures; and checks in relation with public contracts and public examinations.

[2] Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009F0315; Council Decision 2009/316/JHA of 6

extracted from national criminal records. That information can be used in criminal proceedings (in which case provision of the information is mandatory) or for "purposes other than criminal proceedings" (in which case information can only be provided if it is permitted by the national law of the two Member States involved in the transaction). The system was introduced to help implement the obligation for convictions handed down in other Member States to be taken into account in criminal proceedings.[3]

The system has grown significantly since the legislation came into force. The European Commission reported in June 2017 that after five years of operation, all 28 EU Member States were connected to the system, although "24% of possible interconnections" were missing.[4] 300,000 messages were sent during 2012, a number that had grown to 2,000,000 by the end of 2016. The most active states in that year were: Germany (which sent over 246,000 requests for information, notifications of convictions and replies to requests for information); the UK (over 143,000 of the three types of message sent); Italy (almost 81,000); Poland (69,374); and Romania (almost 58,000).[5]

According to the legislation establishing ECRIS, every Member State must ensure that all its criminal records include information on the nationality or nationalities of the convicted person. When one or more of those nationalities is that of another Member State, that other Member State – the "Member State of nationality" – must be informed of and store the information on the conviction. Information on any subsequent alterations or deletions to the information in the criminal record must also be sent to the Member State of nationality.

In this way, an individual's state of nationality becomes the central repository for their criminal record and requests for criminal record information on that individual need only be sent to that state. However, because non-EU states do not participate in the ECRIS, information on the criminal records of third-country nationals is not systematically available to Member States unless "blanket requests" are made to all other Member States, in order to see whether they hold such information. As the agreed text of the ECRIS-TCN Regulation says, this puts "a disproportionate administrative burden on all Member States, including those not holding information on the third-country national."[6]

April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009D0316

[3] This obligation was introduced by a Council Framework Decision in 2008: Council Framework Decision of 2008/675/JHA of 24 July 2008 on taking account of convictions in the Member States of the European Union in the course of new criminal proceedings, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008F0675

[4] As a decentralised information exchange network, each Member State has to establish a connection with each of the other 27 Member States. This is also how the Prüm system for exchanging data on DNA, fingerprints and vehicle registration data works.

[5] European Commission, Report from the Commission to the European Parliament and the Council concerning the exchange through the European Criminal Records Information System (ECRIS) of information extracted from criminal records between the Member States, COM(2017) 341 final, 29 June 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017DC0341

[6] Recital 6.

3. Upgrading the system

In an attempt to address this situation, in January 2016 the European Commission published a proposal for a Directive on an ECRIS for third-country nationals.[7] This would have required the national authorities of any Member State convicting a non-EU national to ensure the storage of a set of personal data in pseudonymised[8] form in an "index-filter".

The "index-filter" would have been made available in a decentralised manner so that all Member States could search it.[9] A successful search would have produced a notice telling the searching Member State to contact the Member State(s) holding information on the individual they were looking for. This decentralised system was subsequently discarded for a number of reasons (see further below), even though it would have been less intrusive on privacy rights – and potentially less expensive – than the system that has now been established.[10] Other aspects of the Directive, dealing with amendments to the existing ECRIS, will come into force alongside the ECRIS-TCN Regulation.[11]

Following the rejection of the decentralised system, the Regulation was proposed in June 2017 and it is this text on which the Parliament and Council recently reached agreement. It establishes a centralised database of convicted third-country nationals' identity data (alphanumeric data, fingerprints and facial images, if the latter are permitted by national law). Like the proposed "index-filter" it replaces, a "hit" in the centralised database would inform the searching Member State which other Member State(s) to contact for more information. The issues surrounding the establishment of this database; the imposition of a new fingerprinting obligation for convicted persons; and the potentially discriminatory implications of some of the rules are examined below.

4. Another new centralised database: necessity or interoperability?

The establishment of a centralised database for the ECRIS-TCN is controversial, because it runs counter to the requirement for the authorities to employ the least intrusive option when

---

[7] Proposal for a Directive of the European Parliament and of the Council amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA, COM(2016) 7 final, 19 January 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2016:7:FIN

[8] The proposal referred to anonymised identity information, when in fact it would have been pseudonymised. See: EDPS, 'Opinion on the exchange of information on third country nationals as regards the European Criminal Records Information System (ECRIS)', Opinion 3/2016, 13 April 2016, p.9, https://edps.europa.eu/sites/edp/files/publication/16-04-13_ecris_en.pdf

[9] Article 4a of the proposal for a Directive.

[10] A revised version of the Directive was submitted by the Dutch Council Presidency "in liaison with the Commission" and serves to "complement the existing Framework Decision on matters of general nature related to the functioning of ECRIS." The compromise text agreed between the Council and Parliament is contained in Council document 15535/18, http://data.consilium.europa.eu/doc/document/ST-15535-2018-INIT/en/pdf

[11] The text of the Directive as agreed is contained in Council document 15702/18, https://data.consilium.europa.eu/doc/document/ST-15702-2018-INIT/en/pdf

infringing upon individual rights (in this case, principally the rights to privacy and data protection).

