Face Recognition Technology in Swiss Law Enforcement

Deployment, Legal Basis and Super-Recognizer-Centered Solution

Meike Ramon*

Alexandre Barbey**

Sylvain Métille***

Die polizeiliche Nutzung der Gesichtserkennungstechnologie (FRT) für Zwecke der öffentlichen Sicherheit ist ein Thema, das mehrere Fragen aufwirft. In diesem Beitrag verfolgen wir einen multidisziplinären Ansatz zu diesem Thema. Aus wissenschaftlicher Sicht erläutern wir die technischen Begriffe und die verschiedenen Einsatzmöglichkeiten von FRT, fassen die Ergebnisse einer landesweiten Umfrage bei der Schweizer Polizei zusammen und stellen einen innovativen, menschenzentrierten Ansatz vor, der Super-Recognizer in den Mittelpunkt des zukünftigen FRT-Einsatzes stellt. Aus rechtlicher Sicht muss der Prozess des FRT-Einsatzes das Recht auf informationelle Selbstbestimmung respektieren und seine spezifischen Merkmale müssen klar definiert sein. Wir analysieren die aktuellen schweizerischen Rechtsgrundlagen für den Einsatz von FRT in verschiedenen Szenarien, darunter die Bekämpfung von Hooliganismus, die Überwachung der internationalen Grenzen und die Strafverfolgung. Zuletzt geben wir Empfehlungen für Gesetzesrevisionen, die eine rechtlich zulässige Nutzung von FRT ermöglichen würden, welche die Privatsphäre natürlicher Personen berücksichtigt und respektiert.

L'utilisation de la technologie de reconnaissance faciale (FRT) par la police à des fins de sécurité publique soulève plusieurs questions. Dans cet article, nous adoptons une approche multidisciplinaire. D'un point de vue scientifique, nous définissons les termes techniques et les différentes utilisations possibles de la FRT, nous résumons les résultats d'une enquête nationale menée auprès des corps de police suisses et nous présentons une nouvelle approche centrée sur l'humain, qui place les Super-Recognizers au centre de l'utilisation future de la FRT. D'un point de vue juridique, tout déploiement de la FRT doit respecter le droit à l'autodétermination informationnelle et ses caractéristiques spécifiques doivent être clairement définies. Nous analysons le cadre légal suisse en vigueur pour déterminer les possibilités d'utilisation de la FRT dans différents scénarios, en particulier la lutte contre le hooliganisme, la surveillance des frontières internationales et les procédures pénales. Enfin, nous formulons des recommandations en vue d'une révision législative qui permettrait une utilisation légale de la FRT, qui respecte la vie privée des personnes physiques.

Contents

I. Introduction

The continuously increasing volume of digital information present in our lives has been naturally accompanied by the development of technical solutions required for their processing. One aspect that remains highly controversial is the use of automatic processing of personal

[*] Meike Ramon, Assistant Professor at the University of Lausanne, Head of Applied Face Cognition Lab and Director of the Cognitive and Affective Regulation Lab (photo © SNSF).

[**] Alexandre Barbey, Ph.D. student and graduate assistant at the University of Lausanne.

[***] Sylvain Métille, Associate Professor at the University of Lausanne, Attorney-at-Law.
The authors thank the participants in the Privacy Law Scholars Conference Lausanne 2023 for their useful feedback on an early draft of this article.

information. While in general this can pertain to several sources of personal information, a large part of the public discourse focuses on the processing of image or video material displaying physical persons, in particular the ability to infer their identity based on facial information.

Facial information is the most obvious means to infer a physical person's identity, although in principle several biometric measures can be used to this end (e.g., voice or gait).[1] In our daily lives, humans intuitively use facial identity information for two main purposes. First, we determine prior familiarity, i.e., we ascertain whether a person is known to us. For instance, we can recognize a person we have seen before, even without knowing who they are. Second, provided they are known to us, we can identify physical persons at the individual level. For example, we rapidly identify family members, friends, or acquaintances.

The richness of information conveyed by faces together with the increasing availability and potential processing of facial information is inevitably associated with ethical and legal considerations.[2] These pertain, for example, to the ownership, scope, and nature of the processing, as well as to the sharing and storage of facial information. A major driver in these discussions is the use of automatic solutions for processing facial information, which we refer to as Face Recognition Technology (FRT). All humans continuously process facial information of other people that they encounter. However, our brains do not have the capacity to store or share this information in the way that technology and globalization have enabled. Given its wide-ranging implications,[3] discussions about FRT and Artificial Intelligence (AI) more generally involve a range of different stakeholders. The most prominent are citizens and NGOs, as well as representatives from academia, industry, media, government, and law enforcement.

In this paper we seek to provide a multidisciplinary analysis of the use of FRT by law enforcement. Our aim is threefold: provide an overview of the most important concepts and definitions (II.), offer insights into public opinions concerning FRT, and the *de facto* use of FRT by police forces (III.), and present a legal analysis of the possible (and legally permissible) use cases of FRT (IV.).

Our aim is to reach the widest possible readership to establish the constructive dialogue necessary for the prudent and effective use of FRT in the long term. As academics from the fields of law and cognitive science, the authors of this paper offer an applied perspective on FRT. The paper summarizes data obtained from Swiss police forces and provides an analysis of the legal basis for the use of FRT according to Swiss law. However, we believe that the lessons learned and the challenges around the use of FRT are not unique to Switzerland but extend to other countries as well.

II. General Description of Face Recognition Technology (FRT)

A. Background and Technical Basis

FRT comprises automatic solutions (automated, or partially automated procedures) for the analysis of facial information.[4] All implementations of FRT rely on ***algorithms***, which can be defined as procedures or sets of rules that are used for solving a task or problem.[5] Since the beginnings of FRT development in the 1960s,[6] automatic solutions have changed dramatically, both in terms of their requirements and proficiency.[7] All involve machine learning, which is a sub-field of «the science and engineering of making intelligent machines» that «studies how computer agents can improve their perception, knowledge, thinking, or actions based on experience or data».[8] Broadly speaking, machine learning can fall into

[1] The face is a source of multiple features, which can be processed to infer different types of information. These include emotional states, which can be inferred via analysis of facial expressions from static images or videos using Facial Emotion Recognition (FER) technology (cf. e.g., Internet: https://edps.europa.eu/system/files/2021-05/21-05-26_techdispatch-facial-emotion-recognition_ref_en.pdf [20.11.2023]). In this paper we focus exclusively on the processing of *identity via unchangeable facial information*.

[2] Maëlig Jacquet, Interprétation des scores de reconnaissance faciale automatique pour l'investigation et le tribunal, Thesis Lausanne, Lausanne 2021, 21.

[3] Jared Bennett, Case Study. Facial Recognition, Internet: http://ai.stanford.edu/users/sahami/ethicscasestudies/FacialRecognition.pdf (20.11.2023).

[4] Tiago de Freitas Pereira et al., Eight Years of Face Recognition Research: Reproducibility, Achievements and Open Issues, s.l. s.d., Internet: https://arxiv.org/pdf/2208.04040.pdf (20.11.2023).

[5] European Data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. Version 2.0, s.l. 2023, Internet: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area_en (20.11.2023) (cit. EDPB), 8 and 13; Jacquet (n. 2), 18 ss. and 33 ss.

[6] Suryakant B. Thorat/Sunil K. Nayak/Jyoti P. Pandale, Facial Recognition Technology: An analysis with scope in India, International Journal of Computer Science and Information Security 2010, Vol. 8 no 1, 325 ss.

[7] de Freitas Pereira et al. (n. 4).

[8] Christopher Manning, Artificial Intelligence Definitions, in: Stanford University Human-Centered Artificial Intelligence, Stanford 2020, Internet: https://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf (20.11.2023).

two main categories: classical machine learning and deep learning.[9] It is important to keep in mind that FRT as such is an analysis of images (processing) and not the collection or retention of new images, which are determined by the users of FRT.

Classical machine learning algorithms for FRT required high image quality since analyses depended on the availability of predefined features or facial landmarks. The benefits are ease of interpretation, high performance on small datasets, and modest computational and thus financial investment. However, processing is laborious, efficiency hinges on the availability of critical features, and system performance decreases with increasing datasets.

A major performance increase was achieved half a decade later. «From the year 2015, state-of-the-art face recognition [technology] has been rooted in ***deep learning*** models.»[10] According to Oxford Languages, deep learning (DL) is «a type of machine learning based on artificial neural networks in which multiple layers of processing are used to extract progressively higher-level features from data». One characteristic of DL is that increased training (with larger datasets) leads to improved performance.

Two main types of neural networks can be distinguished: *Convolutional Neural Networks* (CNNs) and *Transformers.*[11] CNNs treat images as structured pixel arrays and process them via hidden representational feature maps of the original image, which do not contain information that humans can extract. Transformers aim to solve some of the limitations of CNNs: differential weighting of important pixels, multi-use filters (as opposed to concept-specific ones), and generalization across the entire pixel space (as opposed to spatially proximal ones).

B. Terms and Definitions

The term FRT is often used to refer to multiple, distinct types of processes (cf. section II.C. and III.A.). To avoid confusion and ensure conceptual distinctiveness, we provide an overview of the most pertinent concepts and definitions around FRT. Note that these are not exhaustive, but rather relevant in the context of the present paper.

