Ceza Hukuku ve Kriminoloji Dergisi-Journal of Penal Law and Criminology 2017; 5(2):89-106
ISSN: 2148-6646 / E-ISSN: 2602-3911

http://dergipark.gov.tr/iuchkd

Research Article / Araştırma Makalesi

DOI: 10.26650/JPLC360268

Databases and Criminal Procedures in Switzerland and Turkey with Regard to European Council's Standards

Avrupa Konseyi Standartları çerçevesinde İsviçre ve Türk Hukukunda Veri Tabanları ve Ceza Muhakemesi

Begüm BULAK UYGUN[1]

[1]Dr. Iur, MLaw (Faculty of Law, University of Geneva), LLM (College of Europe), ELFA Vice-President, Geneva, Switzerland

ABSTRACT

Databases are increasingly used by law enforcement to effectively investigate and prosecute criminal offences. The growing tendency and need for law enforcement to use big data is particularly challenging when the data is stored abroad. As law enforcement authorities' coercive powers are limited to their national territories, the path to enhanced judicial cooperation in criminal matters and police cooperation is of paramount importance.

With the increasing use of big data, personal data processing takes place when the concerned individuals whose data is actually being processed are absent. This raises issues related to data regulations and to the effectiveness of existing mechanisms of legal protection for data subjects.

This article deals with concerns relating to privacy protection in the context of data retention and judicial data exchange in Europe. To this end, a comparative analysis of Swiss and Turkish legal frameworks with regard to the European Court of Human Right's case law provides a useful tool in identifying the legal standards that can help strike a fair balance between legitimate interests in database use and personal privacy protection. The specifics of the interplay between the right to privacy and the prevention and combatting of crime in Swiss and Turkish cultures also creates a fertile ground to discuss the flaws in existing regulations.

Keywords: Databases, Privacy, Personal Data, Cross-border investigations, Judicial Cooperation, Police Cooperation, Criminal Procedure, Law Enforcement, Europol

ÖZ

Veri tabanları, kolluk kuvvetleri tarafından yürütülen soruşturma ve kavuşturmalar için giderek daha fazla ve etkili bir şekilde kullanılmaktadır. Kişisel verilerin toplanması bir suçun işlenmesini önlemek gibi meşru bir amaca hizmet ederken, aynı zamanda veri sahibinin özel hayatına da müdahale niteliğindedir. Bu nedenle güvenlik önlemlerinin alınması ve kişisel verilerin korunması bir denge içerisinde olmalıdır.

Büyük verilerin artan kullanımıyla, kişisel verilerin işlenmesi ilgili kişilerin bilgisi dışında gerçekleşmektedir. Bu durum kişisel verilerin korunmasına ilişkin mevcut düzenlemelerin ve ilgili kişisel veri sahiplerine sağlanan hukuki güvencelerin etkinliğine ilişkin hususları gündeme getirmektedir.

Günümüzde yargı alanlarını ve sınırları aşan suçlar yalnızca ulusal bir mesele değildir. Kolluk kuvvetlerinin yetkileri ulusal topraklarla sınırlı olduğundan ötürü, cezai konularda polis ve adli işbirliği büyük önem arz etmektedir. Bu özellikle, ciddi suçların çoğunun uluslararası boyutu göz önünde bulundurulduğunda geçerlidir.

Mevcut çalışmada Avrupa'da verilerin saklanması ve adli veri değişimi bağlamında kişisel verilerin korunması ele alınmaktadır. Bu bağlamda, Avrupa İnsan Hakları Mahkemesi içtihatları ilgili İsviçre ve Türk yasal düzenlemelerinin karşılaştırmalı analizinde veri tabanı kullanımı ile kişisel verilerin korunması arasında adil bir dengenin oluşturulmasını sağlayabilecek yasal standartların belirlenmesinde önem teşkil etmektedir. Kişisel verilerin korunması ile suçun önlenmesi ve suç ile mücadele arasındaki karşılıklı etkileşim İsviçre ve Türkiye'deki mevcut düzenlemelerdeki farklılıkları tartışmak için verimli bir zemin yaratmaktadır.

Anahtar Kelimeler: Veri tabanları, Kişisel veriler, Büyük veriler, Kolluk Kuvvetleri, Polis ve Adli İşbirliği, Ceza Muhakemesi, Adli veri değişimi, Avrupa Polis Ofisi, Avrupa İnsan Hakları Mahkemesi

Date of receipt: 21.09.2017 • **Date of acceptance:** 25.09.2017

Corresponding author: Begüm Bulak Uygun, E-mail: begumbulak@gmail.com

Disclaimer: This article was verbally presented on 28.04.2016 at the Swiss Institute of Comparative Law and thus it does not take into account any legal changes after this date.