In its impact assessment accompanying the proposal for a Directive, the European Commission said that a decentralised system fulfils the general and specific objectives,"[12] is more cost-efficient than a centralised option and "complies better with the principle of non-discrimination" as it "does not require an additional layer at EU level not existent for EU nationals".[13] However, following studies into the practical requirements for setting up such a system, the Commission declared that the technology under consideration was not in fact suitable, despite one study highlighting technology "suitable for large scale environments such as ECRIS."[14]

Perhaps more important than these technical issues, however, was political pressure. At the Justice and Home Affairs Council on 9 June 2016 the Member States' interior and justice ministers declared:

> *"Ministers supported a change of the approach from a decentralised system, as proposed by the Commission, to a centralised automated one for the exchange and storage of both fingerprints and alphanumeric data of convicted third country nationals. They invited experts to continue the discussion on the technical details of such a system in particular with regards to data protection and the possibility of*

[12] The general objectives: to improve the functioning of a common area of security and justice by improving information exchange in criminal matters; to reduce crime and foster crime prevention (including terrorism); to ensure equal treatment of TCN and EU nationals with regard to an efficient exchange of criminal record information. The specific objectives: to reduce the number of unnecessary requests for TCN-related criminal record information and the resulting costs; to increase criminal record information exchange through ECRIS with regard to TCN.

[13] Impact Assessment Accompanying the proposal for a Directive of the European Parliament and of the Council amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA, SWD(2016) 04 final, 19 January 2016, p.33, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2016:0004:FIN

[14] The Impact Assessment that accompanied the proposal for a Directive said: "From an in-depth assessment of these IT solutions, it emerged that the IT solution "Ma3tch" already used by the FIU.net would meet the needs of the ECRIS TCN system." Yet the same Impact Assessment also said: "to date no sufficiently mature matching technology for anonymised fingerprints offering sufficient capacity has been tested in large-scale information exchange systems. More research is required to assess the efficient application of Privacy by Design approach to biometrics such as fingerprints." Subsequent studies confirmed that the Ma3tch technology would not be suitable, due to problems with deploying the technology on fingerprints at large scale. However, a study by the consultancy Kurt Salmon highlighted "alternative pseudonymisation strategies which are based on the removal of biographical identity data from fingerprints. These strategies are suitable for large scale environments such as ECRIS." See: SWD(2016) 04 final, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2016:0004:FIN

complementing the automated features by the possibility of performing also manual checks at national level."[15]

Discussions between "the ECRIS community" and the Commission's high-level expert group on information systems and interoperability also took place. In May 2017 the high-level expert group issued its final report, which included recommendations for a centralised ECRIS-TCN.[16] A further study examined the feasibility of a centralised ECRIS-TCN and set out "the high-level architecture, key principles and processes of the envisaged centralised ECRIS TCN solution."[17]

a. Three reasons

In the June 2017 proposal for a Regulation, three main arguments were offered to justify the shift to a centralised system: that it would be cheaper and less complex to develop than a decentralised system; that it would assist with the implementation of the interoperability agenda; and that it would not be any more intrusive for the fundamental rights to privacy and data protection than a decentralised system.

With regard to the issue of cost, the Commission stated in the Impact Assessment:

---

[15] 'Outcome of the meeting', Justice and Home Affairs Council, Luxembourg, 9 and 10 June 2016, http://statewatch.org/news/2016/jun/eu-jha-council-9-10-jun-prel.pdf

[16] The group made two recommendations on ECRIS-TCN:
"In its upcoming legislative proposal, the Commission, in close cooperation with eu-LISA, should ensure that the ECRIS-TCN system could make use of a future shared biometric matching service and, if appropriate, common identity repository."
"In its upcoming legislative proposal, the Commission should ensure that relevant data under the ECRIS-TCN system can be used in the context of assessing travel authorisation requests of third-country nationals."
Also under discussion were "whether or not actual conviction information should be stored at central level in order to make it available for security and border control purposes" (something also examined by the Wavestone study); "whether a central ECRIS-TCN database would be suitable for use in a European search portal"; and how the use of criminal records information for ETIAS [European Travel Information and Authorisation System] decisions can be best ensured." See: European Commission High-level expert group on information systems and interoperability, 'Final report', May 2017, p.23, http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1

[17] This study examined "the technical feasibility and cost impacts of implementing a centralised ECRIS TCN solution as well as… the interoperability, future-proofing and possible extensions of the system." It thus also looked at the "integration of the centralised ECRIS-TCN solution with other European large scale systems"; "the possibility of using a shared Biometric Matching Service (BMS); "granting direct access to ECRIS TCN to third parties such as Eurojust and Europol"; and "extending the ECRIS TCN solution by including the identity data of convicted EU nationals." See: Wavestone, 'Feasibility study and cost assessment of a centralised ECRIS TCN solution', 13 June 2017, http://ec.europa.eu/newsroom/document.cfm?doc_id=45363

"Although there are some differences between the centralised and decentralised options, these differences are not so important that they would justify spending significantly more on the creation of a decentralised solution."[18]

However, judging by the figures provided in the various studies carried out, the centralised solution may not be any cheaper than a decentralised one.[19] The June 2017 proposal for a Regulation foresaw total one-off costs to the EU and the Member States of €26.3m, with ongoing costs starting at €8.2m per year and increasing to a maximum of €17.5m per year. These annual maintenance costs would soon make it costlier than the most expensive decentralised option examined in a Commission-contracted report, estimated at €46.6m in one-off costs with €10.8m annual maintenance costs. In any case, as the European Data Protection Supervisor pointed out: "costs cannot become a significant factor in judging the lawfulness of the limitation of fundamental rights."[20]