Biometrics. The measurement and analysis of unique, unchangeable physical or behavioral characteristics, such as fingerprints, facial features, voice patterns, or iris patterns, that can be used to identify physical persons.[12] Biometric data that uniquely identifies a natural person qualifies as sensitive personal data (art. 5 FADP[13]),[14] thus requiring careful processing.

Face detection. The process of detecting the presence of a face and locating its position in an image or video.[15]

Face recognition technology (FRT). A software application that uses algorithms to analyze a person's facial information. The main goals of its application include (1) identity verification, (2) similarity-based classification of face images, or (3) determining a person's identity. Note that these three use cases differ as to whether they require the presence of a database of known persons (cf. section II.C.).

Facial template. A template is a digital representation of a person's facial features, captured or generated by a facial recognition system, which is used to verify and/or infer their identity. Templates need not represent the face in a way that is informative for humans. Rather, they represent the information that is diagnostic for the system.[16]

Accuracy. The ability of a facial recognition system to correctly verify or identify physical persons. A system's accuracy determines its effectiveness. Factors such as lighting, image quality, or similarity of facial features have an impact on systems' accuracy.[17]

False positives. Incorrect identification of a person, i.e., a «false alarm», for example among physical persons with high resemblance.[18]

False negatives. Failure to identify a person correctly, i.e., a «miss», for example due to changes in facial appearance caused by ageing, make-up, or plastic surgery.

Privacy concerns. Privacy is a fundamental right and a basic prerequisite for the exercise of many other fundamental rights, such as freedom of opinion, religion or information, the right to peaceful assembly and the prohibition of discrimination (cf. section IV.A.). All technologies that involve the processing of biometric data entail a po-

[9] For a recent review c.f. e.g., Christian Janiesch/Patrick Zschech/Kai Heinrich, Machine learning and deep learning, Electronic Markets 2021 no 31, 685-695 and Laith Alzubaidi et al., Review of deep learning: concepts, CNN architectures, challenges, applications, future directions, Journal of Big Data 2021 no 8:53, 1 ss.

[10] de Freitas Pereira et al. (n. 4), 1; see also Jacquet (n. 2), 18 and 33.

[11] Yaoyao Zhong/Weihong Deng, Face Transformer for Recognition, in: Cornell University arxiv, Internet: https://arxiv.org/pdf/2103.14803.pdf (20.11.2023).

[12] Dominika Blonski, Biometrische Daten als Gegenstand des informationellen Selbstbestimmungsrechts, Thesis Bern, Berne 2015, 5 ss.

[13] Federal Act of 25 September 2020 on Data Protection (FADP; SR 235.1).

[14] Special categories of personal data in the meaning of art. 9 par. 1 GDPR.

[15] EDPB (n. 5), 10; Blonski (n. 12), 25.

[16] EDPB (n. 5), 9; Jacquet (n. 2), 19 s.

[17] EDPB (n. 5), 12 s.; de Freitas Pereira et al. (n. 4); Blonski (n. 12), 14 s.; Jacquet (n. 2), 19.

[18] EDPB (n. 5), 15; Blonski (n. 12), 14 s.

tential risk for the privacy of physical persons. These include the potential for misuse or abuse of the technology, and the risk of data breaches or theft. Privacy concerns are mitigated through technical and organizational security measures that define the scope, purpose, and transparency of the technology, responsibilities of individuals tasked with processing the data, rights of individuals whose data is processed, as well as possible sanctions should such measures not be adequately respected.

C. Tasks Achievable via FRT Pertaining to Facial Identity

FRT can be deployed for different purposes (i.e., use cases or *processes*). At base, all rely on initial accurate detection of the presence of a face, i.e., face detection. Beyond this, different processes can be distinguished, which serve different purposes, and in turn differ in terms of their requirements: identity verification, identity clustering, and identification of physical persons. Identity verification and clustering, or matching, can be achieved based on image comparison alone, without previously obtained or stored personal information, and thus without inference of a physical person's identity. Identification, on the other hand, involves either prior knowledge of, or determining, *who* is shown in an image or video. By definition, this requires additional, previously collected information.[19]

1:1 identity verification (or authentication) is the process of verifying that a person is who she or he claims to be.[20] The process of identity verification is routinely performed by, for example, authorities or security personnel, or some personal devices. Theoretically, identity verification relies on neither ex-ante nor ex-post storage of personal data. In the absence of such data storage, before and after the process of identity verification, the identity of a processed physical person can in principle remain unknown.[21] As an example, at international border controls, or public events, physical persons are required to provide proof of identity, which is compared against their likeness. From the perspective of the human professional performing this task, it is not required (nor feasible) to retain the visual and semantic information (i.e., appearance and personal data) that they are presented with.[22] However, personal data obtained in the process of technically assisted identity verification could in principle be stored (e.g., passenger lists).

n:n identity clustering. This process entails the grouping or clustering of images of persons based on an *a priori* defined similarity-based threshold. From a computational (not user-facing perspective), the software automatically computes all pairwise image comparisons, each yielding a score reflecting the similarity of compared identities. As for identity verification, this process does not require knowledge of the identity of a physical person. Put simply, identity clustering involves grouping images thought to depict the same person, and telling apart images thought to depict different physical persons, respectively.

1:n identity matching is the process of searching for a person among a group of physical persons. Unlike the prior processes, 1:n identity matching involves comparisons between persons that are unknown and known, where «known» indicates prior knowledge of the identity of a physical person or persons (e.g., via data stored in a database, or associated with an image). Theoretically, the identity of either the «1» or «n», or both, may be known, giving rise to different possible scenarios: (a) one known person could be searched for among a list of known persons; (b) one known person could be searched for among a list of unknown persons; (c) one unknown person can be compared to a list of known persons.[23] Again, the similarity of compared identities is determined via automatically computed pairwise comparisons of images (cf. n:n identity clustering). From the entire list of (known or unknown) candidates, the user (FRT operator) is provided a best-match list of most likely candidates (i.e., whose computed similarity scores surpass a predefined threshold). Differences in the supra-threshold scores provide an indicator of likelihood for an identity match of the target identity among the list of *n* identities (higher scores indicating more likely identity matches). In theory, the best matches' similarity scores could be provided with or without the respective image, and without any further personal information.[24]

[19] EDPB (n. 5), 9 ss.; Blonski (n. 12), 12 s.

[20] EDPB (n. 5), 9.

[21] This remains quite theoretical because in most cases the person will not be identified but still identifiable, which is personal data.

[22] According to the privacy by design, a machine doing a 1:1 identity verification shall not retain the identity or other data once the identity has been verified.

[23] Note: comparing unknown to unknown person(s) is in instantiation of n:n identity clustering

[24] EDPB (n. 5), 9 s.; Blonski (n. 12), 14 s.; CR FADP-Meier/Tschumy, art. 5 N 63, in: Philippe Meier/Sylvain Métille (édit.), Loi fédérale sur la protection des données, Commentaire romand, Basel 2023 (cit. CR FADP-author).

III. Use of FRT by Swiss Police

Law enforcement is one of the varied FRT stakeholders, which differ in their technical background and knowledge and the extent to which they engage with one another – a situation with a high potential for misconceptions. In preparation for an invited presentation to the members of the Cantonal Parliament in Bern, Meike Ramon conducted a survey of opinions on FRT.[25] Parliamentarians and members of the general public exhibited markedly similar response profiles, indicating the media as their main source of information. «Face recognition» was predominantly associated with surveillance and biometric information processing aimed at determining the *identity of physical persons*, with little understanding of the different possible use cases (cf. section II.C.). From both a technical and human ability standpoint, «face detection» and «face matching» are processing steps that can be performed on unknown facial identities, and are necessary precursors to determining physical persons' identities (cf. section II.).[26]

Adding to the mismatch between public opinions and the technical bases, there is a relative lack of information concerning the de facto practices of Swiss police forces. For example, the authors of a recent TA Swiss report state that «*some police agencies do openly communicate that the use of real-time facial recognition is desirable from their perspective*».[27] The authors further stated that «[t]*o investigate the actual use of police facial recognition in Switzerland, the research team contacted three cantonal police forces that were known from press coverage to be using or testing facial recognition*».[28] Thus, this report focused on a highly selective assessment based on media reporting that cannot be expected to represent all cantonal police.

A. National Survey of Swiss Police

We sought to obtain an objective representation of the status quo concerning FRT across the *entire Swiss law enforcement environment*. Specifically, we aimed to formally assess the actual deployment of FRT, its scope and legal basis for later communication to the public. To this end, our survey solicited information from 39 organizations. Responses were recorded within a two-month period (May-June 2023), with intermittent reminders in the final month. Full details (organizations contacted, complete list of survey questions, and responses collected, as well as communications between organizations who contacted MR) can be found in the Open Science Framework project[29] accompanying this paper.[30] Generally, we approached police press offices, given their mandate to communicate on behalf of the respective organization. Figure 1 (see following page) summarizes the invited organizations and the responses that were obtained.

Of the ten organizations who completed the survey, eight indicated previous or current use of technology for processing biometric data. The other two indicated that there are no considerations to «use technology for this purpose in the future».[31] The most processed type of biometric data using technology is DNA and hand information; no organization indicated processing of eye information. All eight organizations provided information on the legal conditions for processing data, and regarding procedures used or intended to be used to ensure quality control. Five provided information on purposes for which data processing is not permitted. Concerning facial information processing, five organizations indicated prior/current use of technology and provided information on non-/permissible purposes of current or future FRT use, data sources, and persons authorized to use it. The three organizations who indicated no prior or current processing of facial information responded that they were considering using technology for this purpose in the future and provided information regarding the legal conditions for processing data in their organization.