Citation: Bulak Uygun, B. (2017). Databases and criminal procedures in Switzerland and Turkey with regard to European Council's standards. *Ceza Hukuku ve Kriminoloji Dergisi-Journal of Penal Law and Criminology 2017; 5(2):89-106*.
https://doi.org/10.26650/JPLC360268

EXTENDED ABSTRACT

We are witnessing a decade where human activities have led to an unprecedented scale of data collection and processing. Databases are being increasingly used by law enforcement to effectively investigate and prosecute criminal offences. Databases undeniably enhance the efficiency of investigations and assist in the prevention and prosecution of crime. However, the use of databases should also be assessed in relation to the protection of fundamental rights. Given the fact that the storage and processing of data are deployed to control, detect, deter, and prevent crime, databases and privacy are strongly linked. Depending on the case, the important aim of investigating serious crime may not sufficiently justify data retention.

With the increasing use of big data, personal data processing takes place in the absence of the concerned individuals whose data is actually being processed. This raises issues related to data regulations and the effectiveness of existing mechanisms of legal protection for data subjects.

On a different note, crime is no longer solely a national concern: it crosses jurisdictions and borders with ease. The growing tendency and need for law enforcement to use big data is particularly challenging when the data is stored abroad. Data transfer is particularly problematic if the recipient country cannot ensure an appropriate level of data protection. Because law enforcement authorities' coercive powers are limited to their national territories, the path to enhanced judicial cooperation in criminal matters and police cooperation is of paramount importance. This is particularly true given the transnational dimension of most of serious crimes. It is essential for countries to cooperate in investigating and prosecuting criminal acts. This is particularly true in Switzerland and Turkey because of their status in the regional context: both lie outside the European Union (EU) but still have a high degree of interaction with the EU.

This article deals with concerns relating to privacy protection in the context of data retention and judicial data exchange in Europe. A comparative analysis of Swiss and Turkish legal frameworks with regard to the European Court of Human Right's case law provides a useful tool in identifying the legal standards that can help strike a fair balance between legitimate interests in database use and personal privacy protection. The specifics of the interplay between the right to privacy and the prevention and combatting crime in Swiss and Turkish cultures also creates a

fertile ground to discuss the flaws in existing regulations. To this end, we describe the core principles in database processing with reference to the Council of Europe's standards. Then we evaluate the legal frameworks of two countries under consideration. Last but not least, we assess the practical implications of these legal frameworks with regard to transmittal of personal data, with reference to the European Police Office.

1. Introduction

Security concerns are at the forefront of data storage, and the increasing use of databases in criminal procedures raises problems in terms of ensuring the respect and protection of fundamental rights. Databases are in widespread use in criminal justice worldwide, and they have undoubted advantages: Databases contribute considerably to rapid intervention in crime investigation and allow for information exchange between countries, but they undoubtedly have an impact on individual privacy that creates the need for appropriate regulation regarding the use and storage of the data collected. Police undoubtedly collect and use sensitive personal data, and processing this information infringes on the fundamental right to protection of privacy. If enforcing criminal laws requires preserving personal information, greater awareness is needed of the threat to privacy that is implicit in accumulating vast amounts of personal information in data banks.

Traditionally, investigations and criminal proceedings were mainly conducted at the national level. Mostly focused on the national dimension of serious crime, national law-enforcement authorities were unwilling to cooperate across national boundaries. However, many crimes in the 21st century have a transnational dimension that requires at least a regional if not a global law enforcement response. Separately, we are witnessing a decade driven by digital data that are being used in many sectors, notably in law enforcement, and electronic indexing now enables an unprecedented scale of data collection and processing.

Increasingly, cross-border investigations and prosecutions resulted in the need for closer judicial cooperation, and the use of databases is considered one of the key elements in significantly improving the administration of justice, especially for law-enforcement authorities to exchange data more efficiently and effectively.

As noted above, crime is not solely a national concern but crosses jurisdictions and borders with ease. Because it is crucial for countries to cooperate in investigating

and prosecuting criminal acts,[1] it is more important than ever to have coherent and compatible data protection frameworks. Alongside concerns that national databases threaten to undermine the right to privacy, cross-border exchanges of personal data by law-enforcement bodies also have considerable implications. Data transfer is particularly problematic when the receiving country cannot ensure appropriate protection. Moreover, although law-enforcement agencies would usually obtain due authorization for the use of specific data, the data sharing does not necessarily require such authorization. Clearly, a high level of personal data protection for individuals would ensure effective law enforcement and judicial cooperation in criminal matters.[2]

Given the judicial data interchange and storage of data in Europe, this paper suggests a comparative assessment of the Swiss and Turkish legal frameworks with regard to European minimum standards. More specifically, this research addresses the data interchange between the law-enforcement bodies, in particular, the privacy challenges associated with surveillance, primarily within the realm of criminal justice databases. That is, this paper sketches the extent to which data protection laws interact with criminal procedural law in order to evaluate the effectiveness of police and judicial cooperation.[3] When assessing individual privacy in the area of criminal law, the concern must be the extent to which criminal procedures are constrained by a respect for privacy.[4]

In order to identify parallels and discrepancies between the two legal frameworks under study, the relevant national laws will be assessed based on European legal standards, and the operational practice will be measured based on the systems' effectiveness and independence. Before embarking on this assessment, the paper provides an overview of the criteria laid down in European Court of Human Rights' (ECtHR) case law with a particular focus on the right to private life and data protection in the context of criminal justice systems. The following section concentrates on and evaluates existing legislation and practice at the national level in order to evaluate compliance with European standards. To this end, it is important to identify the

1 European Commission, Communication to the Council and the European Parliament : Towards enhancing access to information by law enforcement agencies, COM (2004) 429 final, 16.06.2004.