Beyond the price factor, the push for a centralised system also appears to have been significantly influenced by the push for "interoperability" of the EU's policing and migration databases and information systems.[21] While the recitals (introductory paragraphs) of the discarded Directive highlighted that "recent terrorist attacks demonstrated in particular the urgency of enhancing relevant information sharing" – something that could have been achieved through a decentralised system – the June 2017 proposal for a Regulation went further. According to this text, the "political stance regarding systematic use of fingerprints for

---

[18] SWD(2016) 04 final, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2016:0004:FIN

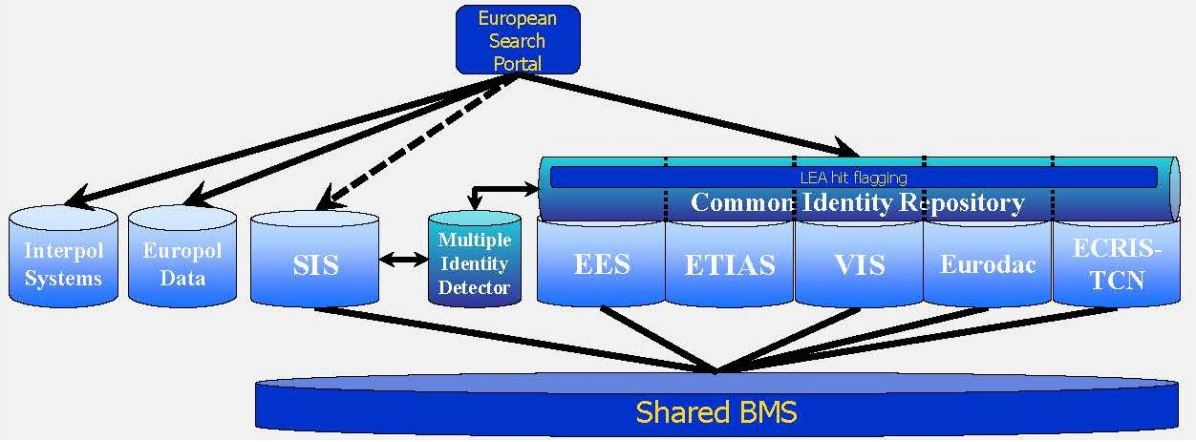
[19] The costs presented by the Commission have changed significantly throughout the procedure in line with different technical appraisals. The decentralised option without mandatory fingerprints favoured by the Directive (January 2016) was initially estimated to cost the EU and the Member States a total of €1.86m with yearly maintenance costs of €706,000. With compulsory fingerprints, these figures would rise to €42.5m and €12.5m. The centralised option was estimated to cost €6.1m with maintenance costs of €1.5m (with fingerprints, €39.5m and €11.7m respectively).
In the Kurt Salmon study (June 2016), the most expensive decentralised option examined was estimated to cost the EU and the Member States €46.6m with €10.8m annual maintenance costs, with three other decentralised options estimated at: €36.5m one-off costs (and €9.4m in annual maintenance); €26.6m (€2.3m); and €22m (€2.7m). The two most expensive centralised options examined were estimated at €15.9m in one-off costs and just over €2m in annual maintenance, followed by two options estimated at €6.9m (€2m annual maintenance).
The Wavestone study (June 2017) estimated that a centralised ECRIS-TCN would cost the EU and the Member States a total of approximately €48m over seven years – €8.8m in one-off costs in 2018, 2019 and 2020, and subsequent annual costs of €3.6m.
The proposed Regulation (June 2017) foresees total one-off costs to the EU and the Member States of €26.3m, with ongoing yearly costs starting at €8.2m and increasing to a maximum of €17.5m. Thus it seems that the annual maintenance costs of the system foreseen by the Regulation will eventually make it far more expensive than the most expensive decentralised option examined by the Kurt Salmon study.

[20] European Data Protection Supervisor, 'Opinion on the proposal for a Regulation on the ECRIS-TCN', Opinion 11/2017, 12 December 2017, p.10, https://edps.europa.eu/data-protection/our-work/publications/opinions/proposal-regulation-ecris-tcn_en

[21] See: Statewatch Observatory: Creation of a centralised Justice & Home Affairs database is "a point of no return", http://www.statewatch.org/interoperability/eu-big-brother-database.htm

secure identification and generally the attitude towards data sharing and security has changed," following a fresh spate of deadly terrorist attacks in Europe.[22]

There was now a need "to exploit synergies between different European information exchange systems," supported by "a centralised ECRIS-TCN system containing both fingerprints and other identity information," argued the Commission. In fact, the proposal said, "interoperability would not be possible if a decentralised solution as proposed in January 2016 would have been pursued."[23] It would not be unreasonable, then, to suggest that the tail was wagging the dog – yet no matter how enticing the EU's interoperability agenda is to policy-makers, it is not in itself a relevant reason for establishing a new centralised database.[24]



Interconnections foreseen between EU and other databases under the "interoperability" proposals, with the ECRIS-TCN as one of the five EU databases to be directly connected to the Common Identity Repository and shared Biometric Matching Service.[25] Source: European Commission, COM(2017) 794 final

Finally, the Commission argued that a centralised system would not necessarily be any more intrusive than a decentralised one with regard to privacy and data protection rights. Oddly, however, the Commission itself argued in the 2016 impact assessment that a decentralised system "complies better with the principle of non-discrimination" as compared to a centralised

---

[22] The interoperability agenda has long been on the cards and EU officials have repeatedly suggested that one 'super-database' would help prevent terrorist atrocities. No matter how unlikely this may be, it has provided greater impetus to the interoperability agenda.