[25] Meike Ramon, Gesichtserkennung. Presentation für die Mitglieder des Grossen Rats des Kantons Bern (CH), Sept 2022, Internet: https://doi.org/10.17605/OSF.IO/B3FXV (20.11.2023).

[26] Meike Ramon/Simon Rjosk, beSure® – Berlin Test For Super-Recognizer Identification. Part I: Development. Verlag für Polizeiwissenschaft, Frankfurt am Main 2022; Meike Ramon, Super-Recognizers – a novel diagnostic framework, 70 cases, and guidelines for future work, Neuropsychologia 2021/158.

[27] Murat Karaboga et al., Automatisierte Erkennung von Stimme, Sprache und Gesicht. Technische, rechtliche und gesellschaftliche Herausforderungen, in: TA Swiss 79/2022, Zurich 2022, Internet: https://doi.org/10.3218/4141-5 (20.11.2023), 114.

[28] Karaboga et al. (n. 27), 116. Of the three police forces in question, the Schaffhausen Police indicated that it does not use face recognition software; the Cantonal Police of St. Gallen and Aargau responded to the ethics questionnaire provided by the authors (177 ss).

[29] Internet: https://osf.io/ytbw7/ (20.11.2023).

[30] We solicited responses to various questions, including for instance and from the onset regarding the use of technologies to process biometric data more generally, which were followed by more specific questionnaire items. Responses were summarized for all items and respondents were able to revise/correct their responses before final submission.

[31] NB: AI indicated that «[i]*n the area of the forensic service, we work together with the St. Gallen cantonal police, which is why we do not process this data ourselves*».

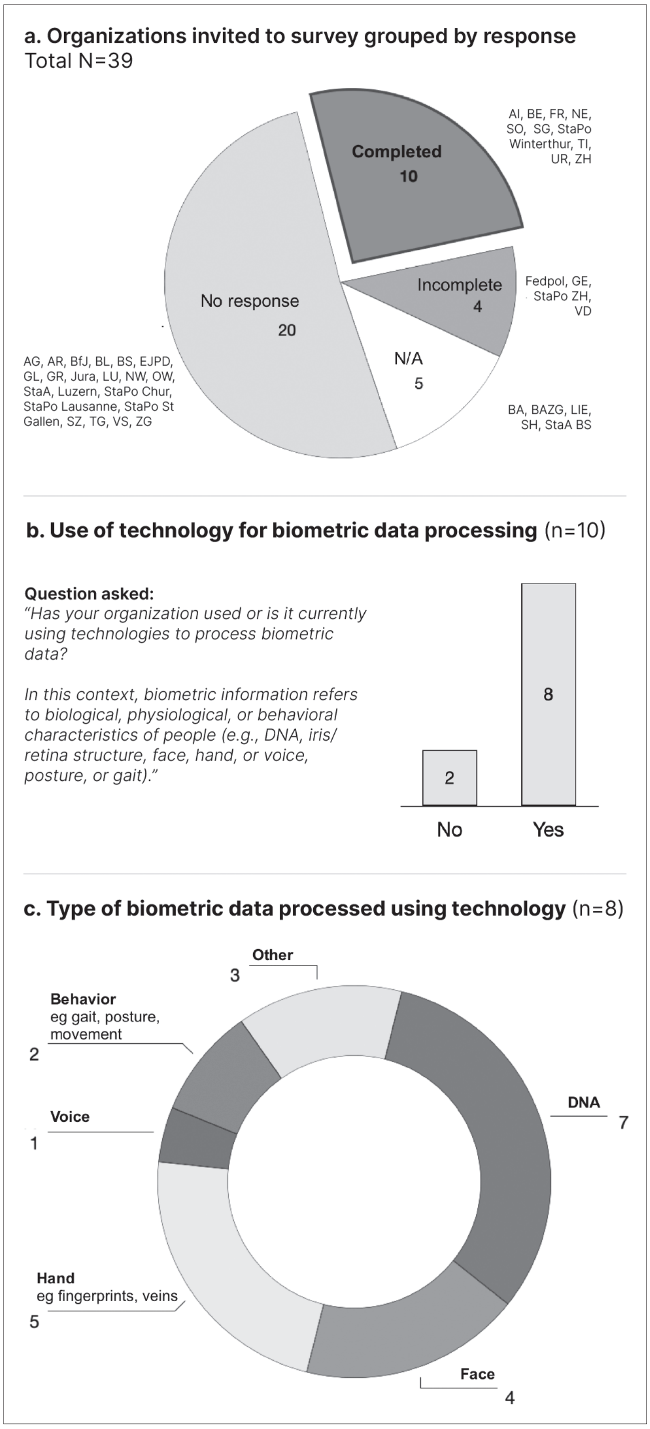

Figure 1. Summary of survey responses.

B. Proposed Human-Centered Approach for Responsible Use of FRT

Concerning the use of FRT, the majority of Ramon's[32] survey respondents expressed the view that its deployment ought to be permitted under specific conditions, using open-source tools or solutions developed by authorities, used by a select group of experts. Concerning this last point, regardless of whether or not technology is used, humans have always had, and will likely continue to make the ultimate call for identification-related decisions. For example, forensic facial examiners are regularly consulted to provide expert, image-based assessments of the facial identity of physical persons depicted in images or video footage of crimes. These experts apply procedures, which they are trained to use, and have specific requirements regarding image quality and available information. As a result, in many cases their procedures are not applicable, for example, when images are of very low quality and/or provide extremely limited visual information.

An interesting recent development in law enforcement is the growing interest in so-called Super-Recognizers, originally discovered and studied by cognitive scientists[33]. These individuals have a naturally occurring (i.e., untrained) superior ability for processing facial identity information. The available evidence suggests that this skill cannot be acquired via training. They excel at *unfamiliar* face identity processing, which is extremely difficult for neurotypical observers (even given high resolution images).[34] Current evidence demonstrates that Super-Recognizers form a robust representation of a physical person's facial appearance even given very limited exposure or information.[35] As a result, Super-Recognizers can proficiently match unfamiliar identities despite extreme changes in viewpoint, or due to ageing, and even extreme cases of partial occlusion.

A growing number of (inter)national police authorities are interested in, or actively engaging in, the identification and deployment of Super-Recognizers. Acknowledging their unique capacities, Super-Recognizers have been

[32] Ramon (n. 26).

[33] Richard Russel/Brad Duchaine/Ken Nakayama, Super-recognizers: People with extraordinary face recognition ability, Psychonomic Bulletin & Review 2009, 16 (2), 252 ss.; Ramon (n. 26).

[34] Meike Ramon/Maria Ida Gobbini, Familiarity matters: A review on prioritized processing of personally familiar faces, Visual Cognition 2018 Vol. 26 no 3, 179 ss., Internet: https://doi.org/10.1080/13506285.2017.1405134 (20.11.2023).

[35] Jeffrey D. Nador/Tamara A. Alsheimer/Ayla Gay/Meike Ramon, Image or Identity? Only Super-recognizers' (Memor)Ability is Consistently Viewpoint-Invarian*t*, Swiss Psychology Open 2021 1(1): 2, 1 ss., Internet: https://doi.org/10.5334/spo.28 (20.11.2023).

proposed as a «perceptual technology» in the context of the European safety project «SafeCi – Safer Space for Safer Cities».[36] The Berlin Police recently completed a six-year project devoted to the development of beSure®, a bespoke police tool to identify Super-Recognizers.[37] Several German and Swiss police officers have already been identified as Super-Recognizers using validated lab procedures, many of them first reported in Ramon[38]. The Winterthur Police was the first to reportedly hire one such individual because of their ability,[39] and recently Meike Ramon has tested St. Gallen police officers to identify Super-Recognizers among their ranks[40]. Notably, Swiss legal scholars view the deployment of Super-Recognizers as qualitatively different and significantly less invasive as compared to automatized processing achieved solely via FRT.[41]

According to Ramon,[42] Super-Recognizers can represent the foundation of a novel type of human-centered approach to tasks sought to be achieved via FRT and/or forensic experts that could be pioneered in Switzerland. Given the available empirical evidence suggesting that Super-Recognizers process facial identity in a fundamentally different and complementary way than both neurotypical humans and algorithms[43], they should be deployed where (future) FRT use is required and permitted.[44] Integrating humans with a superior, natural ability would address concerns around: (a) the use of FRT; (b) documented performance variability among trained human experts;[45] and (c) well-established limited effects of training[46]. To maximize proficiency and informative value, Super-Recognizers should have access to state-of-the-art technology developed and/or tested through leading Swiss biometric experts.[47] Restricting the use of FRT to Super-Recognizers with the aim of improving the outcome of automated processes would also provide an effective human oversight.[48] The right to have a human in the loop or an automated decision reviewed by a natural person as required by art. 21 FADP for example is of little value if the human in question does not have the skills required to make a thorough review. Implementing Super-Recognizers in this manner, a process ideally accompanied and evaluated by independent scientific experts, would serve to improve the adopted procedures and to maintain trust in legal processes.

