FRA Opinion – 1/2015
[ECRIS]

Vienna, 4 December 2015

Opinion of the European Union Agency for Fundamental Rights concerning the exchange of information on third-country nationals under a possible future system complementing the European Criminal Records Information System

THE EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA),

Bearing in mind the Treaty on European Union (TEU), in particular Article 6 thereof,

Recalling the obligations set out in the Charter of Fundamental Rights of the European Union (the Charter),

In accordance with Council Regulation 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights (FRA), in particular Article 2 with the objective of FRA "*to provide the relevant institutions, bodies, offices and agencies of the Community and its EU Member States when implementing Community law with assistance and expertise relating to fundamental rights in order to support them when they take measures or formulate courses of action within their respective spheres of competence to fully respect fundamental rights*",

Having regard to Article 4 (1) (d) of Council Regulation 168/2007, with the task of FRA to "*formulate and publish conclusions and opinions on specific thematic topics, for the Union institutions and the EU Member States when implementing Community law, either on its own initiative or at the request of the European Parliament, the Council or the Commission*",

Having regard to Recital 13 of Council Regulation 168/2007, according to which "*the institutions should be able to request opinions on their legislative proposals or positions taken in the course of legislative procedures as far as their compatibility with fundamental rights are concerned*",

Having regard to previous opinions of FRA on related issues; in particular: on the proposed Data protection reform package,[1] on the draft Directive regarding the European Investigation Order,[2] and on the proposal to establish a European Public Prosecutor's Office.[3]

Having regard to the request of the European Commission of 6 November 2015 to FRA for an opinion on fundamental rights aspects of a possible legislative instrument supplementing the existing European Criminal Records Information System as regards information on third-country nationals convicted in the European Union,

Emphasising that in the absence of a draft legislative text and a clear scope of the possible instrument, it is only possible to offer preliminary observations as regards its potential fundamental rights implications, and underlining its readiness to provide more specific input once a draft legislative text is available.

SUBMITS THE FOLLOWING OPINION:

---

1 FRA (2012), *Opinion on the proposed data protection reform package,* 1 October 2012, available at: http://fra.europa.eu/en/opinion/2012/fra-opinion-proposed-eu-data-protection-reform-package.

2 FRA (2011), *Opinion on the draft Directive regarding the European Investigation Order,* 14 February 2011, available at: http://fra.europa.eu/en/opinion/2011/fra-opinion-draft-directive-regarding-european-investigation-order-eio.

3 FRA (2014), Opinion on a proposal to establish a European Public Prosecutor's Office, 4 February 2014, available at: http://fra.europa.eu/en/opinion/2014/fra-opinion-proposal-establish-european-public-prosecutors-office.

Opinions

Treating comparable situations equally

The general principle of equality allows for limitations to equal treatment as set out in Article 20 of the Charter to the extent that these limitations respect the essence of the right and are objectively justified. The necessity and proportionality of treating third-country nationals differently than EU nationals would need to be thoroughly assessed in light of the objective of the possible future system complementing the European Criminal Records Information System in relation to third-country nationals (ECRIS-TCN). As illustrated in the following opinions, introducing a third-country national specific system without taking into account relevant third-country national specific factors raises a number of issues.

Avoiding use of ECRIS-TCN for immigration law enforcement

To avoid the risk that ECRIS-TCN is used to withdraw or to refuse the issuance or extension of a residence permit, the EU legislator would need to clearly define the system's purpose in a manner that limits EU Member States' discretion. An express prohibition to use ECRIS-TCN for immigration law enforcement purposes outside of criminal proceedings should be examined.

Preventing disproportionate consequences of migration-related offences

To prevent unjustified adverse effects against third-country nationals, including possible secondary effects of convictions that are questionable from a refugee law point of view, convictions relating to irregular entry and stay should not be processed under ECRIS-TCN for purposes other than criminal proceedings. This would also avoid additional integration challenges for people granted international protection.

Addressing the risks of data transfers to third countries

Safeguards need to sufficiently address possible fundamental rights consequences of sharing information generated by an EU Member State with third countries. The right to the protection of personal data set out in Article 8 of the Charter must fully apply, and harmonised rules for data transfers regarding third-country nationals should be set. Clear limits need to be established to prevent a transfer of information where there is a serious risk that such transfer may result in violation of other fundamental rights. This is particularly important when information relates to persons in need of international protection.

Reducing interference with the right to the protection of personal data by setting up a decentralised index

Basing ECRIS-TCN on a decentralised system connecting indexes set up by each EU Member State accompanied by adequate anonymisation techniques would entail less interference with the right to privacy in comparison to an index centrally established at EU level. Risks of interference with the right to privacy would be further reduced by setting up a mechanism facilitating the correction of inaccuracies, and by effective cooperation between EU Member States and data protection authorities.

Assessing the use of fingerprints compared with other less intrusive means

Arguments for the use of fingerprints are not exclusive to third-country nationals. To assess the necessity and proportionality of using fingerprints for the index, the alternatives of using passports and/or residence permits, as well as the possibilities offered by already existing EU and national databases, need to be taken into account. These need to be considered in comparison to the inclusion of fingerprints of all or certain categories of third-country nationals.

Anonymising the ECRIS-TCN index without increasing the risk of false matches

If fingerprints are used, only templates should be stored. Strong anonymisation techniques should be applied without increasing the risk of false matches. Should this not be possible, the suitability of using fingerprints must be re-assessed.

Considering alternatives for *bona fide* requests for information on own criminal record

The use of ECRIS beyond criminal proceedings and protection of children from the risk of abuse is not the primary objective of the system. This should be taken into account when assessing the proportionality of limitations to the right to privacy and the justification for differentiated treatment of third-country nationals through the potential new ECRIS-TCN index. If fingerprints are included in the future ECRIS-TCN, consideration should be given to keeping the possibility for third-country nationals to request and receive criminal record certificates using the current ECRIS system, particularly in case of* bona fide *persons seeking employment where there are no doubts about their previous stay in other EU Member States.

Ensuring that ECRIS-TCN allows for effective vetting procedures

ECRIS-TCN should make it possible for employers to verify in an effective manner the existence of any disqualification from exercising activities involving direct and regular contacts with children arising from past criminal convictions.

Reviewing carefully the impact on children

In addition to criminal law implications of irregular entry and stay, third-country national children may also be exposed to forms of exploitation – for example by traffickers – which may lead to the involvement of children in criminalised activities. The creation of an index system would amplify the likelihood that such past criminal activities are uncovered and lead to a disproportionate effect on children. In light of the vulnerability of children, consideration should be given to either excluding children from the scope of ECRIS altogether or from the index, or to limiting exchanges to very serious crimes committed by children.

Facilitating the exercise of the rights of data subjects

An effective right to access data and have it rectified, and the right to information for third-country nationals should be ensured in ECRIS-TCN. This needs to take into account issues such as the absence of an EU Member State of nationality, possible language barriers and, if fingerprints are involved, potential errors in the utilised technology.

Ensuring remedies are effective also for third-country nationals

Since inaccurate criminal records may be more common in cases involving third-country nationals, safeguards would need to be built into ECRIS-TCN to ensure that only accurate data are exchanged and used, particularly for records pre-dating the establishment of the system.

Particularly challenging situations include those where convictions have been issued after* in absentia *proceedings, and where ECRIS-TCN information is used for other purposes than criminal proceedings. In relation to such contexts, there is a need to assess how safeguards can be put in place to ensure that remedies – including the availability of legal aid, and interpretation and translation – are effective also for third-country nationals.

Fundamental rights assessment as part of regular review

The fundamental rights implications of ECRIS-TCN cannot be fully anticipated and need to be assessed as part of a regular review of the system. Such an assessment needs to cover the compliance with and impact on fundamental rights, evaluating the effect of ECRIS-TCN on the fundamental rights of third-country nationals in comparison with the effect of ECRIS on the fundamental rights of EU nationals. Based on such an assessment, proposals for the revision of the system could be presented.