[23] SWD(2016) 04 final, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2016:0004:FIN

[24] This point was also raised by the EDPS: "the objective of ensuring interoperability of ECRIS-TCN with other EU large-scale IT systems in the area of freedom, security and justice does not in itself justify the necessity of a centralised solution nor, of the data envisaged for processing." See: EDPS, 'Opinion 11/2017', p.10,

[25] The function and aim of each of these elements of the interoperability plan – the biometric matching system (BMS), European search portal (ESP), central identity register (CIR) and multiple-identity detector (MID) – is explained in pages 6-8 of the Commission's proposal (COM(2017) 794 final): http://www.statewatch.org/interoperability/interoperability/commission/eu-com-794-interop-regulation-swd-police-judicial-cooperation-asylum-migration-0352-17.pdf

system, which would lead to "unnecessary differences in the treatment of the personal data of EU nationals and TCN."[26]

By 2017, the Commission had switched tack. A supporting document to the June 2017 proposal said that "whilst it could be argued that [a centralised system] creates an additional layer of complexity" – as the 2016 proposal did indeed argue – "there is no doubt that effective data protection regimes can be created at the central level." While this may be true, it does not in itself justify the creation of another centralised database. Furthermore, no detailed assessment of the proposed centralised system and its impact on fundamental rights was ever carried out, "although this is an important element of the Commission policy of better regulation, and an essential prerequisite when fundamental rights are at stake."[27]

The justifications for the shift to a centralised system were, then, rather flimsy. If anything, it seems that the interoperability agenda propelled the decision to create a centralised database as much as any considerations on cost or fundamental rights. Beyond the questionable reasoning that led to the establishment of a centralised database, meanwhile, such a system generates further problems of its own.

b. Sensitive data in the centralised system

Article 5 of the agreed text requires that every individual record in the ECRIS-TCN database contain a set of alphanumeric data,[28] and may also hold two types of biometric data – fingerprints and a facial image.

National authorities will be obliged to include fingerprints in the ECRIS-TCN database "with the aim of identifying the Member State or Member States in possession of criminal records information on a third country national". The Commission stated that the mandatory inclusion of fingerprints was being proposed:

> *"because the discussions on the 2016 proposal [for a Directive] have clarified that there is strong support from the legislators for including fingerprints, even if discussions on the details of the implementation have not yet been finalised."*[29]

---

[26] European Commission, 'Impact Assessment', SWD(2016) 4 final, 19 January 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2016:0004:FIN

[27] EDPS, 'Opinion 11/2017', *op. cit.*, p.10, https://edps.europa.eu/data-protection/our-work/publications/opinions/proposal-regulation-ecris-tcn_en

[28] According to Article 5(1)(a)(i) of the agreed text, the following alphanumeric data will be obligatory: surname (family name); first name(s) (given names); date of birth; place of birth (town and country); nationality or nationalities; gender; previous name(s), if applicable; the code of the convicting Member State. Parents' names may also be included, if they are contained in the national criminal record, and if it is available to the national central authority then the following should also be included: identity number, or the type and number of the person's identification document(s), as well as the name of the issuing authority thereof; pseudonym and/or alias name(s).

[29] European Commission, Analytical Supporting Document, SWD(2017) 248 final, 29 June 2017, https://ec.europa.eu/info/sites/info/files/analytical_supporting_document_accompanying_the_proposal_2.pdf

While fingerprints are no doubt useful for reliable confirmation of identity, there is little indication that their use is actually necessary in this case – as remarked by the EDPS, from 2012 to 2016 between 1% and 3% of requests through the existing ECRIS resulted in multiple identities being found. The EDPS' suggestion that "the use of fingerprints should be for the identification of TCN only if the identity of TCN cannot be ascertained by other means," fell on deaf ears (although it seems that even this proposal would have required the collection of fingerprints, in case they were needed later).

The agreed text includes two criteria for entering fingerprints in the central database, in Article 5(b). Firstly, "fingerprints of third-country nationals that have been collected in accordance with national law during criminal proceedings" – that is to say the application of existing national law, where it deals with such matters. Second is a two-pronged provision:

> *"as a minimum, fingerprints on the basis of either of the following criteria:*
>
> *where the third country national has been convicted to a custodial sentence of a minimum of six months;*
>
> *or*
>
> *where the third country national has been convicted in relation to a criminal offence which is punishable under the national law of the Member State by a custodial sentence for a maximum period of at least 12 months."*

This new "minimum" criteria will, in many Member States, introduce a new requirement for fingerprinting convicted persons, provided that their conviction meets one of the two thresholds. This issue has been controversial since the start of the move towards the ECRIS-TCN. In a document accompanying the January 2016 proposal for a Directive, the Commission noted that:

> *"… a number of Member States have expressed constitutional concerns and drawn attention to problems regarding the practical implementation of mandatory fingerprints in ECRIS. Many Member States do currently not use fingerprints in their national criminal record registers or are connected to their national AFIS."*

Furthermore, said the January 2016 document:

> *"…some Member States are concerned about possible double standards for EU nationals on the one hand and TCN on the other hand and the fact that not all convicted persons contained in the national criminal record registers have had fingerprints taken, as national rules differ according to categories of offences and between Member States."*

This new rule introduces precisely such a double standard, which it seems will be widespread across the EU. As of January 2016, according to the European Commission, "eight Member States exchange fingerprints in ECRIS: EE, ES, FI, UK, LT, LV, RO and SE [Estonia, Spain, Finland, UK, Lithuania, Latvia, Romania and Sweden]," while "only a few include fingerprints in their criminal records (UK, PT, LV [UK, Portugal, Latvia]) or have a link between their

criminal records and their fingerprint database(s) (LT, HU, RO [Lithuania, Hungary, Romania]).”[30]

Now, all states will be obliged to include the fingerprints of non-EU nationals in national criminal records, so that they can be provided to the ECRIS-TCN database – yet no such requirement will exist in many Member States for their own nationals (dual nationals are also excluded, see section 5.b). Article 12 of the Regulation requires that Member States establish “a secure connection between their national criminal records and fingerprints databases and the national central access points,” presumably to facilitate the transfer of non-EU nationals’ fingerprints to the national criminal record system and subsequently to the ECRIS-TCN.

Regarding facial images, meanwhile, Article 5 of the agreed text says:

> *“The data record may also contain facial images of the convicted third country national, if the national law of the Member State where a conviction is handed down allows for the collection and storage of facial images of a convicted person.”*

This allows Member States to include facial images alongside the other data they store in the ECRIS-TCN. However, according to Article 6(2), before the system can be searched with facial images the Commission:

> *“shall, taking into account the necessity and proportionality as well as technical developments in the field of facial recognition software, assess the availability and readiness of the required technology.”*

If a positive assessment ensues, the Commission will have to adopt a delegated act to permit the use of facial images as a search key, in accordance with Article 34a of the Regulation.

It should be noted that the Directive on ECRIS-TCN, which also amends aspects of the existing ECRIS, will introduce a requirement for national authorities to provide facial images of EU nationals as part of their response to requests for information through the existing ECRIS, if they are available to the central authority.[31] This provision was added to the text by the Council.

---

[30] Footnote 32, p.15, SWD(2016) 4 final, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2016:0004:FIN

[31] Contained in a new Article 11(1)(c)(iv). Article 11 of Framework Decision 2009/315/JHA, as amended by the Directive, will read:
When transmitting information in accordance with Article 4(2) and (3), the central authority of the convicting Member State shall transmit the following information:
(…)
(c) information that shall be transmitted, if available to the central authority (additional information):
(i) the convicted person’s identity number, or the type and number of the person’s identification document;
(ii) fingerprints, which have been taken from that person; and
(iii) if applicable, pseudonym and/or alias name(s).
(iv) facial image.”

There was no attempt by the Commission to justify the necessity and proportionality of including facial images in the ECRIS-TCN database. It appears, however, that the desire for "interoperability" played its part here too. According to the "analytical supporting document" published with the proposal for a Regulation:

> *"the system should be designed to take possible future interconnections into consideration, the Member States confirmed that, in their opinion, the one element which should be implemented right from the start would be the use of the shared biometric matching service [BMS, one component of the interoperability agenda]. In addition, Member States indicated that the possibility to store facial images should be created from the start, so that at a later stage facial recognition software could be deployed for even more effective identification."*[32]

5. Discrimination

As noted above, the system discriminates against non-EU citizens by requiring that they be fingerprinted in situations where the same may not be required for EU citizens. However, the system also introduces a number of other discriminatory measures that are not necessarily justified. These arise from the hit/no-hit function of the database and the situation of dual nationals who hold citizenship of EU and non-EU states.

a. The hit/no-hit system

Under the current ECRIS system, Member States may make requests for information on convictions for use in both criminal proceedings and other situations – for example, for background checks on job applicants.[33] This is also the case for the ECRIS-TCN system. However, when requests for information on EU nationals are made through the ECRIS, the requested Member States' authorities do not have to respond. This means they can comply with the requirement to not disclose any information unless doing so is legal in both the requesting and the requested state.[34]

In the case of the ECRIS-TCN, whatever the reason for their search, national authorities will receive a "hit" if their query matches information held in the central database. In his opinion on the Regulation, the EDPS highlighted that "the mere knowledge of the existence of a

---

[32] European Commission, 'Analytical Supporting Document', SWD(2017) 248 final, p.8,

[33] Article 7 of the agreed text sets out seven grounds for searching the ECRIS-TCN in relation to for non-criminal proceedings: checking person's own criminal record at their request; security clearances; obtaining a license or permit; employment vetting; vetting for voluntary activities involving direct and regular contacts with children or vulnerable persons; visa, acquisition of citizenship and migration procedures, including asylum procedures; and checks in relation with public contracts and public examinations.
This is, however, not exhaustive – under Article 7(1a), any Member State may "use the ECRIS-TCN system for any purposes other than those set out in paragraph 1," provided that those purposes are "provided under and in accordance with national law." Member States which intend to make use of the ECRIS-TCN for other purposes must notify the Commission, which is then obliged to publish them in the Official Journal of the EU.