IV. Privacy Considerations

A. Privacy as a Fundamental Right

Art. 13 par. 2 of the Swiss Constitution[49] enshrines the fundamental right to informational self-determination.[50]

[36] Funded by the EU's Internal Security Fund, this project brought together a consortium of ten European Police authorities. They exchanged best practices to analyze and evaluate existing concepts, strategies and technical solutions to improve the protection of public spaces and to ensure public safety in Europe. European police and security authorities can order the final handbook, «*European Recommendations for the Protection of Public Spaces against Terrorist Attacks»*, which summarizes the results.

[37] Ramon/Rjosk (n. 26); Meike Ramon/Matthew J. Vowels, Large-Scale Super-Recognizer Identification in the Berlin Police, Internet: https://osf.io/preprints/psyarxiv/x6ryw (20.11.2023). The identified officers are tasked with challenging criminal cases, e.g. investigations into the December 2022 New Year's riots (Jana Herrmann, Alle(s) im Blick, 2023, Internet: https://www.rbb24.de/panorama/beitrag/2023/04/super-recognizer-gesichtserkennung-berlin-brandenburg-polizei-fahndung.html (20.11.2023)). The largest German police force is also adopting beSure® to test their officers (Tim Wegner, Wie im Tunnel, Internet: https://unna.polizei.nrw/artikel/wie-im-tunnel [20.11.2023]).

[38] Ramon (n. 26).

[39] Dominik Steiner, Ein Experte für Gesichtserkennung geht auf Verbrecherjagd, 2023, Internet: https://www.srf.ch/news/schweiz/stadtpolizei-winterthur-ein-experte-fuer-gesichtserkennung-geht-auf-verbrecherjagd (20.11.2023); Daniel Gerny, Sie erkennen Gesichter besser als jede Software: Erstes Schweizer Polizeikorps setzt auf Super-Recognizer, 2023, Internet: https://www.nzz.ch/schweiz/sie-erkennen-gesichter-besser-als-jede-software-erstes-schweizer-polizeikorps-setzt-auf-super-recognizer-ld.1718837 (20.11.2023).

[40] Kantonspolizei St. Gallen, Super-Recognizer, 2023, Internet: https://fokus-kaposg.ch/2023/11/15/super-recognizer/ (20.11.2023).

[41] Monika Simmler/Julia Canova, Die Unrechtmässigkeit des Einsatzes automatisierter Gesichtserkennung im Strafverfahren – ein weiterer Beitrag zu einer anhaltenden Debatte, ZSR 2023, 201 ss, 211.

[42] Ramon (n. 26); Ramon (n. 25); Meike Ramon, Unique traits, computational insights: studying Super-Recognizers for societal applications, preprint, Internet: https://osf.io/preprints/psyarxiv/8zejy (20.11.2023).

[43] Ramon/Vowels (n. 37) and Ramon/Rjosk (n. 26).

[44] Simmler/Canova (n. 41), 211.

[45] P. Jonathon Phillips et al., Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms, PNAS 2018 Vol. 115 no 24, 6171 ss., Internet: https://doi.org/10.1073/pnas.1721355115 (20.11.2023).

[46] Alice Towler/David White David/Richard I Kemp, Evaluating Training Methods for Facial Image Comparison: The Face Shape Strategy Does Not Work, Perception 2014, Volume 43, 21 ss.; Alice Towler et al., Do professional facial image comparison training courses work?, PLoS One 2019 14(2), 1 ss.

[47] Internet: https://www.idiap.ch/en (20.11.2023).

[48] Rebecca Crootof/Margot E. Kaminski/W. Nicholson Price II, Humans in the Loop, Vanderbilt Law Review 2023, 429 ss., 464 ss., 474 ss., 504 and 507.

[49] Federal Constitution of 18 April 1999 of the Swiss Confederation (Cst.; SR 101).

[50] CR Cst. I-Hertig Randall/Marquis, art. 13 N 62, in: Vincent Martenet/Jacques Dubey (édit.), Constitution fédérale I, Commentaire

This fundamental right protects anyone against any processing of personal data by the State.[51] The notion of processing is broad and includes all kinds of data processing, in particular the collection, retention, analysis, destruction, and transmission to third parties of personal data concerning an identified or identifiable natural person (art. 5 let. d FADP).[52, 53] In the context of this article, physical characteristics, photographs or videos of a person are considered personal data.[54] Despite its limiting wording, stating that «[e]*very person has the right to be protected against the misuse of their personal data*», art. 13 par. 2 Cst. protects not only from the misuses, but also restricts any processing of personal data by a government body.[55] Each natural person enjoys this fundamental right,[56] making even simply adding a person to a database problematic[57].

Article 8 par. 1 ECHR generally protects privacy and is the counterpart of the Swiss right to informational self-determination.[58] Article 7 of the Charter of Fundamental Rights of the European Union (the Charter) comes from art. 8 par. 1 ECHR. Even if Switzerland is not bound by the Court of Justice of the European Union (CJEU) case law, it must be taken into consideration.[59] Several European Court of Human rights (ECHR) cases are of interest for our study. In *Leander v. Sweden*, the ECHR ruled with regard to the laws governing files processed by the State that, «*in a system applicable to citizens generally* […] *the law has to be sufficiently clear in its terms to give them an adequate indication as to the circumstances in which and the conditions on which the public authorities are empowered to resort to this kind of secret and potentially dangerous interference with private life.* […] *In addition, where the implementation of the law consists of secret measures, not open to scrutiny by the physical persons concerned or by the public at large, the law itself, as opposed to the accompanying administrative practice, must indicate the scope of any discretion conferred on the competent authority with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the physical person adequate protection against arbitrary interference*».[60]

In *Wisse v. France*, the ECHR stated that «*monitoring a physical person's actions in a public place using a camera system without recording visual data does not in itself constitute an intrusion into the physical person's privacy […]. On the other hand, the recording of data and its systematic or permanent nature may give rise to such considerations. Therefore* [...] *the Court found that the compilation of data by the security services on particular physical persons, even without using covert surveillance methods, constituted an interference with the applicants' private lives*».[61] While some may argue that images recorded in a public place do not deserve to be protected, this is in fact wrong.[62] The retention and further analysis of images may reveal a lot more information than what could just be seen in a public space at a specific time, in particular if one thinks of the addition of some data. Additional data may include, for example, that the person drinking a beer is a Muslim, that the person traveling on Saturday is Jewish, or that one member of this lovely couple is married to another person. The mere fact of filming (sometimes even without viewing the footage) may have a chilling effect, for example, in case of a (permitted) political demonstration. Thus, according to the ECHR's case law, there is an interference with the right to privacy when the government records data by means of cameras. The EU AI Act proposal explicitly prohibits the use of real time remote biometric identification in publicly accessible spaces for the purpose of law enforcement (with strict exceptions) because this creates an unacceptable risk of violating

romand, Basel 2021 (cit. CR Cst. I-author); Philippe Meier, Protection des données. Fondemants, principes généraux et droit privé, Bern 2011, N 17; BSK Cst.-Diggelmann, art. 13 N 32, in: Bernhard Waldmann/Eva Maria Besler/Astrid Epiney (édit.), Bundesverfassung, Basler Kommentar, Basel 2015 (cit. BSK Cst.-author); St. Galler Kommentar Cst.-Schweizer/Striegel, art. 13 N 79, in: Bernhard Ehrenzeller et al. (édit.), Die schweizerische Bundesverfassung I, St. Galler Kommentar, 4th ed., Zürich/St.Gallen/Geneva 2023 (cit. SGK Cst.-author).

[51] CR Cst.-Hertig Randall/Marquis (n. 50), art. 13 N 62; Meier (n. 50), N 17 and 26.

[52] CR Cst.-Hertig Randall/Marquis (n. 50), art. 13 N 62; Meier (n. 50), N 30; SGK Cst.-Schweizer/Striegel (n. 50), art. 13 N 85.

[53] The GDPR contains similar definitions.

[54] BSK Cst.-Diggelmann (n. 50), art. 13 N 33; Meier (n. 50), N 30; SGK Cst.-Schweizer/Striegel (n. 50), art. 13 N 87.

[55] BSK Cst.-Diggelmann (n. 50), art. 13 N 34; Michael Montavon, Cyberadministration et protection des données. Étude théorique et pratique de la transition numérique en Suisse du point de vue de l'État, des citoyen-ne-s et des autorités de contrôle, PhD Thesis (Université de Neuchâtel), Geneva/Zürich/Basel 2021, 193 s.; SGK Cst.-Schweizer/Striegel (n. 50), art. 13 N 85.

[56] Pascal Mahon, Droit constitutionnel. Droits fondamentaux, Vol. II, 3rd ed., Basel 2015, 103; SGK Cst.-Schweizer/Striegel (n. 50), art. 13 N 81.

[57] BSK Cst.-Diggelmann (n. 50), art. 13 N 35.

[58] HK ECHR-Nettesheim, art. 8 N 33, in: Jens Meyer-Ladewig/Martin Nettesheim/Stefan Raumer (édit.), EMRK Europäische Menschenrechtskonvention, Handkommentar, 5th ed., Basel 2023 (cit. HK ECHR-author).

[59] EDPB (n. 5),14.

[60] ECHR, 9248/81, *Leander v. Sweden*, 26.3.1987, N 51.

[61] ECHR, 44647/98, *Peck v. the United Kingdom*, 28.1.2003, N 59 (our translation).