Introduction

FRA received a request from the European Commission on 6 November 2015 to deliver an opinion on the fundamental rights aspects of "*a possible legislative instrument supplementing the existing European Criminal Records Information System as regards information on third-country nationals convicted in the European Union*". FRA understands that the request aims to support the preparation of an impact assessment of the envisaged legislative instrument. This opinion reflects FRA's preliminary observations compiled in absence of a draft legislative text. They are, therefore, of a general nature and aim to flag issues that should be considered during the impact assessment phase. FRA remains ready to provide more specific input to the draft text at a later stage in the legislative process.

The European Criminal Records Information System (ECRIS), based on Framework Decision 2009/315/JHA (ECRIS Framework Decision)[4] and Decision 2009/316 (ECRIS Decision)[5], in force since April 2012, allows for an exchange of information on criminal records between European Union (EU) Member States. The two instruments oblige an EU Member State that hands down a conviction against a national of another EU Member State to notify the EU Member State of nationality of the convicted person'. The EU Member State of nationality then acts as a repository of information on all convictions passed in relation to its nationals in the EU and has the obligation to provide up-to-date information on its nationals' criminal records on request of another EU Member State, in a standardised format. Fingerprints of the convicted persons, if available, can be provided as part of the process.

Information on criminal records is used for different purposes. First, EU Member States can request it for consideration in their own criminal proceedings against a person to adapt the decision to be taken to the individual situation. This could be for the purpose of deciding on an appropriate sentence in light of, in particular, prevention of new crimes and recidivism. Second, criminal records can be requested for any other purpose permitted by the national law of the requesting EU Member State, although the requested EU Member State has the option to refuse such a request based on its national law. Such other purposes can cover administrative procedures, for example the issuance of a firearm licence or appointing a guardian for a child. Finally, information on criminal records is needed during vetting procedures for specific jobs, including in particular those which entail working with children.

According to Council of Europe standards and as explicit in Recital 15 of the ECRIS Framework Decision, use of information on criminal records outside criminal proceedings must be as limited as possible not to compromise the chances of social rehabilitation of the convicted person.[6]

---

4 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, OJ 2009 L 93, pp. 23-32.

5 Council Decision 2009/316/JHA of 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, OJ 2009 L 93, pp. 33-48.

6 This is underscored in the Council of Europe (1984), Committee of Ministers, *Recommendation on the Criminal Record and Rehabilitation of Convicted Persons*, No. R(84)10, 21 June 1984, fourth preambular recital, available at: https://wcd.coe.int/ViewDoc.jsp?id=693339&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383. See also Council Framework Decision 2008/675/JHA on taking account of convictions in the Member States of the European Union in the course of new criminal proceedings of 24 July 2008 referenced in Recital 11 of Framework Decision 2009/315/JHA and the Report from the Commission to the European Parliament and the Council on the implementation by the Member States of the Framework Decision 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 COM (2014) 312 final.

ECRIS allows for requesting information on criminal records, by means of the same procedure as for EU nationals, also in relation to third-country nationals. According to the European Commission, however, ECRIS is not an effective tool to exchange information on prior convictions of third-country nationals in another EU Member State. This is due to the fact that, in the absence of an EU Member State of nationality, criminal records of third-country nationals are not stored by a single 'repository' EU Member State in the same way as for own nationals. As a result, unless there is convincing evidence of the individual's previous stay in other EU Member States, 'blanket' requests for information have to be sent to all other EU Member States, which leads to considerable administrative burden. Furthermore, the European Commission notes that unambiguous identification of third-country nationals can be difficult or impossible because of lack of reliable identity documents, different alphabets or very common foreign names. EU Member States therefore view ECRIS as less reliable in respect to third-country nationals, and thus tend to use it less often than for EU nationals.

For this reason, the European Commission seeks an appropriate solution for a more efficient exchange of information related to convicted third-country nationals. The intention to improve the functioning of ECRIS *vis-à-vis* third-country nationals was highlighted in the Commission's Communication on the *European Agenda on Security*[7] and endorsed by the Council of the EU.[8]

The plan is to establish a system that would allow to search in an index of identity information on third-country nationals through a 'hit/no-hit' function. A hit (information that a match has been found) would provide an indication that the person has already been convicted in another EU Member State. In such case, a regular request for information on the person's convictions based on the current ECRIS system could be submitted to the EU Member State where the match was found. The European Commission considers the following options:

- decentralised hit/no-hit anonymised/coded index system where EU Member States would be obliged to store information in their national databases, or
- centralised hit/no-hit index system with an obligation of EU Member States to store information in a central database, possibly operated by an existing EU agency or the European Commission itself.

The index could be based on alphanumeric identifiers (for example name and surname, previous names and aliases, date and place of birth, number of identification/travel document) and/or fingerprints. In this case, the question is whether it would be proportionate to introduce an obligation of processing fingerprints as biometric identifiers given their sensitive nature and the fact that for EU nationals the use of fingerprints remains discretionary for EU Member States.

This opinion assesses the interference with fundamental rights which may result from the eventual future instrument, bearing in mind that, with certain exceptions, the fundamental rights are not absolute. They may be restricted, provided that the restrictions genuinely correspond to an objective of general interest and do not go beyond what is strictly

[7] European Commission (2015), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. The European Agenda on Security,* COM (2015) 185 final, Strasbourg, 28 April 2015, p. 7, available at: http://data.consilium.europa.eu/doc/document/ST-8293-2015-INIT/en/pdf.

[8] See, for instance, Conclusions of the Council of the EU and of the Member States meeting within the Council on Counter-Terrorism, Brussels, 14406/15, 20 November 2015, p. 7, available at: http://data.consilium.europa.eu/doc/document/ST-14406-2015-INIT/en/pdf.

necessary to achieve this objective and do not interfere with the essence of these rights.[9] FRA acknowledges the possible positive effects of such an instrument on third-country nationals as regards the legal certainty provided to persons with a clean criminal record and the important role it can play in protecting people from becoming victims of crime, particularly in protecting children from abuse. More generally, such a system can have positive effects from an overall justice perspective by contributing to appropriate sentencing which again might facilitate social rehabilitation.

At the same time, however, despite being a neutral tool that does not aim to extend the purpose of the current system, the possible future system complementing the European Criminal Records Information System in relation to third-country nationals, 'ECRIS-TCN', entails a risk of considerable adverse impacts on the fundamental rights of third-country nationals which should be mitigated; these include:

- the principle of equality before the law (Article 20 of the Charter);
- the protection of the rights of the child (Article 24 of the Charter);
- the right to an effective remedy (Article 47 of the Charter);
- the right to respect for private and family life (Article 7 of the Charter);
- the right to the protection of personal data (Article 8 of the Charter).

The right to protection of personal data is enshrined in Article 8 of the Charter and Article 16 of the Treaty on the Functioning of the European Union (TFEU). A violation of the right to the protection of personal data may occur not only when specific data protection related principles and rules – for example the purpose limitation principle or the data security rules – are not respected, but also when other laws and fundamental rights are affected by the data processing.[10]

Without being exhaustive, this opinion discusses selected topics in light of the aforementioned fundamental rights at stake. In addition to a legal assessment based on fundamental rights standards, the opinion highlights potential practical effects of the envisaged system that should be taken into consideration when drafting the legislative proposal.

[9] CJEU, Joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Hessen*, paras. 48, 67, 72 and 74; CJEU, C-291/12, *M. Schwarz v. Stadt Bochum*, paras. 39-40.

[10] CJEU, C-524/06, *Huber v. Germany*, 16 December 2008; Article 29 Working Party, Opinion 3/2013 on purpose limitation, p. 20.