[34] Article 7 of Framework Decision 2009/315/JHA.

criminal conviction" could "have an adverse impact on TCN," and potentially "give rise to discriminatory attitudes." Furthermore:

> *"The information would also not be useful if it cannot be further retrieved and thus it would not comply with the data quality principle (i.e. only the personal data which are necessary for the stated purpose may be processed)."*[35]

The EDPS suggested that the system should be designed to trigger a hit "only for the purposes for which the requested Member State(s) is allowed to provide information in accordance with its national law" – undoubtedly complex, but compliant with fundamental rights requirements. The system could also have been designed to automatically notify the requested Member State that another Member State authority was seeking information they held, allowing them to choose whether to reply or not.

In the event, however, all that has been put in place is a recital in the Regulation that states:

> *"A hit indicated by the ECRIS-TCN system should not automatically mean that the third country national concerned was convicted in the indicated Member State(s). The existence of previous convictions should only be confirmed based on information received from the criminal records of the Member States concerned."*[36]

This hardly seem sufficient to prevent suspicion being cast over people whose data triggers a "hit" in the ECRIS-TCN database, but cannot be obtained from the Member State holding it.

b. Dual nationals

The Commission's proposal for a Regulation discriminated against dual nationals who hold citizenship both of EU and non-EU states. It sought to define "third country national" as:

> *"a national of a country other than a Member State regardless of whether the person also holds the nationality of a Member State, or a stateless person or a person whose nationality is unknown to the convicting Member State."*

The Meijers Committee of legal experts pointed out that:

> *"According to this proposal, a large category of Union citizens will for the first time in Union Law no longer be treated as Union citizens but as nationals of third countries. De facto, this proposal will introduce the idea of first and second class Union citizens."*[37]

The Council and Commission's main concern with this issue was that "dual nationals should be included in the system in order to 'close the loopholes', given that people could 'hide' behind another nationality" (no evidence has been provided – at least publicly – to back up this assertion). In June, it seemed that the Parliament had prevailed, with a Council document

---

[35] EDPS, 'Opinion 11/2017', p.13
[36] Recital 19.
[37] Meijers Committee, 'Note on the definition of third-country nationals in the Commission's ECRIS-TCN proposal', 2 October 2017, http://www.commissie-meijers.nl/sites/all/files/cm1710_note_on_ecris-tcn.pdf

noting a compromise in which dual nationals would not be included in the ECRIS-TCN.[38] By early September, however, while the question of how "third-country national" was to be defined was still up for discussion (in the end, the Parliament's preferred definition made it into the final text[39]), the Parliament had accepted the Council and Commission position on the inclusion of dual nationals in the database.[40]

This has been achieved through the expansive scope of the text – Article 2 states that "the provisions of this Regulation that apply to third country nationals also apply to citizens of the Union who also hold the nationality of a third country and who have been subject to convictions in the Member States," rendering moot the issue of how "third-country national" is defined.

There is only one exception to Article 2, which concerns fingerprints. Article 5(1)(b)(ii) of the agreed text (requiring fingerprinting of non-EU nationals unless they have been convicted to a sentence of less than six months or for an offence which carries a maximum sentence of less than 12 months, as discussed in section 4.b), will not apply to dual nationals. However, as with all other non-EU nationals, dual nationals will have a facial image included in the system provided national law makes it possible to do so. The Commission, meanwhile, was so upset with the non-inclusion of dual nationals' fingerprints in the database that it issued a declaration on the issue.[41]

Excluding dual nationals' fingerprints from the database appears to have been the Parliament's attempt to prevent discrimination – or, at least, to make the system 'less' discriminatory.[42] The Meijers Committee was not impressed by the final text. It warned that

---

[38] 9894/18, 11 June 2018

[39] "Third country national" is defined in the agreed text as "a person who is not a citizen of the Union within the meaning of Article 20(1) TFEU, or a stateless person or a person whose nationality is unknown". Article 20(1) TFEU states: "Every person holding the nationality of a Member State shall be a citizen of the Union. Citizenship of the Union shall be additional to and not replace national citizenship."

[40] Council document 11310/18, http://statewatch.org/news/2019/feb/eu-council-ecris-tcn-dual-nationals-fingerprints-ep-11310-18.pdf

[41] "The Commission regrets that the co-legislators have decided to limit the inclusion of fingerprints of convicted third country nationals and dual EU/third country nationals in the ECRIS-TCN system. Since fingerprints are currently the most reliable form of identification of individuals, the Commission regrets these limitations on the inclusion of fingerprints, which in its view will make the ECRIS-TCN system less effective in achieving its aim of ensuring that criminal records information is reliably made available for the purposes of criminal procedures, preventing child abuse, granting licences and other legitimate purposes laid down in national law in line with the Directive." See: Council document 15701/18 ADD 1, https://data.consilium.europa.eu/doc/document/ST-15701-2018-ADD-1/en/pdf