[62] Simmler/Canova (n. 41), 207.

fundamental rights.[63] The prohibition covers any remote, real-time FRT deployment to determine the identity, ethnicity, gender, political or sexual orientation, or emotion of a natural person in public spaces and places. It also covers any instance of an FRT solution that gathers personal data on a mass scale in an indiscriminate way (e.g., by «scraping» photographs and facial pictures via social networks).[64]

The interference is only admissible under art. 8 par. 2 ECHR if it is based on a clear, accessible, and foreseeable law.[65] As a fundamental right, informational self-determination may also be restricted under the conditions of art. 36 Cst. The restriction must have a legal basis and significant restrictions must be provided for by a formal act (*Formelles Gesetz*, *loi au sens formel*).[66] It is important to underline that the requirement of the legal basis cannot be lifted by the consent of the data subject.[67] Moreover, restrictions on fundamental rights must be justified by the public interest or by the protection of the fundamental rights of others (art. 36 par. 2 Cst.). Police interests, such as security and public order, are recognized as valid public interests but in this area, minimum qualitative requirements must be met.[68]

Diggelmann argues that the interest of the data subject in using his or her right to informational self-determination may conflict with the public interest in combating crime.[69] The clash between these interests is crucial to the issue at hand, namely whether the police can use FRT. Collecting face images, extracting unique characteristics, maintaining a database comparing collected images to those in a database and adding information to a database represent restrictions to each physical person's right to informational self-determination.[70] On the other hand, the police have arguments related to internal security in favor of such procedures. A balance of these interests is necessary.

Any restriction to a fundamental right must be proportionate to the purpose (art. 36 par. 3 Cst.). This implies that the measure must be necessary and suitable to achieve the objective of the restriction. Every interest must ultimately be considered in relation to each other.[71] Lastly, the essence of fundamental rights is sacrosanct (art. 36 par. 4 Cst.). Collectively, these fundamental rights considerations demonstrate that the requirement of a formal, clear and predictable legal basis is mandatory for the police to use face recognition software.[72] The use of FRT requires data (images) of physical persons, from which biometric data can be extracted and compared.

Depending on whether the FRT controller is a federal body, for instance Fedpol, or a cantonal body, such as cantonal and city police forces, the applicable data protection laws vary (cantonal bodies being generally subject to cantonal data protection laws). In all cases, however, a legal basis is required for the processing of data, which must be a formal law in the case of the processing of sensitive data (art. 34 par. 2 let. b FADP, *e.g.,* art. 5 al. 2 Vaud-ADP). The Swiss Supreme Court ruled that the collection of data from a large number of physical persons without their knowledge constitutes a serious infringement on personal freedom, even if only a limited number of physical persons have access to the data.[73]

In EU case law, the *Digital Rights Ireland* case of 8 April 2014[74] invalidated an EU directive on data retention in the field of telecommunications. The CJEU ruled that the obligation to retain data relating to a person's private life (traffic and location data) without his or her knowledge, for a minimum period of six months without discrimination according to the data categories, with unclear rules, for the purpose of combating serious crime, violates the fundamental rights to private life and communications and to the protection of personal data (art. 7 and 8 of the Charter).

In a 2016 Opinion[75] on a draft agreement between Canada and the EU on the transfer and processing of airline passenger name record data, the Advocate General concluded that the processing – consisting of the automated collection of data relating to the private sphere of mil-

[63] Proposal of 21 April 2021 for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act «AI Act») and amending certain union legislative acts, 5.2.2., recital 23 and art. 5.

[64] EDPB (n. 5), 29.

[65] ECHR, 27798/95, *Amann v. Switzerland*, 16.2.2000, N 55.

[66] CR Cst.-Dubey (n. 50), art. 36 N 82; StGK Cst.-Schweizer/Krebs (n. 50), art. 36 N 26; EDPB (n. 5), 15 s. Every formal act meets the requirements of art. 36 par. 2 Const., *i.e.* a cantonal formal legal basis can meet this condition. The English version states that a *federal act* has no legal force.

[67] CR Cst.-Dubey (n. 50), art. 36 N 76.

[68] CR Cst.-Dubey (n. 50), art. 36 N 107; StGK Cst.-Schweizer/Krebs (n. 50), art. 36 N 26 and references; Nadja Braun Binder/Eliane Kunz/Liliane Obrecht, Maschinelle Gesichtserkennung im öffentlichen Raum, sui generis 2022, Nr 204, N 27.

[69] BSK Cst.-Diggelmann (n. 50), art. 13 N 34.

[70] Simmler/Canova (n. 41), 207.

[71] CR Cst.-Dubey (n. 50), art. 36 N 119; StGK Cst.-Schweizer/Krebs (n. 50), art. 36 N 53 s.; EDPB (n. 5), 17 ss.

[72] EDPB (n. 5), 15 s.

[73] ATF 122 I 360 c. 5c.

[74] Joint Cases C-293/12 and C-594/12.

[75] Opinion 1/15 of Advocate General Mengozzi delivered on 8 September 2016, Internet: https://curia.europa.eu/juris/document/document.jsf?docid=183140&doclang=EN (20.11.2023).

lions of physical persons, their transfer to the Canadian authorities, and their retention for a period of five years for the purpose of combating terrorism – constituted a significant interference with the fundamental right to respect for private and family life. It did not matter to the Advocate General that most of the persons concerned were not inconvenienced and that the majority of the information was not sensitive. Thus, according to this opinion, even at the stage of simply taking photographs of physical persons, a formal law is necessary for data processing within the meaning of art. 34 par. 2 let. c FADP.[76]

The requirement of formal law is not overdue and, according to the proportionality principle, one should be very cautious in allowing the collection of biometric data and its further processing with FRT. Biometric data is *per se* sensitive personal data, irremediably linked to the person.[77] Clear guidance, real oversight and a formal framework are necessary.

Having established the need for a legal basis, we now turn to review which laws can serve as such a basis. To our knowledge, there are only two cases for which Swiss legislation expressly allows the use of FRT. The first was introduced in the context of the 2008 UEFA European Football Championship and targets identification of hooligans (B). The second concerns the longstanding practice of video surveillance at international borders (C). In the following sections we discuss these two cases and we cover federal criminal law provisions on criminal investigations and the use of biometric identification (IV.D.) as preventive surveillance by the police forces (IV.E.).

B. HOOGAN

In preparation for the 2008 UEFA European Football Championship, which took place in Switzerland and Austria, art. 24*a* ss of the Federal law instituting measures for the maintenance of internal security (LMSI) were adopted. This was at first a temporary[78] legislation that allowed the authorities to take additional measures to ensure security during sports events, such as a perimeter ban (art. 24*b* aLMSI), a ban on travel to a particular country (art. 24*c* LMSI), an obligation to report to the police (art. 24*d* aLMSI), and measures concerning police custody (art. 24*e* aLMSI).[79]

Even if some safety measures were repealed, art. 24*a* par. 1 LMSI was not. This shows the risk of an expansion of surveillance. First deployed as a temporary measure and justified by a specific international and large-scale event, the measure has ultimately become permanent and applicable to more standard sports events that take place on an almost daily basis. This also indicates a political choice in favor of strong policing of football and hockey games.[80]

Art. 24*a* par. 1 LMSI now provides the legal basis for the operating of an electronic information system named HOOGAN that records data on persons who have exhibited violent behavior at sports events. It exists for the purpose of fighting violence during sports events (art. 4 par. 1 OMAH)[81].[82] It stores data – e.g., photographs, surname, first name, date and place of birth, hometown, address, type of measure taken (art. 24*a* par. 3 LMSI) – of persons who are known to have committed acts of violence at a sports event and against whom one of the safety measures mentioned above has been issued (art. 6 par. 2 let. a and 8 OMAH). HOOGAN refers to both the database and the electronic comparison system.

According to article 10 of the Ordinance on the HOOGAN information system, data can be processed in electronic personal recognition systems. Depending on the aim, selected services from Fedpol and cantonal police authorities and a restricted circle of other individuals and organizations may have access to HOOGAN (art. 9 par. 1 OMAH). The ordinance specifies rules pertaining to storage time and data sharing in Switzerland and with foreign authorities (art. 10-12 OMAH). The provisions of the Cyber Risks Ordinance[83] and Ordinance to the Federal Act on Data Protection[84] apply to data security.

HOOGAN is only used for the top leagues' games where the authorities have decided that the public should be required to show their ID.[85] The current regulations al-

[76] Braun Binder/Kunz/Obrecht (n. 68), N 28.

[77] As opposed to a user ID that could be changed when exposed.

[78] RO 2006 3703 and RO 2009 5090: art. 24*b*, 24*d*, 24*e* and 24*h* were repealed on 31th December 2009.

[79] Message du 17 août 2005 relatif à la modification de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (Mesures contre la propagande incitant à la violence et contre la violence lors de manifestations sportives), FF 2005 5285 ss, 5290.

[80] See for example Jacquet (n. 2), 12.

[81] Ordonnance du 4 décembre 2009 sur les mesures de police administrative de l'Office fédéral de la police et sur le système d'information HOOGAN (OMAH; SR 120.52).

[82] Sylvain Métille, Mesures techniques de surveillance et respect des droits fondamentaux, PhD Thesis Neuchâtel, Basel 2011, 245.

[83] Ordinance of 27 May 2020 on Protection against Cyber Risks in the Federal Administration (CyRV; SR 120.73).