1. Safeguards to address the specific situation of third-country nationals

Treating comparable situations equally

The general principle of equal treatment in Article 20 of the Charter requires that "*comparable situations not be treated differently and different situations not be treated alike unless such treatment is objectively justified*".[11] Introducing certain differences into the existing ECRIS mechanism, such as the establishment of an index or systematic processing of fingerprinting solely on the basis of whether the individual is an EU or third-country national, requires objective justification as per Article 52 (1) of the Charter and needs to be based on a comprehensive evaluation of the current system.[12]

Furthermore, building a different system for third-country nationals compared to the one in place for EU nationals may lead to a situation where crime statistics portray a disproportionate number of third-country nationals as convicted offenders, particularly when offence categories incorporate irregular entry into EU territory, as described below. This could result in stigmatisation of third-country nationals.

Besides compromising the principle of formal equality, ECRIS-TCN could exacerbate some of the potential effects of the current ECRIS system linked to the specific situation of third-country nationals, which would justify the inclusion of tailored safeguards so that also substantive equality is ensured. These specific issues are further elaborated in the following sections.

FRA opinion

The general principle of equality allows for limitations to equal treatment as set out in Article 20 of the Charter to the extent that these limitations respect the essence of the right and are objectively justified. The necessity and proportionality of treating third-country nationals differently than EU nationals would need to be thoroughly assessed in light of the objective of the possible future system complementing the European Criminal Records Information System in relation to third-country nationals (ECRIS-TCN). As illustrated in the following opinions, introducing a third-country national specific system without taking into account relevant third-country national specific factors raises a number of issues.

Avoiding use of ECRIS-TCN for immigration law enforcement

Although ECRIS-TCN is intended to be a neutral tool, it will have certain adverse consequences for third-country nationals which are either irrelevant or less adverse for EU nationals. The purpose of ECRIS is to consider past convictions in the course of new criminal proceedings and to ensure the application of possible disqualifications arising from a conviction for certain crimes related "*to perform[ing] professional activity related to supervision of children*" in other Member States.[13] Article 7 (2) of the ECRIS Framework Decision, however, also provides for the use of ECRIS for "*purposes other than of criminal proceedings.*" The provision leaves it up to Member States' national legislation to define these purposes. Based on national legislation for regulating the use of information on

[11] CJEU, C-203/86, *Kingdom of Spain* v. *Council of the European Union*, para. 25, and C-15/95, *EARL de Kerlast v. Union régionale de coopératives agricoles (Unicopa) and Coopérative du Trieux,* para. 35.

[12] In this regard, findings collected in preparation of the implementation report pursuant to Article 13 (3) of the ECRIS Framework Decision should be taken into account.

[13] ECRIS Framework Decision, recitals (11), (12).

criminal records, this can include data transfers to administrative authorities or private parties. Not providing for objective criteria in implementing the purpose limitation principle (clearly specifying the purpose in advance), undermines legal clarity and data protection safeguards and creates the risk that ECRIS-TCN is used for purposes that are incompatible with the rationale for which it was established.[14]

While this issue concerns all persons whose information is exchanged under ECRIS, it can have particularly serious implications in the case of third-country nationals. If ECRIS-TCN is accessible to immigration police or authorities in charge of issuing or renewing residence permits, it may in practice turn into an immigration policy tool. Evidence of past criminal offences may, depending on national legislation, be a ground for withdrawing or for not issuing or extending a residence permit. A well-functioning ECRIS-TCN could enable – and possibly motivate – immigration authorities to consult the system either on a systematic or targeted basis to determine if a person has previously been convicted in the EU.

Currently, third-country nationals who have committed a crime are entered into SIS II if the conviction is combined with an expulsion order and an entry ban. A planned change of the SIS II Regulation will make it mandatory for EU Member States to record entry bans and return decisions in SIS II.[15] If ECRIS-TCN is used systematically for immigration law enforcement purposes, it would extend substantially the *de facto* effects of a criminal conviction. A hit in ECRIS-TCN and not only a hit in SIS II could be used to end a right of residence and initiate a return decision. Such use of ECRIS-TCN would represent a substantial departure from the primary purpose of ECRIS from judicial cooperation in criminal matters to measures in the fields of return and combating irregular migration. This 'function-creep' should be avoided because of its unforeseeable effect on fundamental rights but also the issue of legal basis.[16] It may also entail less direct fundamental rights implications. For instance, the withdrawal of a residence permit may impact on the right to respect for family life under Article 7 of the Charter. The issue of legal clarity and a clearly defined purpose may be addressed in general on the occasion of ECRIS-TCN while explicitly excluding the use of ECRIS-TCN for immigration law enforcement purposes.

FRA opinion

To avoid the risk that ECRIS-TCN is used to withdraw or to refuse the issuance or extension of a residence permit, the EU legislator would need to clearly define the system's purpose in a manner that limits EU Member States' discretion. An express prohibition to use ECRIS-TCN for immigration law enforcement purposes outside of criminal proceedings should be examined.

---

[14] Similarly the CJEU held in Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd. and Seitlinger and Others*, 8 April 2014, para. 60, 62, 65 that the failure to lay down any objective criterion to determine the limits of access to data by competent national authorities constitutes a serious interference with the fundamental rights at issue.

[15] Council of the European Union, Draft Council Conclusions on the Insertion of Alerts in the SIS pursuant to Article 24 of the SIS II Regulation upon a Return Decision (11648/15), 8 September 2015.

[16] A major change in the practical use of the system would raise the question of appropriate legal basis, as measures taken by the EU in the fields of return and combating irregular migration would need to be based on Article 79 of the TFEU and not on its provisions on judicial cooperation in criminal matters. Incompatibility between the scope of application of an instrument and its legal basis can have adverse effects on fundamental rights, including the right to protection of personal data. In this respect, see CJEU ruling in Joined cases C-317/04 and C-318/04, 30 May 2006, in which the Court annulled the Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection.

Preventing disproportionate consequences of migration-related offences

There are crimes that are specific to third-country nationals, such as irregular entry or stay, or travelling with false visas or travel documents. The design of ECRIS-TCN should not result in disproportionate impact on the rights of third-country nationals convicted for such offences.

The impact of sanctions which may be questionable from a refugee law point of view needs to be considered. As stated in a FRA Focus paper of early 2015, the possibilities for people in need of international protection to legally enter and stay in an EU Member State are limited.[17] For this reason, many of these persons resort to smuggling networks to reach safety or join their families. They cross the external borders of the EU outside official border crossing points or using forged or counterfeit travel documents.

Article 18 of the Charter and Article 78 of the TFEU,[18] require EU asylum law to comply with the provisions of the 1951 Convention Relating to the Status of Refugees (Refugee Convention). All EU Member States are party to the convention. Article 31 of the Refugee Convention prohibits the penalisation of refugees for irregular entry or stay, provided certain conditions are fulfilled – for example, that refugees present themselves to the authorities without delay. According to the Executive Committee of the High Commissioner's Programme (ExCom) of the United Nations High Commissioner for Refugees (UNHCR), the non-penalisation provision of the Refugee Convention extends also to the use of fraudulent documentation which may be necessary for the refugee to leave the country in which their physical safety or freedom are endangered.[19] This can be linked to various circumstances ranging from the need to use a false document to pass an exit check to the physical inability to obtain the documents necessary for legal entry (such as a passport and visa) when fleeing from a conflict zone. A range of other crimes related to irregular entry or stay – including for example, the new crime of unauthorised border fence crossing introduced by Hungary in September 2015[20] – are also clearly covered.

Criminal law policies to address irregular entry or stay diverge substantially among the EU Member States, and a conviction handed out in an EU Member State may be questionable from a refugee law point of view. Through ECRIS-TCN, the information on such convictions would become easily available to all other EU Member States. If persons in need of international protection are sentenced for such crimes and their convictions entered into

---

17 FRA (2015), *Legal entry channels to the EU for persons in need of international protection: a toolbox - FRA focus*, March 2015, p. 2, available at: http://fra.europa.eu/sites/default/files/fra-focus_02-2015_legal-entry-to-the-eu.pdf.