[42] A Council document explains that this approach means that dual nationals' fingerprints will be included in the system on the same basis as EU nationals' fingerprints are in the existing ECRIS: "the ECRIS-TCN system will contain identity information of both third country nationals (TCN) and dual nationals (= EU-citizens that also have the nationality of a third country). However, while as regards TCN fingerprints will be inserted on the basis of the Council general approach (with the two minimum rules), as regards dual nationals fingerprints will only be inserted when they have been collected in accordance with national law. In this way, the conditions under which fingerprint data can be included in the ECRIS-TCN system with regard to dual nationals will be comparable to the conditions under which fingerprint data are exchanged between Member States with respect to citizens of the Union

"the ECRIS-TCN database, if adopted, would fail to respect the fundamental right to non-discrimination" and urged MEPs "not to adopt proposals which would violate primary Union law or international human rights conventions."[43]

In any case, the inclusion of dual nationals in the database may not prevent them from "hiding" behind one of their nationalities, as feared by the Council and Commission. Thus, an "access facility" has been set up.[44] This means that national authorities, Europol, Eurojust and the European Public Prosecutor's Office will be able to "query the ECRIS-TCN system to verify whether, in respect of a person having the nationality of a Member State, any Member State holds criminal record information concerning this person as a third country national" (set out in Article 7(2a)).

The Parliament's hope of preventing the creation of two 'tiers' of EU citizens was thus eliminated in the trilogues, with the only consolation being that dual nationals will not be subject to the same fingerprinting requirements as non-EU nationals. The question remains, however: which people are most likely to be checked via the "access facility"? A cynic might suggest that it is probably non-white EU citizens who will be most likely to be suspected of also holding the nationality of another country. There are no provisions in the agreed text of the Regulation to ensure that queries through the "access facility" are based on factual indications, rather than mere suspicion or prejudice.

The whole topic is to be assessed by the Commission in the future. According to Article 34 of the agreed text, the Commission's first overall evaluation of the system must assess "the appropriateness of the biometric data used"; an assessment of "the insertion of fingerprints in the ECRIS-TCN system, in particular the application of the minimum criteria as referred to in Article 5(1)(b)(ii); and:

> *"the extent to which, on the basis of relevant statistical data and further information from the Member States, the inclusion in the ECRIS-TCN system of identity information on citizens of the Union who also hold the nationality of a third country has contributed to the achievement of the objectives of the Regulation."*

This assessment "may be accompanied, if necessary, by legislative proposals."

---

under the ECRIS system established by Framework Decision 2009/315/JHA." See: Council document 11310/18, http://statewatch.org/news/2019/feb/eu-council-ecris-tcn-dual-nationals-fingerprints-ep-11310-18.pdf

[43] Inclusion of dual nationals in new criminal records database "incompatible" with the right to non-discrimination, *Statewatch News Online*, 28 January 2019, http://www.statewatch.org/news/2019/jan/ecris-tcn-meijers.htm

[44] The term "access facility" does not appear in the text but is used to describe this process in a number of Council documents discussing the proposed Regulation. See: 11310/18 (link above) and 9750/18, https://data.consilium.europa.eu/doc/document/ST-9750-2018-INIT/en/pdf

6. Conclusion

'Foreign criminals' are not often afforded much sympathy by the press or politicians, but they too have fundamental rights. The way in which the ECRIS-TCN has been established, however, suggests that this is not of great concern to the EU institutions.

While the development of the ECRIS-TCN was perhaps something of an inevitability, it seems that it has been established as a centralised biometric database primarily to satisfy the needs of the EU's interoperability initiative (itself being rushed through the legislative procedure with an alarming lack of scrutiny). A less-intrusive, decentralised option was discarded following technical studies and, crucially, significant political pressure.

The introduction of this centralised system will mean the imposition of an obligation for Member States to fingerprint convicted non-EU nationals, even where there is no such obligation to do so for EU nationals convicted on their territory, and where there is little evidence to suggest that the collection of fingerprints for this purpose is even necessary. The constitutional order of certain Member States is thus being re-arranged to suit the EU's "interoperability" initiative. While non-EU nationals may currently be the primary target of these changes, similar developments can also be seen elsewhere.[45]

The significant difference in treatment between EU nationals, non-EU nationals and dual nationals introduced by the proposals is also clearly discriminatory. The "hit/no-hit" function of the ECRIS-TCN, which will allow officials to see that some conviction-related information on an individual is held by another Member State, may lead to prejudicial attitudes or actions on the part of the authorities. EU citizens are shielded from this possibility through the way the existing ECRIS functions.

At the same time, the need to include dual nationals in the database has not been demonstrated, and their inclusion not only creates two 'tiers' of EU citizen, but may well lead to non-white EU citizens being subject to checks in the ECRIS-TCN through the "access facility" under the assumption that they are more likely to hold dual citizenship.

When announcing new databases or information systems, the Council often likes to note in its press releases that they are being set up with full fundamental rights safeguards in place – something notably absent from its announcement on the ECRIS-TCN.[46] The Austrian minister of justice is no doubt correct when he says that the EU must "ensure that someone cannot just escape their criminal past by moving to another member state." The question remains as to why that could not be done without unnecessarily infringing upon individual rights.