[84] Ordinance of 14 June 1993 to the Federal Act on Data Protection (DPO; SR 235.11).

[85] Conférence des directrices et directeurs des départements cantonaux de justice et police, Modification du concordat du 15 novembre 2007 instituant des mesures contre la violence lors de manifestations sportives. Rapport de la Conférence des directrices et di-

low for 1:n identity matching by electronic personal recognition systems (art. 10 par. 2 OMAH). Only the data of the persons who appear in the HOOGAN database are recorded; data (images) from other people is not stored.[86] However, the limits of what can be done are not detailed. It is unclear whether this electronic system entails processes such as those enabled via FRT for processing of biometric information. For instance, does the system use cameras linked to FRT systems, or does it only to compare pictures from a person's ID card, or only their name to the HOOGAN database? Art. 3*a* of the concordat of 15 November 2007 instituting measures against violence at sports events (2012 version) and the ATF 140 I 2 c. 9.3 – validating the compatibility of the revised version of the Concordat with Art. 13 para. 2 fed. Cst. – may indicate that the comparison is made between the database recorded in HOOGAN and the name (rather than the facial photograph) on the ID document[87] presented to the control authorities.

The Federal Data Protection and Information Commissioner (FDPIC) addressed the issue of face recognition in sports stadiums in his 2008/2009 report. According to the report, the existing legal framework allows the use of FRT linked to HOOGAN because there is an overriding private or public interest.[88] However, data protection principles remain applicable. In particular, HOOGAN data must not be cross-referenced with other data and it must be deleted immediately upon the ending of the sporting event (art. 10 par. 3 OMAH). Moreover, data subjects must be informed of the FRT by billboards at the entrance of the stadium. While current legislation seems to allow the use of FRT at the entrance of stadiums under certain conditions, it is not possible to use FRT beyond that for proportionality reasons, especially during a game in the stadium.[89] If the use of FRT is acceptable here, this is in particular because only the images of the persons entering the stadium (and not any image collected within or around the stadium) are compared to a limited number of images of people who have committed acts of violence and against whom safety measures have been imposed. The collection of data and use of FRT is transparent and no person is obliged to enter the stadium. In addition, the use of FRT cannot in and of itself lead to a definitive entry denial, but rather it may lead to a human verification (that should happen without delay). One may ask, however, if someone could oppose the use of FRT and request to enter through a gate with only human controls.

C. Identity Verification at International Borders

Art. 103 of the Federal Act on Foreign Nationals[90] provides a clear legal basis for the use of FRT at airport arrivals for foreign nationals that are not citizens of member states of the European Community (EC) or the European Free Trade Association (EFTA) or their family members, and employees posted to Switzerland by employers residing in, or with their registered office in, these states (art. 2 par. 2 FNIA).

This is only a possibility offered to the authorities in charge of border control, rather than an obligation (art. 54 OEV)[91]. Data – including a face photograph that is the biometric reference – may be collected when a person entering Switzerland by air is suspected of being an illegal immigrant or posing a concrete threat to Switzerland's internal or external security (art. 55 and 56 OEV). The system may be used to identify someone being checked by police in the transit zone of the airport, filing an asylum application there, or wanting to pass through passport control without being able to present valid identity documents (art. 57 OEV). If a match results from 1:n identity matching, collected data (art. 55 OEV) may be transferred to the State Secretariat for Migration (SEM), cantonal migration authorities, and Swiss representations abroad (art. 59 OEV). There are strict rules about the data retention period. Stored data must be deleted after 30 days; special rules apply if a criminal procedure or asylum and immigration procedure is initiated (art. 60 par. 1 and 2 OEV). The photograph taken for comparison and the related biometric data must be deleted immediately after the consultation of data (art. 60 par. 3 OEV). There has traditionally been a broader acceptance of control at the border when they target non-residents.[92]

Art. 103*b* ss FNIA is the legal basis for the Entry/Exit System (EES). The operation of the system is different from that of Art. 103 FNIA. The aim here is to carry out more effective and secure border controls to ensure, by

recteurs des départements cantonaux de justice et police du 2 février 2012, s.l. 2012, 24.

[86] PFPDT, 16ème Rapport d'activités. 2008/2009, Berne 2009, 50.

[87] Idem.

[88] PFPDT (n. 86), 51.

[89] PFPDT (n. 86), 52.

[90] Federal Act of 16 December 2005 on Foreign Nationals and Integration (FNIA; SR 142.20).

[91] Ordonnance du 15 août 2018 sur l'entrée et l'octroi de visas (OEV; SR 142.204).

[92] See for example Hillel R. Smith, Do Warrantless Searches of Electronic Devices at the Border Violate the Fourth Amendment?, CRS Legal Sidebar 2021, 2.

means of an automatic calculator, that the maximum duration of stay in the Schengen area has not been exceeded.[93] These articles are linked to European Regulation 2017/2226 and to the Schengen area. A central database stores face images.[94]

Art. 103*g* FNIA provides a legal basis for the automated border control (ABC) with a biometric passport through electronic gates. Both EU and EFTA and non-EU citizens can use the automated control system (art. 45 OEV). There is no obligation to use it. Each member state of the Schengen area is free to set up such electronic gates.[95] In Switzerland, cantons where the airport is located are competent to establish such systems.[96] This process does not use a centralized database. The biometric reference is stored in the passport's chip.[97] Therefore, it is a 1:1 verification at the gate. In adopting this provision, the legislator provided for the data captured at the door to be compared with other databases: EES, RIPOL, SIS, SYMIC and ASF-STD from Interpol. If the person turns out to be the legitimate passport holder and is not registered in these other information systems, he can walk through the door.[98] Automated border control exists at Zurich Airport and Geneva Airport.

D. Swiss Criminal Code and Procedure Code

As soon as suspicions justify the initiation of criminal proceedings by the police or the prosecutor, the CrimPC applies (and the FADP and the cantonal data protection laws do not apply anymore). The Swiss Constitution and the ECHR remain applicable so requirements relating to fundamental rights are fully applicable (cf. *supra* IV.A). The CrimPC does not contain explicit provisions allowing for the use of FRT.[99] We will nevertheless examine whether the CrimPC may provide, through an extensive *de lege lata* interpretation of its provisions, a legal basis for the use of FRT by law enforcement authorities.

Provisions on evidence (art. 139 ss CrimPC) establish the principle that any means of evidence capable of establishing the truth may be administered (art. 139 par. 1 CrimPC), apart from the prohibited means (art. 140 CrimPC). However, there is a safeguard when the evidence infringes fundamental rights. In this case, there must be a clear legal basis for the investigative technique.[100] Failing to meet this requirement, evidence provisions cannot serve as a legal basis for FRT deployment.[101] Note, however, that in our view the use of FRT solely within a specific case, using only the data lawfully collected and stored in the case file, does not breach the provisions of the CrimPC as it does not compare with other sources.[102] For example, to find out when the defendant appears in legally collected CCTV images of several hours duration, the FRT can be used by comparing these images with the legally collected photograph of the defendant. The infringement of the fundamental rights of the defendant and of third parties that appear in the CCTV images is limited. First, the FRT is only used on CCTV images stored in the case file that are already known to be relevant to the investigation. That is very different from running FRT on all Swiss CCTV streams of public places to find a person that would be compared with the entire database of all criminals. Only the defendant, for whom criminal proceedings have been initiated, is being sought using FRT. Second, the template derived from the defendant photograph and the CCTV images stay in the case file. Third, the comparison result does not appear anywhere else, for example in a centralized database. Fourth, in any case, the result is reviewed by a human being who uses FRT only to avoid the task of viewing several hours of video.

Coercive measures (art. 196-298*d* CrimPC) are subject to a *numerus clausus* (art. 197 par. 1 let. a CrimPC). The use of FRT is not listed, and therefore it is clear that these provisions cannot serve as a legal basis for this purpose.[103]

[93] Message du 21 novembre 2018 concernant l'approbation et la mise en œuvre des échanges de notes entre la Suisse et l'UE concernant la reprise des bases juridiques en vue de la création et de l'utilisation du système d'entrée et de sortie (EES) (règlements [UE] 2017/2226 et 2017/2225 ; développements de l'acquis de Schengen) et modification de la loi sur les étrangers et l'intégration (LEI), FF 2019 175 ss (cit. Message Entrée Sortie), 184.

[94] Message Entrée Sortie (n. 93), 185.

[95] Message Entrée Sortie (n. 93), 185.

[96] Message Entrée Sortie (n. 93), 215.

[97] Message Entrée Sortie (n. 93), 216.

[98] Message Entrée Sortie (n. 93), 215 s.

[99] Simmler/Canova (n. 41), 209.

[100] Simmler/Canova (n. 41), 219 s.; CR CrimPC-Bénédict, art. 139 N 2 and 5, in: Yvan Jeanneret/André Kuhn/Camille Perrier Depeursinge (édit.), Code de procédure pénale suisse, Commentaire romand, 2nd ed., Basel 2019 (cit. CR CrimPC-author); BSK CrimPC-Gless, art. 139 N 16, in: Marcel Alexander Niggli/Marianne Heer/Hans Wiprächtiger (édit.), Schweizerische Strafprozessordnung/Jugendstrafprozessordnung, Basler Kommentar, 3rd ed., Basel 2023 (cit. BSK CrimPC-author); Gérard Piquerez/Alain Macaluso, Procédure pénale Suisse, 3rd ed., Geneva/Zürich/Basel 2011, N 965 s.