18 In this context see also Recital 15 of the Reception Conditions Directive, Directive 2013/33/EU of the European Parliament and of the Council of 26 June 2013 laying down standards for the reception of applicants for international protection, OJ L 180/96, 29 June 2013.

19 UNHCR (1989), *Problem of Refugees and Asylum-Seekers Who Move in an Irregular Manner from a Country in Which They Had Already Found Protection*, EXCOM Conclusions, No. 58 (XL) – 1989, 13 October 1989, para. i), available at: www.unhcr.org/3ae68c4380.html. Arguments for the necessity to resort to fraudulent documents in certain situations have been further developed by national courts of some EU Member States, including the clarification that this waiver of criminalisation should extend to all persons claiming asylum in good faith (presumptive refugees), not just those ultimately accorded refugee status. See for example *R v. Uxbridge Magistrates Court and Another, Ex parte Adimi*, [1999] EWHC Admin 765; [2001] Q.B. 667, United Kingdom: High Court (England and Wales), 29 July 1999, paras 15-16, available at: www.refworld.org/docid/3ae6b6b41c.html, or *X (Somalia)*, 12/01278, Netherlands, The Supreme Court (*Hoge Raad*), 3 December 2013, para. 2.6.2., available in Dutch at: http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2013:1561&keyword=vluchtelingenverdrag.

20 Hungary, Article 352/A of Act C of 2012 on the Criminal Code (*2012. évi C. törvény a Büntető Törvénykönyvről;* Criminal Code), njt.hu/cgi_bin/njt_doc.cgi?docid=152383.297990#foot_121_place.

criminal records available across the EU, this may lead to further negative consequences such as being barred from certain jobs that require a clean criminal record. These consequences are reinforced since people in need of international protection often settle in countries other than the EU Member State of first entry. A conviction related to irregular stay or entry will make integration of people granted international protection more difficult. It may also undermine the aim of facilitating the integration of people granted international protection, as reflected in the Qualification Directive.[21]

Looking specifically at irregular entry and stay, such behaviour infringes immigration laws in all EU Member States and triggers a return procedure. In some – but not all – EU Member States, these acts also constitute offences that are separately punishable with imprisonment and/or a fine. As of 1 January 2014, 17 EU Member States provided for the possibility of custodial sentences for irregular entry and 10 EU Member States had this option for irregular stay. For irregular entry, the maximum length of imprisonment ranged from one month in Croatia to three months in Belgium and five years in Bulgaria. For irregular stay, it ranged from 60 days in Croatia to three years in Cyprus. In other EU Member States these acts only constitute administrative offences.[22]

EU law poses some limitations to Member States' criminal law responses. Referring to the duty of loyal cooperation under Article 4 (3) of TEU, the Court of Justice of the European Union (CJEU) concluded that "*a Member State may not apply criminal law rules which are liable to undermine the application of the common standards and procedures established by Directive 2008/115/EC [the Return Directive] and thus to deprive it of its effectiveness*".[23] Imprisonment of a migrant in an irregular situation for the offence of having unlawfully entered or stayed in the territory of an EU Member State must not, therefore, take precedence over the application of the Return Directive, including its fundamental rights safeguards. In *Achoughbabian*, the CJEU said that imprisonment for the offence of irregular stay, before carrying out the removal, unnecessarily delays the removal process, even when imprisonment is rarely imposed in practice.[24] It is, therefore, not allowed under EU law to apply a custodial penalty to a migrant in an irregular situation for irregular entry or stay, before a return decision is adopted and while it is implemented.[25]

In spite of CJEU case law, as shown in a 2014 FRA report, in a number of EU Member States it is still possible under national law to apply custodial sentences to persons subject to return procedures.[26] If such convictions are entered into national criminal records, other EU Member States may take decisions based on previous criminal records relating to situations that, according to the CJEU, need to be addressed by using pre-removal detention and not custodial sentences under criminal law. In this sense, the use of envisaged ECRIS-TCN could

---

21 Directive 2011/95/EU of the European Parliament and of the Council of 13 December 2011 on standards for the qualification of third-country nationals or stateless persons as beneficiaries of international protection, for a uniform status for refugees or for persons eligible for subsidiary protection, and for the content of the protection granted, OJ 2011 L 337, pp. 9-26, Article 34 read in conjunction with Recital 41.

22 See FRA (2014), *Criminalisation of migrants in an irregular situation and of persons engaging with them,* Annex (EU Member States' legislation on irregular entry and stay, as well as facilitation of irregular entry and stay), Luxembourg, Publications Office.

23 CJEU, C-61/11, *El Dridi, alias Soufi Karim*, 28 April 2011, paras. 55–59; CJEU, C-329/11, *Achoughbabian v. Préfet du Val-de-Marne*, 6 December 2011, paras. 39 and 43; CJEU, C-430/11, *Criminal proceedings against Md Sagor*, 6 December 2012 (concerning the imposition of a fine), para. 32.

24 CJEU, C-329/11 *Achoughbabian v. Préfet du Val-de-Marne*, 6 December 2011, para. 40.

25 *Ibid.*, para. 45. The CJEU did not, however, exclude the possibility that EU Member States impose a fine for irregular entry or stay, see CJEU, Case C-430/11, *Criminal proceedings against Md Sagor*, 6 December 2012, para. 50.

26 FRA (2014), *Criminalisation of migrants in an irregular situation and of persons engaging with them*, Luxembourg, Publications Office, p. 4 (information as of February 2014).

risk leading to a spill-over effect across borders of convictions that raise questions under EU law, unless the envisaged measure contains safeguards in this regard.

More generally, the divergent approach used by EU Member States to deal with irregular entry and stay may lead – if information on past convictions is easily accessible through ECRIS-TCN to all EU Member States – to inequality in impact on people who are convicted in one EU Member State and live in another. For example, a third-country national who is convicted of irregular entry or irregular stay in Member State A and applies for a job for which a clean criminal record is required in Member State B would be treated less favourably compared with other third-country nationals who also entered irregularly or stayed irregularly in an EU Member State which does not punish irregular entry/stay. The same act would thus result in different consequences in Member State B, depending on the EU Member State in which the act was committed. As mentioned above, these may also pose severe challenges to the integration of the third-country nationals in question.

FRA opinion

To prevent unjustified adverse effects against third-country nationals, including possible secondary effects of convictions that are questionable from a refugee law point of view, convictions relating to irregular entry and stay should not be processed under ECRIS-TCN for purposes other than criminal proceedings. This would also avoid additional integration challenges for people granted international protection.

Addressing the risks of data transfers to third countries

A third country may request an EU Member State to share information on previous convictions of one of its nationals in the EU – for example for extradition purposes or in the context of a criminal proceeding against the individual concerned in the third country. Information on past criminal convictions is of a sensitive nature and has to be handled with utmost care, especially when these are shared with third countries who are not bound by the data protection rules applicable to EU Member States.

Data transfers to third countries are regulated by Article 7 (3) and (4) and Article 9 (4) of the ECRIS Framework Decision as *lex specialis*, and Articles 13 and 14 of the Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters as *lex generalis*.

Framework Decision 2008/977/JHA applies to the data which an EU Member State has received from another EU Member State. Therefore, safeguards contained therein primarily apply to information on criminal records received from another EU Member State.