---

[45] For example, in the proposals to make all national identity cards biometric through the inclusion of two fingerprints and a facial image. A key rationale behind this initiative is to make EU citizens more "interoperable" with the mandatory checks against criminal databases that are now required at the borders of the Schengen area for EU citizens and non-citizens alike. See: 'EU plans to include fingerprints in identity cards are unjustified and unnecessary', *Statewatch News Online*, 11 June 2018, http://www.statewatch.org/news/2018/jun/eu-id-cards-pr.htm

[46] https://www.consilium.europa.eu/en/press/press-releases/2018/12/11/exchanging-criminal-records-eu-agrees-a-reformed-ecris-system/

Annex: EU agencies' access to the system

Article 14 of the Regulation sets out the grounds on which Eurojust (the judicial cooperation agency), Europol (the police cooperation agency) and the European Public Prosecutor's Office (EPPO, responsible for investigating fraud against the EU budget) may have access to the ECRIS-TCN.

Article 14(1) says:

> *"Eurojust shall have direct access to the ECRIS-TCN system for the purpose of the implementation of Article 16, as well as for fulfilling its statutory tasks as referred to in Article 3 of Council Decision 2002/187/JHA, as amended, to identify the Member State(s) holding information on previous convictions of third country nationals."*

The Council Decision establishing Eurojust was replaced in November 2018 with a Regulation. Article 2 of that text sets out Eurojust's tasks, and thus the grounds on which it may access the ECRIS-TCN:

> *1. Eurojust shall support and strengthen coordination and cooperation between national investigating and prosecuting authorities in relation to serious crime which Eurojust is competent to deal with in accordance with Article 3(1) and (3), where that crime affects two or more Member States, or requires prosecution on common bases, on the basis of operations conducted and information supplied by the Member States' authorities, by Europol, by the EPPO and by OLAF.*
>
> *2. In carrying out its tasks, Eurojust shall:*
>
> *(a) take into account any request emanating from a competent authority of a Member State, any information provided by Union authorities, institutions, bodies, offices and agencies competent by virtue of provisions adopted within the framework of the Treaties and any information collected by Eurojust itself;*
>
> *(b) facilitate the execution of requests for, and decisions on, judicial cooperation, including requests and decisions based on instruments that give effect to the principle of mutual recognition.*
>
> *3. Eurojust shall carry out its tasks at the request of the competent authorities of the Member States, on its own initiative or at the request of the EPPO within the limits of the EPPO's competence."*

Regarding Europol's access, Article 14(2) of the agreed text on ECRIS-TCN says:

> *"Europol shall have direct access to the ECRIS-TCN system for the purpose of fulfilling its statutory tasks as referred to in Article 4(1)(a), (b), (c), (d), (e) and (h) of Regulation 2016/794 to identify the Member State(s) holding information on previous convictions of third country nationals."*

The relevant provisions of Regulation 2016/794 (the Europol Regulation) say:

"1. Europol shall perform the following tasks in order to achieve the objectives set out in Article 3:

(a) collect, store, process, analyse and exchange information, including criminal intelligence;

(b) notify the Member States, via the national units established or designated pursuant to Article 7(2), without delay of any information and connections between criminal offences concerning them;

(c) coordinate, organise and implement investigative and operational actions to support and strengthen actions by the competent authorities of the Member States, that are carried out:

(i) jointly with the competent authorities of the Member States; or

(ii) in the context of joint investigation teams in accordance with Article 5 and, where appropriate, in liaison with Eurojust;

(d) participate in joint investigation teams, as well as propose that they be set up in accordance with Article 5;

(e) provide information and analytical support to Member States in connection with major international events;

(h) support Member States' cross-border information exchange activities, operations and investigations, as well as joint investigation teams, including by providing operational, technical and financial support;"

Regarding the EPPO, Article 14(2a) of the agreed text of the ECRIS-TCN Regulation says:

"The European Public Prosecutor's Office shall have direct access to the ECRIS-TCN system for the purpose of fulfilling its statutory tasks as referred to in Article 4 of Regulation (EU) 2017/1939 to identify the Member State(s) holding information on previous convictions of third country nationals."

Article 4 of Regulation 2017/1939 (the EPPO Regulation) says:

"The EPPO shall be responsible for investigating, prosecuting and bringing to judgment the perpetrators of, and accomplices to, criminal offences affecting the financial interests of the Union which are provided for in Directive (EU) 2017/1371 and determined by this Regulation. In that respect the EPPO shall undertake investigations, and carry out acts of prosecution and exercise the functions of prosecutor in the competent courts of the Member States, until the case has been finally disposed of."

Statewatch is a non-profit-making voluntary group founded in 1991. It is comprised of lawyers, academics, journalists, researchers and community activists. Its European network of contributors is drawn from 18 countries. Statewatch encourages the publication of investigative journalism and critical research in Europe the fields of the state, justice and home affairs, civil liberties, accountability and openness.

One of Statewatch's primary purposes is to provide a service for civil society to encourage informed discussion and debate - through the provision of news, features and analyses backed up by full-text documentation so that people can access for themselves primary sources and come to their own conclusions.

Statewatch is the research and education arm of a UK registered charity and is funded by grant-making trusts and donations from individuals.

Web: www.statewatch.org | Email: office@statewatch.org | Phone: (00 44) 203 691 5227

Post: c/o MDR, 88 Fleet Street, London EC4Y 1DH

Charity number: 1154784 | Company number: 08480724
Registered office: 2-6 Cannon Street, London, EC4M 6YH