[101] Simmler/Canova (n. 41), 219 s.; Braun Binder/Kunz/Obrecht (n. 68), N 29.

[102] See also Stefan Kühne, Automatisierte Bearbeitung von Personendaten im Strafprozess- und Polizeirecht, Sicherheit & Recht 2022, 13 ss., 22.

[103] Idem.

Articles 260 and 261 CrimPC allows for the recording and retention of identification data (including facial images) but there is nothing about the creation of templates or a database of multiple facial images that could be used by FRT.[104] In addition, even if art. 280 and 282 CrimPC allow for images to be recorded in public spaces, they cannot be compared with other sources. Therefore, these images cannot be analyzed with FRT.

General provisions on data collection and processing (art. 95 ss CrimPC) are far too broad to allow for the use of FRT[105] and clearly do not meet the clarity and predictability requirements mentioned above. In the Swiss Criminal Code,[106] art. 354 is a specific provision on (national and international) assistance in criminal matters. To identify a wanted or unknown person, the Federal Department of Justice and Police may compare biometric identification data collected by authorities in the performance of their legal duties, including photographs.[107] This provision is not the legal basis for the collection of a physical person's identification data.[108] The purpose of this provision is to be able to centralize and compare data, but only for the purpose of identifying a wanted or unknown person.[109]

Reading the Federal Council's Message about the law on criminal records modifying Art. 354 SCC, we note that the legislator intended to adopt a legal basis for the automatic fingerprint identification system (AFIS).[110] The AFIS Ordinance[111] only provides for fingerprints to be automatically compared with each other. Photographs are considered as biometric data and are collected in AFIS, but there is no provision for photographs to be compared with each other in AFIS, let alone for a video stream in which physical persons appear, either live or recorded, to be compared with the photographs in AFIS. An interpretation based on the will of the legislator shows that Art. 354 SCC does not allow the use of FRT.[112] If, however, the provision was to be interpreted broadly, it should be noted that Art. 354 SCC would only allow for case-by-case comparison between two photographs,[113] i.e., 1:1 identity verification or 1:n identity matching. A new information system would have to be created, and new rules adopted.

This is precisely the goal of the AFIS 2026 project. It represents the required renewal of the current AFIS, which was created in 2016 for a 10-year lifespan. AFIS 2026 foresees the integration of a facial image comparison module. This would allow images of a suspect in the possession of prosecuting authorities to be automatically compared with images contained in AFIS for identification purposes. This would be a powerful tool for law enforcement authorities, and one can see it as acceptable and proportionate as only people already in AFIS will be identified. This mainly includes data seized during criminal proceedings to establish the identity of wanted or unknown persons (art. 8 AFIS Ordinance), meaning the presumed perpetrator or unidentified victim.[114] In addition, the unknown person to be identified is the subject of an ongoing investigation.

AFIS 2026 would enable a comparison between face images, on a case-by-case basis, as currently practiced for fingerprints.[115] This would not allow a comparison between images in AFIS and, for example, photographs of identity documents. The purpose is also not to enable real-time surveillance linked to CCTV cameras. This would, of course, not be desirable and would be an unacceptable *Rasterfahndung*.[116] To our knowledge, however, no legal text has yet been adopted, and the AFIS ordinance has not been modified. A credit had been approved for AFIS 2026 but it is still in the planning stage. It is not yet possible to determine how this will be implemented. Thus, the legal framework described above remains the only guide as to what is permissible under applicable laws. The AFIS 2026 project would therefore only require an amendment to the ordinance. In our view, only selected police personnel should have access to the facial image comparison module. In any case, its scope remains limited and does not constitute a carte blanche for unrestricted use. In particu-

[104] Simmler/Canova (n. 41), 214.
[105] Simmler/Canova (n. 41), 214 s.
[106] Swiss Criminal Code of 21 December 1937 (SR 311.0; SCC).
[107] CR SCC II-Tirelli, art. 354 N 3, in: Alain Macaluso/Nicolas Queloz/Laurent Moreillon/Robert Roth (édit.), Code penal II, Commentaire romand, Basel 2017 (cit. CR SCC II-author); BSK SCC II-Gamma, art. 354 N 7, in: Marcel Alexander Niggli/Hans Wiprächtiger (édit.), 4th ed., Basel 2019 (cit. BSK SCC II-author).
[108] CR SCC II-Tirelli (n. 107), art. 354 N 1.
[109] CR SCC II-Tirelli (n. 107), art. 354 N 6.
[110] Message du 20 juin 2014 relatif à la loi sur le casier judiciaire, FF 2014 5525, 5675.
[111] Ordonnance du 6 décembre 2013 sur le traitement des données signalétiques biométriques (SR 361.3).
[112] Statement of the Federal Council to interpellation Min Li 22.3993 «Base légale pour la reconnaissance faciale automatisée dans les procédures pénales?» of 16 November 2022: the Federal Council states that FRT and comparing two facial images are not the same. Article 354 SCC only allows the second one.
[113] CR SCC II-Tirelli (n. 107), art. 354 N 6.
[114] BSK SCC II-Gamma (n. 107), art. 354 N 11.
[115] Federal Council, *Press release – Le Conseil fédéral approuve le crédit d'engagement pour le renouvellement du système AFIS*, Berne, 6 April 2023.
[116] Eveline Roos/Konrad Jeker, Antennensuchlauf im Rahmen einer Rasterfahndung, forumpoenale 3/2012, 175 ss., 176.

lar, the AFIS 2026 project does not include the possibility of a real-time face recognition.[117]

If the legislator wants to allow for the use of FRT by law enforcement authorities, a new law needs to be adopted, in a way similar to the DNA Profiles Act,[118] which provides clarity and precision.[119]

E. Police Surveillance

Police activity can be divided into three main categories: surveillance, investigation, and intelligence.[120/121] Police surveillance has a preventive purpose, and thus includes activities carried out before an(y) offense is committed. Police investigations are part of criminal procedure governed by the Swiss Criminal Procedure Code (CrimPC).[122] A criminal procedure governed by the CrimPC is initiated as soon as there is a suspicion of any offense (minor or otherwise) having been committed. Criminal proceedings are pending as soon as the preliminary proceedings are open, i.e., as soon as the police investigate, or the public prosecutor opens an investigation (art. 300 par. 1 CrimPC). This Code is applicable to cantonal and federal police authorities (art. 15 par. 1 CrimPC). The FADP does not apply to pending criminal proceedings (art. 2 par. 3 FADP).[123]

The applicable legal framework is not the same depending on the stage at which one envisages to use FRT. Federal bodies (like Fedpol) are subject to the FADP and cantonal bodies are subject to cantonal laws (which contain similar provisions). The FADP does not contain a specific provision on the use of FRT, but several provisions are of interest. As stated above, FRT can involve different types of processing of personal data. A biometric template is extracted from the data to be compared against an existing police database that links physical persons' faces to an identity. According to Art. 5 let. c FADP biometric data is per definition sensitive data. Apart from the requirement for a formal legal basis based on fundamental rights considerations, art. 34 par. 2 FADP requires a legal basis in the formal sense for the processing of sensitive data.[124]. A legal basis must therefore exist for the creation of the database, as well as for the use of FRT.[125] Lastly, Article 21 FADP provides that the controller must inform the data subject that an automated decision was made, and the data subject can ask for a review by a human being.

Several principles contained in the FADP seem to oppose the deployment of FRT by the police. The principle of proportionality (Art. 6 par. 2 FADP, 36 par. 3 Cst., 8 par. 2 ECHR) requires that of the available possible means, the one(s) most suitable and causing the least serious harm should be chosen. Finally, a measure's effect regarding the data concerned must be balanced against the expected result.[126] The purpose principle (art. 6 par. 3 FADP) restricts the possible uses of the potentially collected data, which must be determined before the processing begins and not altered thereafter.[127] When federal bodies are the controllers, the purpose must be defined in a legal basis, and with greater precision should fundamental rights be affected (art. 34 par. 1 FADP, 36 par. 1 Cst., 8 par. 2 ECHR).[128]

The cantons have the power to legislate on this matter each for their own police forces (cantonal and city police forces).[129] To our knowledge, most of the cantons did not specifically legislate the use of FRT by their police forces for surveillance purposes,[130] bar one historical exception. In the canton of Zurich, before the enactment of the Foreign Nationals and Integration Act[131], an ordinance[132] regulated the use of FRT at Zurich Airport by the Zurich

[117] Statement of the Federal Council to interpellation Min Li 22.3993 «Base légale pour la reconnaissance faciale automatisée dans les procédures pénales?» of 16 novembre 2022.

[118] Federal Act of 20 June 2003 on the Use of DNA Profiles in Criminal Proceedings and for Identifying Unidentified or Missing Persons (RS 363).

[119] Statement of the Federal Council to interpellation Min Li 22.3993 «Base légale pour la reconnaissance faciale automatisée dans les procédures pénales?» of 16 novembre 2022.

[120] Kühne (n. 102), 17.

[121] This article focuses on traditional police activities and does not cover intelligence and surveillance deployed by police forces at the request of the Federal Intelligence Service (FIS). The FIS's cooperation with other federal authorities and the cantons is regulated by the Federal Act on the Intelligence Service (IntelSA SR 121).