Transfers of data originating from an EU Member State, including criminal convictions, to a third country are essentially regulated by the national law of this EU Member State. The current data protection regime governing data transfers to third countries in the area of police and judicial cooperation in criminal matters is to a great extent dependent on Member States' national law, despite the harmonisation achieved by the Council of Europe's Data Protection Convention (Convention 108) and its Additional Protocol.[27] More harmonisation

[27] Council of Europe, Convention for the protection of individuals with regard to automatic processing of personal data, CETS No. 108, 1981; Additional Protocol No. 181 to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows.

is expected by the forthcoming EU data protection reform package which, however, will provide effects only in two years after entering into force.[28]

Rules on the transfer of data to third countries should reflect the EU data protection *acquis*, in particular Article 8 of the Charter which applies to all persons irrespective of their nationality. Based on Article 8, transfers of data originating from an EU Member State need to comply with the requirement for an adequate level of protection in that third country or be accompanied by appropriate safeguards.[29]

In addition, the transfers of personal data must not prejudice the rights of refugees and persons requesting international protection and, more generally, the fundamental rights of third-country nationals if there is a serious risk that as a result of such transfer, third-country nationals will be subjected to acts of retaliation (for example against family members or friends) and other violations of their fundamental rights. Article 35 (2) of Regulation 603/2013/EU on Eurodac and Article 31 (3) of Regulation 767/2008/EC on the Visa Information System (VIS) may serve as inspiration. These provide for additional checks with a view to safeguard the rights of refugees and persons requesting international protection and to safeguard certain absolute fundamental rights, for example to prevent the risk of persons being subjected to torture, inhuman or degrading treatment.[30]

FRA opinion

Safeguards need to sufficiently address possible fundamental rights consequences of sharing information generated by an EU Member State with third countries. The right to the protection of personal data set out in Article 8 of the Charter must fully apply, and harmonised rules for data transfers regarding third-country nationals should be set. Clear limits need to be established to prevent a transfer of information where there is a serious risk that such transfer may result in violation of other fundamental rights. This is particularly important when information relates to persons in need of international protection.

[28] Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities of the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and the free movement of such data, COM (2012) 10 final.

[29] See also the recent CJEU judgment in C-362/14, *Maximilian Schrems v. Data Protection Commissioner*, 6 October 2015, para. 73 holding that the protection should be essentially equivalent.

[30] CJEU, C-112/00, *Eugen Schmidberger, Internationale Transporte und Planzüge v. Republik Österreich*, 12 June 2003, para. 80.

2. Fundamental rights considerations linked to the creation of an index and the use of biometric data

Reducing interference with the right to the protection of personal data by setting up a decentralised index

ECRIS-TCN would work on the basis of an index of convicted third-country nationals allowing for automatic searches of people with past criminal records. In case of a match in the index, information on convictions would be exchanged bilaterally between EU Member States. Such an index could either be centrally established at EU level or interconnect decentralised indexes set up by each EU Member State. In case a decentralised system is created, the data will be anonymised or coded, whereas this will not be the case if an index is centrally established at EU level.

In both instances the hit/no hit search method will be used. This search method has clear advantages from a data protection perspective compared with a model providing automatic access to the full set of data contained in the criminal record. Using this method, the requested EU Member State can still control the data to be transmitted.

Regardless of which option is chosen, establishing an index means creating a new database. Even if the data stored therein does not contain the full information, it still creates new risks for the persons included in the database.[31] Therefore, its establishment should be provided for by law, be necessary and proportionate and justified in comparison to EU nationals.[32] The index should serve genuine needs with respect to third-country nationals which cannot be addressed otherwise than in a proportionate manner. The current issues identified by the European Commission with respect to third-country nationals – cumbersome procedures involving sending-out requests for information to all other EU Member States and the difficulties in handling these requests by the recipients – could be used in an evidence-based assessment to justify such an index. The absence of less restrictive available measures needs, nevertheless, to be further demonstrated.

The use of adequate anonymisation techniques in a decentralised index system would provide for enhanced privacy guarantees, taking into account that data on criminal convictions, including information on whether a person is convicted at all, are considered sensitive data in many EU Member States. Such data are identified as a special category under Article 6 of Convention 108. Even if the data in the index are irreversibly transformed into unintelligible digits – so-called hash values – this does not necessarily mean that the data stored are rendered truly anonymous. The hash values of data transmitted and those stored in the index will be compared to generate a hit/no hit result, and the purpose of this operation is to reveal whether the person concerned is included in EU Member States' criminal records.[33] Which technique or combination of various techniques to apply must be subject to further analysis depending also on the nature of the data, for example whether fingerprints or alphanumeric data are used. At any rate, the interoperability of the decentralised national index systems and the accuracy of the results obtained through a hit/no hit functionality must be ensured together with an equal level of data security measures. The EU legislator should therefore include the requirement for anonymisation in the law and should also define common rules for the anonymisation techniques. Moreover,

[31] See Opinion of the European Data Protection Supervisor of 28 February 2006 on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability, COM (2005) 490 final, para. 38.

[32] CJEU, C-524/06, *Huber v. Germany*, 16 December 2008.

[33] See Article 29 Working Party, Opinion 5/2014 on anonymisation techniques.

in case a centralised index is opted for, the reasons for not using anonymisation techniques should be further justified.

The choice for decentralised indexes or a centralised index must comply with the personal data protection principles, in particular with the principles of necessity and proportionality and the principle of data minimisation. The data should be shared only to the extent absolutely necessary for the purpose of cooperation between EU Member States. The data aggregation, which a centralised model entails, implies more risks for the persons included in the database, notably when data are used in a broader context than necessary or for incompatible purposes by third parties. In addition, should fingerprints be included in the system, given their specific nature and the risks associated with data security, 'linkability' and function-creep, the choice of a decentralised index system should be considered in the first place.[34]

In a decentralised index system, each EU Member State's authority appointed to keep the index will remain the data controller for its own data and must ensure data accuracy. As, however, inaccuracies may be identified at a later stage, for example in new court proceedings or in general after the data are transmitted for other purposes, the EU legislator should consider a mechanism for cooperation between EU Member States and timely notification of such inaccuracies to the responsible EU Member State that would allow for corrections. This should entail also cooperation and coordination between data protection authorities, and on the occasion of supplementing the current rules on ECRIS the effective supervision of the system may encompass both ECRIS and ECRIS-TCN.[35]

FRA opinion

Basing ECRIS-TCN on a decentralised system connecting indexes set up by each EU Member State accompanied by adequate anonymisation techniques would entail less interference with the right to privacy in comparison to an index centrally established at EU level. Risks of interference with the right to privacy would be further reduced by setting up a mechanism facilitating the correction of inaccuracies, and by effective cooperation between EU Member States and data protection authorities.

Assessing the use of fingerprints compared with other less intrusive means

The processing of biometric data – in this case fingerprints – brings both opportunities and risks. Using fingerprints as identifiers in ECRIS-TCN is under consideration by the European Commission as a tool to increase the accuracy of matching an individual with a past criminal record. Reducing the matching error rate to a reasonable level is not only a pre-condition for the system to function effectively but also a means to reduce the risk that individuals face hardships due to wrong matches with someone else's criminal record.

[34] Article 29 Working Party, Opinion 3/2012 on developments in biometric technologies, section 4.4.2, according to which linkability occurs when data may be linked with other data from another processing and central storage of fingerprints implies risks associated with data security, linkability and function creep.

[35] The European Data Protection Supervisor emphasised this need with respect to the Framework Decision 2009/315/JHA in the Opinion on the Proposal for a Council Framework Decision on the organisation and content of the exchange of information extracted from criminal records between Member States (COM (2005) 690 final), 20 December 2006, para. 48-49 and in the Opinion on the Proposal for a Council Decision on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA, 20 February 2009, para. 8.

At the same time, biometric data, such as fingerprints, contain information capable of automatically and uniquely identifying a person. Given their specific nature,[36] the processing of fingerprints constitutes in itself an interference with the rights to protection of private life and protection of personal data set forth in Articles 7 and 8 of the Charter and in Article 8 of the European Convention on Human Rights (ECHR).[37] It will, therefore, be necessary to demonstrate that the limitation to such rights is justified, i.e. that the processing of biometric data is necessary for and proportionate to the aim of secure identification of convicted persons. Even if the fingerprints are not further used in the criminal proceedings or for other purposes, their inclusion in such an index reveals at the same time sensitive information about these persons. The processing rules for fingerprints must therefore be subject to stricter data protection requirements regarding data quality and security. To this end, it needs to be clearly demonstrated that the use of less intrusive means – in this case alphanumeric data only – is insufficient and that adequate measures are taken for the processing of fingerprints.