[122] Swiss Criminal Procedure Code of 5 October 2007 (CrimPC; SR 312.0).

[123] CR FADP-Métille/di Tria (n. 24), art. 2 N 62; CS FADP-Rudin, art. 2 N 34, in: Datenschutzgesetz, Stämpflis Handkommentar, 2nd ed., s.l. 2023; Kühne (n. 102), 16.

[124] The exceptions in par. 3 do not seem to apply in this case.

[125] CR FADP-Epiney/Posse (n. 24), art. 34 N 47 ss.

[126] CR FADP-Meier/Tschumy (n. 24), art. 6 N 27 s.; Meier (n. 51), N 665; BK FADP-Lambrou/Steiner, art. 4 N 9 ss., in: Datenschutzgesetz Öffentlichkeitsgesetz, Basler Kommentar, 3rd ed., Basel 2014; Braun Binder/Kunz/Obrecht (n. 68), N 17.

[127] CR FADP-Meier/Tschumy (n. 24), N 47, 50 ss.

[128] CR FADP-Epiney/Posse (n. 24), N 36 ss.

[129] CR Cst.-Bleiker (n. 50), art. 57 N 26; CR Cst.-Grodecki (n. 50), art. 123 N 18; CR CrimPC-Arn/Steiner (n. 100), art. 1 N 5; BSK CrimPC-Rhyner (n. 100), art. 306 N 5; CR CrimPC-Parein (n. 100), art. 306 N 2.

[130] Simmler/Canova (n. 41), 206.

[131] Federal Act of 16 December 2005 on Foreign Nationals and Integration (FNIA ; SR 142.20).

[132] Verordnung vom 8. Dezember 2004 über den Einsatz eines biometrischen Gesichtserkennungssystems am Flughafen Zürich (OS 551.113; abolished the 1st January 2008).

cantonal Police Forces with the goal of identifying illegal immigrants.

The canton of Lucerne recently adopted art. 4^{quiquies} and art. 4^{sexies} of the Lucerne Police Act (PolG/LU)[133] (effective since 01.01.2023). Art. 4^{sexies} PolG/LU states that the Lucerne Police may operate or participate in analysis systems for the prevention and investigation of felonies and misdemeanors (art. 10 par. 2 and 3 SCC)[134] that are repeatedly and frequently committed by the same offenders or groups of offenders (serial crimes). Various data, including sensitive data, can be collected and automatically processed for this purpose (art. 4^{sexies} par. 2 PolG/LU). The data must have been collected by the federal police, customs authorities, or police authorities of other cantons (art. 4^{sexies} par. 4 PolG/LU), and rules apply to the retention time. Art. 3b of the Lucerne Police Ordinance[135], which complements PolG/LU, allows specially trained officers to use real-time analysis systems using face recognition data to identify repeat offenders and adapt police measures.

Despite its safeguards, art. 4^{sexies} PolG/LU insufficiently details the specifications of systems permitted/deployed for automatically assisted analyses. Furthermore, its scope is very broad and can include minor offenses and misdemeanors with a potential serial component, even in the absence of convictions or formal investigations. Finally, its purpose – the identification and adaptation of police measures – is also very broadly defined. In our view, this provision does not meet the fundamental rights requirements for the police to use FRT. To be clear, this assessment does not mean that the PolG/LU is unconstitutional or unusable for data processing and other purposes, but only that it cannot be interpreted to allow the use of FRT.

On the other hand, art. 4^{quiquies} PolG/LU is a legal basis for the recording and automatic recognition of vehicle number plates and of the occupants of the vehicle for the tracing of persons or property and for the prosecution of crimes and misdemeanors. Images are collected when a vehicle passes through a camera's field of view and can be automatically compared with databases and used for travel profiling. The provision expressly authorizes comparison with police registers on persons and objects and for specific searches. The provision is insufficiently precise concerning the automatic comparison of vehicle occupants and its scope and purpose are too broad. The proportionality principle prevents this law from being used for authentication (1:1), identity matching (1:n) or identity clustering (n:n). One could question whether the adoption of such a provision for the purpose of using data collected in criminal proceedings is within the canton's jurisdiction.[136] For other cantons that have not adopted a legal basis, there is no doubt that they cannot use FRT for surveillance activities.[137]

Many cantons have general provisions to allow video surveillance systems, with or without recording systems. However, these provisions do not allow these systems to be linked to FRT. They are simply meant to authorize some video-recording and use of the images as evidence in criminal proceedings. For example, the Canton of Vaud's law, article 21b of the Law of 17 November 1975 on the cantonal police (BLV 133.11), states that the authorization of the Public Prosecutor's Office is required to conduct preventive observations involving audio or video recordings. Moreover, specific indications of the potential crimes must exist, and other forms of investigations must be considered as having no chance of success (subsidiarity principle). There is here no doubt that without any specific mention of FRT, no such use can be envisaged (not in real time nor after the recording).

V. Conclusion and Recommendations

The use of FRT is intrinsically linked to the processing of significant amounts of personal, including sensitive, data of persons of interest, including plenty of innocent people. Inasmuch as police forces are required to use the best possible tools to identify criminal offenders, the use of any such tools shall occur under strict compliance with fundamental rights and applicable laws, only to fight serious crimes and with clear legal limits and redress mechanisms. As discussed above, the use of FRT is currently admissible under Swiss laws in two specific situations, i.e., entrance to sporting locations and crossing of international borders. The CrimPC does not expressly allow the use of FRT during criminal investigations. However, we consider that FRT can be legally used in one limited situation: to match the identity of a physical person among pieces of evidence (images, videos) in a specific case, without comparing data with a database. The privacy infringement and

[133] Gesetz vom 27. Januar 1998 über die Luzerner Polizei (PolG/LU; SRL Nr. 350).

[134] Art. 4^{sexies} PolG-LU is not applicable to contraventions (art. 103 SCC).

[135] Verordnung vom 6. April 2004 über die Luzerner Polizei (PolV; SLR Nr. 351).

[136] It looks like art. 4^{quiquies} par. 4 PolG-LU is trying to add a covert surveillance measure that is not included in the CrimPC *numerus clausus*.

[137] Kühne (n. 102), 18. It is up to the legislator to allow the use of FRT.

the risks associated are low in this case and the use of FRT will principally save investigation time.

As stressed by European authorities (in particular by the EDPB and the EDPS), certain use cases of FRT, notably instances of live data processing (i.e., surveillance) represent an unacceptable risk of intrusion into physical persons' private lives and have no place in a democratic society. Even a formal law cannot justify such an intrusion. If a law were to authorize certain limited forms of FRT use in other situations, it should in our view comply with certain requirements. First, data protection principles must be respected (proportionality, purpose limitation, security, transparency, accountability, etc.). In particular, the use of FRT would require judicial control, and should be subsidiary to any less intrusive measure and limited to the localization or identification of persons suspected of having committed a serious crime. Such safeguards are already known for measures like telecommunications surveillance and should be considered as minimum requirements in relation to FRT. In addition, organizations should be obligated (a) to conduct a privacy impact assessment before deploying any FRT; (b) to ensure that only certain, qualified law enforcement professionals – Super-Recognizers among law enforcement professionals – have access to and permission to use FRT, and (c) to be able to explain and overturn any result provided by FRT. Thus, organizations should be responsible for maintaining the required expertise, including up-to-date knowledge concerning limitations of their FRT solution(s) and strategies to minimize their impact.

Decisions about the present and future use of FRT involve balancing interests relating to fighting serious crime, the right to private life, and what is acceptable or desirable in a democratic society. The availability of a technology does not justify its deployment. Likewise, failure to adopt potentially critical available tools can also involve repercussions. Choices should be made carefully, and only after consultation with experts from law enforcement, privacy law and constitutional law, as well as developers and evaluators of automatic solutions for biometric processing. The importance of a long-term consideration cannot be underestimated, lest ultimate and sweeping decisions prevent necessary future applications in different contexts, or a rapid adoption without careful consideration causes permanent and irreversible damage. History has shown that when a surveillance tool is deployed, it is rarely stopped even if it does not prove useful for the originally intended purpose.[138] This is particularly significant given the often slow timescales at which legal and democratic decisions are reached despite the potentially rapidly emerging challenges with which law enforcement often finds itself confronted. The reported desire for transparency[139] can be met, and the expressed high levels of trust towards the Swiss government, judiciary, and police[140] can be maintained, through the deployment of Super-Recognizers as uniquely and naturally able law enforcement professionals, who can be trained in the responsible use of state-of-the-art FRT[141] and who can act within a clear and well-established legal framework that respects the fundamental rights of the citizens.

[138] Neil M. Richards, The Dangers of Surveillance, Harvard Law Review, Vol. 126, 1934 ss., 1938 and 1941.

[139] Murat Karaboga et al. (n. 27).

[140] OECD, Government at a Glance 2021, OECD Publishing, Paris 2021, Internet: https://doi.org/10.1787/1c258f55-en (20.11.2023) and Tibor Szvircsev Tresch et al., Sicherheit 2022. Aussen-, Sicherheits- und Verteidigungspolitische Meinungsbildung im Trend, in: ETHZürich Birmensdorf/Zürich 2022, Internet: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Si2022.pdf (20.11.2023).

[141] Ramon/Rjosk (n. 26), 3629; Ramon (n. 26).