Furthermore, although ECRIS itself is not based on an index system and the exchange of fingerprints is merely one of its discretionary features, arguments raised in favour of using fingerprints as identifiers in ECRIS-TCN are not exclusively applicable to third-country nationals. Some EU Member States, for example, also use different alphabets which can cause complications in matching criminal records due to transliteration.[38] Absence of documents and ensuing difficulties in identifying certain individuals may also occur in the case of EU nationals. For this reason, the necessity of establishing a system for mandatory third-country national fingerprint exchange would not be proven merely by the occasional absence of identification documents, difficulties in reading different alphabets or identifying individuals with very common foreign names.

The use of fingerprints for the index would not be justified if the third-country national passport or residence permit issued by an EU Member State could be used to establish a person's identity. The majority of third-country nationals are living in the EU lawfully and have genuine documents. People who wish to apply for a job working with children or to receive a firearm licence (for example to work for a security company), for instance, usually hold a residence permit and/or a passport issued by the country of origin, as otherwise they would not be allowed to work. According to Regulation (EU) 1030/2002 of 13 June 2002 (as amended by Regulation (EU) 380/2008 of 18 April 2008), residence permits issued by EU Member States to third-country nationals must have a uniform format and standardised security features against forgery, counterfeiting and falsification, including the storing of the facial image and two fingerprints.[39] Similarly, national passports issued by an increasing number of third countries include strong security features against falsification. It would, therefore, be necessary to demonstrate convincingly that the documents held by a third-country national are not sufficient to identify the third-country national.

---

[36] Article 29 Working Party, Opinion 3/2012 on developments in biometric technologies, section 4.4.2, notes that according to some studies fingerprints can reveal ethnical information, thus lead to processing of sensitive data.

[37] ECtHR, *S. and Marper v. United Kingdom* [GC], paras: 68, 84 and 85; CJEU, C-291/12, *M. Schwarz v. Stadt Bochum*, paras. 26–27.

[38] Unisys (2010), Project Final Report "Feasibility Study: Establishment of a European Index of Convicted Third Country Nationals", pp. 25 and 39.

[39] Council Regulation (EC) No. 380/2008 of 18 April 2008 amending Regulation No. 1030/2002 laying down a uniform format for residence permits for third-country nationals, Article 4 (b).

The question of whether the processing of biometric data is proportionate also depends on whether the connection between the individual concerned and a past criminal record can be effectively made by consulting already existing databases. The EU has set up a number of instruments, including the Schengen Information System (SIS II), Eurodac, the Visa Information System (VIS),[40] as well as mechanisms for bilateral exchange of data, such as the Prüm Decisions.[41] In addition, the creation of an entry-exit system is planned which will store biometric data of at least all third-country nationals coming to the EU for a stay not exceeding three months. Most of these systems have been established for other purposes and are not accessible to judicial authorities. Their possible value for identification of third-country nationals and their criminal history would need to be assessed in light of the purpose limitation principle.

SIS II may specifically be accessed by judicial authorities in the context of criminal proceedings.[42] Searchable biometrics will be introduced in SIS II once technically feasible. SIS II includes alerts on various categories of persons, such as persons wanted for arrest and extradition, and individuals who are sought for discreet or specific checks. SIS II would allow for the identification of at least a portion of third-country nationals in the course of criminal proceedings.

Considering the above, the proportionality of processing fingerprints for ECRIS-TCN would be increased if biometrics were only used in absence of reliable alphanumeric data or information from other EU or national databases, where permissible. This could mitigate some of the concerns, particularly where the identity of a person can be established due to the possession of a genuine travel document of reliable quality.

Alternatively, fingerprints could be collected from all convicted persons but two identifiers, for example alphanumeric and fingerprints would be established. The index based on fingerprints would be logically separate from the set of alphanumeric identifiers and could be consulted only in specific circumstances defined by the ECRIS-TCN legal instrument,

---

[40] Regulation (EU) No. 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No. 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No. 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice; Council Decision 2008/633/JHA of 23 June 2008 concerning access for concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences; and Council Decision 2013/392/EU of 22 July 2013 fixing the date of effect of Decision 2008/633/JHA concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences.

[41] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime and Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.

[42] Article 27 (2) of Regulation (EC) No. 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second-generation Schengen Information System (SIS II), and Article 40 (2) of Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), and the List of competent authorities which are authorised to search directly the data contained in the second generation Schengen Information System pursuant to Article 31 (8) of Regulation (EC) No. 1987/2006 of the European Parliament and of the Council and Article 46(8) of Council Decision 2007/533/JHA on the establishment, operation and use of the second generation Schengen Information System.

particularly in cases where the alphanumeric index does not yield an unambiguous result and upon proper justification. Such an option, would, however, raise serious data protection issues, as it would result in aggregation of personal data. From this point of view, this option is unadvisable.

Another option that could be explored in the absence of other less intrusive means would entail setting up a universal threshold for which offences lead to the storing of fingerprints. The threshold could be based on the seriousness of the offence, defined by a closed list of serious offences that would warrant the storing of fingerprints or a more general criterion based on the minimum sentence of deprivation of liberty (as in the case of 'extraditable offences').

FRA opinion

Arguments for the use of fingerprints are not exclusive to third-country nationals. To assess the necessity and proportionality of using fingerprints for the index, the alternatives of using passports and/or residence permits, as well as the possibilities offered by already existing EU and national databases, need to be taken into account. These need to be considered in comparison to the inclusion of fingerprints of all or certain categories of third-country nationals.

Anonymising the ECRIS-TCN index without increasing the risk of false matches

Biometric data is considered highly reliable, and in case of conflicting evidence it is often given priority over other identification data. For that reason, it is particularly important to ensure correctness. A false match would severely affect the liberty and other rights of an individual. The likelihood of a false match thus need to be reduced to the maximum possible extent.

A false match may be the result of the technology used to create the biometric templates. To limit data breaches and other security incidents, biometric features should not be stored without anonymising them. The application of anonymisation techniques, in particular hash functions, may, however, increase the risk of false matches, since non-identical templates linked to the fingerprints of one person would result in two different hash values. If the anonymisation techniques are not adequate, the suitability of using fingerprints is questionable.

FRA opinion

If fingerprints are used, only templates should be stored. Strong anonymisation techniques should be applied without increasing the risk of false matches. Should this not be possible, the suitability of using fingerprints must be re-assessed.

Considering alternatives for *bona fide* requests for information on own criminal record

The usage of ECRIS beyond criminal proceedings and protection of children from the risk of abuse is not the primary objective of the system. In this regard, the ECRIS Framework Decision subscribes to the principle of the Council of Europe Recommendation on the Criminal Record and Rehabilitation of Convicted Persons that *"any other use of criminal records [than in the criminal proceedings for the purpose of determining the appropriate sanction…] should*

be restricted to the utmost".[43] This should be taken into account when determining whether the different treatment of third-country nationals compared to EU nationals by the use of an index, particularly one based on fingerprints, is proportionate.

The disproportion is arguably greatest in case of requests for information by an individual concerning their own criminal records. Reliance on fingerprints as a basis to establish a criminal record certificate would mean the need to undergo a fingerprint scanning procedure every time a third-country national needs to obtain this information, typically for the purpose of applying for a job or obtaining a licence. Given that in some EU Member States, employers tend to commonly require a clean criminal record even without any clear relevance to the job,[44] this could be seen as entailing a disproportionate infringement upon the right to dignity and the right to privacy, as no alternative would exist for *bona fide* third-country nationals who are in possession of valid travel or identity documents.

Furthermore, in many EU Member States certificates on clean criminal records can be obtained at several locations/offices throughout the country. However, if all issuing locations were to operate based on fingerprints and required these from third-country nationals to issue such a certificate – including where requests for criminal record certificates occur only occasionally – this would require appropriate equipment, additional training and adequate data protection measures.

Reducing the overall availability of the service to mitigate data protection risks and facilitate its use could lead to disproportionate difficulties in access. Third-country nationals would always have to travel in person to verify their fingerprints against fingerprints stored through ECRIS-TCN. Factors such as geography or personal mobility linked to age or disability may make the access disproportionately difficult impacting on the rights of the elderly and persons with disabilities set forth in Articles 25 and 26 of the Charter.

FRA opinion

The use of ECRIS beyond criminal proceedings and protection of children from the risk of abuse is not the primary objective of the system. This should be taken into account when assessing the proportionality of limitations to the right to privacy and the justification for differentiated treatment of third-country nationals through the potential new ECRIS-TCN index. If fingerprints are included in the future ECRIS-TCN, consideration should be given to keeping the possibility for third-country nationals to request and receive criminal record certificates using the current ECRIS system, particularly in case of* bona fide *persons seeking employment where there are no doubts about their previous stay in other EU Member States.

[43] Council of Europe (1984), Committee of Ministers, *Recommendation on the Criminal Record and Rehabilitation of Convicted Persons*, No. R(84)10, 21 June 1984, fourth preambular recital, available at: https://wcd.coe.int/ViewDoc.jsp?id=693339&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383.

[44] See, for example, Czech Republic, Public Defender of Rights (*Veřejný ochránce práv*) (2011), Recommendation of the Public Defender on the requirement of a criminal record copy as a determining criterion for employment (*Doporučení ochránce k požadavku výpisu z rejstříku trestů jako určujícímu kritériu pro přijetí do zaměstnání*), Ref. 30/2010/DIS/LO, 22 April 2011, available in Czech at: http://www.ochrance.cz/uploads/tx_odlistdocument/Doporuceni_rejstrik-trestu.pdf.

3. Rights of the child

Ensuring that ECRIS-TCN allows for effective vetting procedures

One of the primary purposes of ECRIS is to protect children from the risk of abuse and exploitation by ensuring that people who work with children undergo proper vetting procedures. The Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) obliges state parties in Article 5 (3) to take measures to ensure that professionals whose work implies regular contact with children *"have not been convicted of acts of sexual exploitation or sexual abuse of children"*. Similar vetting provisions are included in Article 10 of Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography. FRA has stressed the importance of effective vetting procedures in a 2014 handbook published together with the European Commission on *Guardianship for children deprived of parental care*.[45] Without prejudice to other FRA opinions listed here, ECRIS-TCN needs to serve as a reliable source for effective vetting in this respect.

FRA opinion

ECRIS-TCN should make it possible for employers to verify in an effective manner the existence of any disqualification from exercising activities involving direct and regular contacts with children arising from past criminal convictions.

Reviewing carefully the impact on children

The creation of a specific regime for third-country nationals also gives rise to concerns regarding the situation of children. At present, ECRIS does not contain any specific safeguards relating to sharing of information on child convictions with other EU Member States or third countries by those EU Member States that under national law enter such information into their criminal records.

The Council of Europe Recommendation on the Criminal Record and Rehabilitation of Convicted Persons, acknowledged directly in Recital 15 of the ECRIS Framework Decision, emphasises the need *"to restrict to the utmost the communication of decisions relating to minors"*.[46] According to the United Nations (UN) Standard Minimum Rules for the Administration of Juvenile Justice ('The Beijing Rules'), recalled also by the UN Convention on the Rights of the Child, records of juvenile offenders should be kept strictly confidential and closed to third parties, and should not be used in adult proceedings in subsequent cases involving the same offender.[47] Children with a criminal record need to be given a realistic opportunity of rehabilitation and social reintegration. In conformity with these principles, the majority of EU Member States erase the records of previous convictions upon reaching the age of maturity, but in some EU Member States such data are retained. This leads to double standards in the availability of information on criminal records for both EU-national and third-country national children.

---

[45] See Section 2.4 of FRA (2014), *Guardianship for children deprived of parental care: A handbook to reinforce guardianship systems to cater for the specific needs of child victims of trafficking*, June 2014, Luxembourg, Publications Office.

[46] Council of Europe (1984), Committee of Ministers, *Recommendation on the Criminal Record and Rehabilitation of Convicted Persons*, No. R(84)10, 21 June 1984, Section I. (5).

[47] United Nations (1985), *Standard Minimum Rules for the Administration of Juvenile Justice ('The Beijing Rules')*, General Assembly resolution 40/33 of 29 November 1985, Rule 21, available at: http://www.ohchr.org/Documents/ProfessionalInterest/beijingrules.pdf.

Moreover, certain offences may have a disproportionate impact on third-country national children. This is not only the case of offences relating to irregular entry or stay but also to crimes children are compelled to commit as a consequence of being subject to trafficking in human beings. In many cases, children who are exploited by traffickers who force them to engage in criminality or prohibited forms of begging are not identified as victims. Therefore, they are not protected by Article 8 of the Anti-Trafficking Directive (2011/36/EU). A child may in fact have been a subject of exploitation, but he or she is convicted and the offence may be entered in his or her criminal record. The establishment of an index for ECRIS-TCN including children would speed-up the exchange of information on them between EU Member States and possibly to third countries.

The specific risks for children in general, and in particular for third-country national children, need to be considered when scrutinising the necessity and proportionality of the envisaged index. This entails whether children's data should be included in the index at all or at least limited to particular offences only. Eventually, an automatic deletion of children's data in the index when reaching the age of maturity should be envisaged to enhance privacy guarantees and the rights of the child.

In addition, fingerprinting children may lead to a double-interference with the right to the protection of personal data and the rights of the child, given the sensitive nature of fingerprints and the vulnerability of children. This in turn can be exacerbated because of their status as third-country nationals, as described in relation to the potential effects of ECRIS-TCN throughout this opinion.

FRA opinion

In addition to criminal law implications of irregular entry and stay, third-country national children may also be exposed to forms of exploitation – for example by traffickers – which may lead to the involvement of children in criminalised activities. The creation of an index system would amplify the likelihood that such past criminal activities are uncovered and lead to a disproportionate effect on children. In light of the vulnerability of children, consideration should be given to either excluding children from the scope of ECRIS altogether or from the index, or to limiting exchanges to very serious crimes committed by children.

4. Rights of data subjects and effective remedies against inaccuracy of criminal records

Facilitating the exercise of the rights of data subjects

According to Article 8 of the Charter, everyone has the right of access to data that have been collected concerning them and the right to have it rectified. The right to rectification may also lead to deletion of inaccurate or unlawfully processed data or the blocking of data in specific cases in the interest of the data subject. Moreover, the right to information ensures the data subject is informed about the data collection and the purpose of the collection, as well as the possible or actual data recipients. Data controllers have an obligation to inform the data subject and must communicate the information on their own initiative. The obligation to inform the data subject constitutes a strong safeguard to ensure transparency and thus fairness of the data processing. At the same time, it ensures the effectiveness of remedial actions and, ultimately, legal scrutiny by judicial or non-judicial bodies.

Currently, rules on the data subject's rights are found in Articles 4 (4), 16 and 18 of Framework Decision 2008/977/JHA on the protection of personal data in the framework of police and judicial cooperation in criminal matters. The ECRIS Framework Decision includes the right of access to data in its Article 6, according to which the data subject may submit a request for access and the responsible authority has an obligation to forward the request to the central authority of the EU Member State of the person's nationality.

The current rule in ECRIS on the right of access does not take into account the lack of a link to an EU Member State of nationality with regard to third-country nationals, neither does it establish a duty of cooperation between the EU Member State in which the request for access is submitted and the other EU Member States possibly holding information on the third-country national. The possible future legislative instrument should also ensure an effective right of access for third-country nationals. It may, for example, provide for the submission of requests in the EU Member State of habitual residence and place of work, as well as in any other EU Member State; the EU Member State in which the request is made would then be obliged to forward the request to the other EU Member States. Language barriers should also be taken into account to ensure an effective exercise of the right of access. Current practices that the majority of EU Member States have adopted with regard to the EU's large-scale databases, such as SIS II,[48] in accepting requests in other languages, mostly in English, should be considered.

Furthermore, potential errors in the technology for fingerprints entailing incorrect results and mismatches must be taken into account in the possible future legislative instrument within the scope of the right to access and rectification. In particular, common rules must be introduced for the right to obtain rectification instead of relying on national rules on judicial proceedings as current Article 4 (4) of Framework Decision 2008/977/JHA provides for.

Finally, given a higher probability of data inaccuracies due in part to cases of common names and different alphabets, the following aspect should be considered: strengthening the obligation to notify the third-country national upon each data communication on the data recipients and the content of the communicated data. This aims to mitigate the risks, provided the place of residence of the third-country national can be established and the information does not jeopardise the purpose for which the data were transferred to other parties.

[48] SIS II Supervision Coordination Group, *The Schengen Information System – A guide for exercising the right of access*, as updated in October 2015.

FRA opinion

An effective right to access data and have it rectified, and the right to information for third-country nationals should be ensured in ECRIS-TCN. This needs to take into account issues such as the absence of an EU Member State of nationality, possible language barriers and, if fingerprints are involved, potential errors in the utilised technology.

Ensuring remedies are effective also for third-country nationals

In case of unlawful data processing or violation of rights of data subjects, where a remedy is sought, special attention must be paid to third-country nationals.[49] The lack of certainty of correct identity of some third-country nationals, due to questionable reliability of identity documents, very common names and different alphabets, can lead to wrong matches as regards third-country nationals within national criminal records. This may include situations where past convictions of different perpetrators may be falsely linked to the criminal record of the same person. This can particularly be the case for verdicts predating relevant EU standards, such as on procedural guarantees. ECRIS-TCN based on fingerprints could mitigate this risk for future convictions, but it would not remedy inaccuracies already present in current criminal records and then shared in the future mechanism. This underlines the need for built-in safeguards and checks on the accuracy of older data, including clear rules on convictions predating the establishment of ECRIS-TCN.[50]

Inaccuracies in criminal records can typically be challenged by a defendant in court, as long as the defendant is present or properly represented in such hearings. The mobility of third-country nationals across the external EU border, and the often temporary nature of their residence within the EU, however, increases the likelihood of *in absentia* proceedings (even where presence at trial was not possible for reasons beyond the defendant's control) where third-country nationals cannot effectively challenge the information presented on their alleged criminal record.

Effectively challenging inaccuracies can be even more difficult where the information is requested for other reasons than criminal proceedings. An effective remedy requires not only a notification of the person concerned of the identified criminal record and its consequences, but should also allow for a genuine opportunity to challenge the accuracy of the records before judicial and non-judicial bodies and have the data rectified or deleted. Whereas such an opportunity would usually exist in the context of a criminal procedure where the third-country national is present and/or represented, it is less likely to be in place when information on criminal records is used for other purposes without the involvement of the person concerned – be it in court proceedings or in administrative contexts. Language barriers and absence of legal aid may further complicate access to remedies. Special safeguards should therefore be in place to ensure that remedies are genuine and effective.

---

[49] The ECtHR has in judgments under Article 8 ECHR examined the need to ensure effective remedies, see e.g. *M.M. v. The United Kingdom*, 13 November 2012, para. 179 and *M.N. and others v. San Marino*, 7 July 2015, paras. 82–83. Interferences with the right to an effective remedy when individuals seek to pursue legal remedies in order to have access to personal data relating to them, or to obtain the rectification or erasure of such data should also be considered, as the CJEU pointed out in its recent judgment in C-362/14, *Maximilian Schrems v. Data Protection Commissioner*, , 6 October 2015, para. 95.

[50] Currently the ECRIS Framework Decision (Articles 4 (3) and (4) and 5 (2)) as well as Framework Decision 2008/977 of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (Article 8) provide for a mechanism to verify the accuracy of personal data before transmission for the purpose of further usage.

FRA opinion

Since inaccurate criminal records may be more common in cases involving third-country nationals, safeguards would need to be built into ECRIS-TCN to ensure that only accurate data are exchanged and used, particularly for records pre-dating the establishment of the system.

Particularly challenging situations include those where convictions have been issued after* in absentia *proceedings, and where ECRIS-TCN information is used for other purposes than criminal proceedings. In relation to such contexts, there is a need to assess how safeguards can be put in place to ensure that remedies – including the availability of legal aid, and interpretation and translation – are effective also for third-country nationals.

5. Fundamental rights assessment as part of regular review

Given the considerations outlined above, the possible legislative instrument needs to include a mechanism ensuring its regular review, expressly including a systematic evaluation of fundamental rights concerns. Such mechanisms have become a standard part of EU legislative acts that regulate the collection and exchange of personal data or have other significant potential effects on the rights of individuals, such as the Eurodac or the Eurosur Regulation.[51]

In its 2014 opinion on the proposal to establish a European Public Prosecutor's Office, FRA underlined that such a review *"should be put in place at the very outset of the operations and be done continuously or at least at frequent intervals"*.[52] Taking into account that ECRIS is intimately linked to the principle of mutual recognition, regular assessment would further serve to reinforce overall trust among EU Member States as they use the system.

Such regular evaluation should go hand in hand with the review of the system's effectiveness as regards its main objective: providing for a reliable system for the exchange of information on convictions of third-country nationals. The 2010 Unisys Feasibility Study suggests that compliance with fundamental rights standards should be one of the core monitoring indicators of a proper ECRIS-TCN functioning; other indicators mentioned by Unisys are the exhaustiveness of information on criminal records, addressing identification issues, and the actual use and usefulness of the system.[53] The obligation of the European Commission under Article 7 of the ECRIS Decision to regularly report on the exchange of information through ECRIS is insufficient in this regard, particularly since it does not refer to the need to assess the effect on fundamental rights.

To be effective, an evaluation needs to be based on the collection of data that would from the outset allow to evaluate the effect of an information exchange through ECRIS-TCN on third-country nationals compared to EU nationals, assessing the individual issues of concern mentioned in this opinion. This includes:

- the overall proportionality of the different treatment of third-country nationals;
- possible adverse effects of an information exchange of offences that are specifically related to third-country nationals;
- effect on children;
- effect on refugees;
- effect on the right to fair trial and effective remedy;
- existence of sufficient data protection mechanisms particularly in case the option of using fingerprints as biometric identifiers is opted for.

---

[51] Article 40 (4) of Regulation No 603/2013/EU of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast). Article 22 of Regulation 1052/2013/EU of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur).

[52] FRA (2014), *Opinion on a proposal to establish a European Public Prosecutor's Office,* 4 February 2014, p. 24, available at: http://fra.europa.eu/en/opinion/2014/fra-opinion-proposal-establish-european-public-prosecutors-office.

[53] Unisys (2010), Project Final Report "Feasibility Study: Establishment of a European Index of Convicted Third Country Nationals", p. 47-50.

The review mechanism should expressly refer to the possibility of revising the instrument in case non-compliance with fundamental rights principles is established. The lack of proportionality may lead to an annulment of an instrument that otherwise pursues an objective of general interest.[54]

Given the data protection implications of ECRIS-TCN, the mechanism could envisage the participation of national data protection authorities and/or the European Data Protection Supervisor in the assessment.

FRA opinion

The fundamental rights implications of ECRIS-TCN cannot be fully anticipated and need to be assessed as part of a regular review of the system. Such an assessment needs to cover the compliance with and impact on fundamental rights, evaluating the effect of ECRIS-TCN on the fundamental rights of third-country nationals in comparison with the effect of ECRIS on the fundamental rights of EU nationals. Based on such an assessment, proposals for the revision of the system could be presented.

[54] See particularly CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd and Seitlinger and Others*, 8 April 2014, para. 51.