2 See the Council of Europe Recommendation CM/Rec (2010)13, *The Protection of Individuals with Regard to Automatic Processing of Personal Data in the Context of Profiling*.

3 Common rules for processing and protecting personal data in criminal matters as foreseen for the EUROPOL and INTERPOL provide important benchmarks for research in the field of law enforcement cooperation.

4 Erik Claes, Anthony Duff, Serge Gutwirth, Privacy and the Criminal Law, Intersentia, Antwerp, 2006, at 2.

existing national systems and to assess whether their practices are in accord with the practices of the Court. The conclusion makes proposals for rectifying and improving any flawed practices.

2. The European Benchmarks

2.1. Legal Framework

The Council of Europe's instruments contain general operating guidelines regarding data protection that seek to guarantee the right balance between the requirements of combating terrorism and organized crime on the one hand and the duty to respect personal data on the other.

The first of these instruments is the European Convention of Human Rights (ECHR) which provides a right to protection of personal data as a subset of the right to privacy as guaranteed by Article 8. Article 8 ECHR is a qualified right, although the right to a private family life and respect for the home and correspondence is non-absolute and may be restricted under certain circumstances.

Such interference is acceptable only if it passes a three-pronged test. First, the interference under scrutiny has to be prescribed by law or in accordance with law,[5] and the legal basis has to comply with accessibility and foreseeability requirements.[6] Second, the interference must fall under one of the "legitimate aims" in the second paragraph of Article 8 such as national security or public safety or to prevent disorder or crime[7]. Third, the interference must be "necessary in a democratic society"[8]: That is, it must follow a "pressing social need"[9] and not be greater than what is required to attain the social need in question.[10]

In addition to the negative obligation, namely to refrain from interfering in the right to privacy under Article 8, ECHR imposes a positive obligation on the contracting states that aims to ensure effective protection with the adoption of reasonable and appropriate measures.

5 See for instance *Adali v. Turkey*, (ECHR, 31.03.2005), § 271-272.

6 The legal norm has to be accessible to an individual and formulated precisely with regard to its meaning and scope. See, e.g., *N.F. v. Italy*, (ECHR, 2.08.2001), § 26-29.

7 See, e.g., *Rassemblement Jurassien and Unité Jurassienne v. Switzerland*, (ECHR, 10.10.1979); *Chassagnou and Others v. France,* (ECHR, 29.04.1999)

8 *United Communist Party* of *Turkey and Others v. Turkey,* (ECHR, 30.01.1998), § 45.

9 *Freedom and Democracy Party (ÖZDEP) v. Turkey*, (ECHR, 8.12.1999), § 43-44.

10 *Öllinger v. Austria*, (ECHR, 29.06.2006) § 47.

In complement to Article 8 ECHR, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981 (hereinafter: Convention No. 108)[11] and its Additional Protocol define personal data as "any information relating to an identified or identifiable individual"[12]. Convention No. 108 aims "to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him."[13] In other words, it tends to fill the gaps in national legislation on general rules for registering and using personal information. Preceded by two resolutions on data protection,[14] Convention No. 108 contains substantive law provisions as basic principles for data protection such that "each Party should take the necessary steps to give effect to this "common core" in its domestic legislation."[15]

It is crucial that personal data be "obtained and processed fairly and lawfully" and "stored for specified and legitimate purposes."[16] Special categories of data such as criminal convictions may not be processed automatically unless appropriate safeguards are provided by domestic law.[17]

In parallel to the positive obligations incumbent under Article 8 ECHR, Article 10 of Convention No. 108 expressly requires establishing appropriate sanctions and remedies for violating provisions of domestic law under the Convention.

In this respect, the case law emphasizes that "the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 ECHR. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article. The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes."[18]

11 *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 18.01.1981.

12 Article 2 (a) Convention n°108.

13 Article 1 Convention n°108.

14 *Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, p. 5.

15 *Ibidem*.

16 Article 5 Convention n°108.

17 Article 6 Convention n°108.

18 *S. and Marper v. The United Kingdom*, (ECHR, 4.12.2008), § 103.

By analogy with the legitimate aims listed in paragraph 2 of Article 8 ECHR, Article 9, paragraph 2 of Convention No. 108 allows for the possibility to derogate from the basic principles when such derogation is needed in order to protect the fundamental values in a democratic society.[19]

Further, Recommendation No. R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector comprises different rules for collecting, storing, using, and communicating personal data for police purposes.[20] According to Article 5 of Convention N°108, the core principles for data protection from the Council of Europe's legal framework can be summarized as personal data must be processed fairly and lawfully;[21] collected for specified, explicit and legitimate purposes and not used in a way incompatible with those purposes;[22] adequate, relevant and not excessive in relation to the purposes for which they are stored;[23] accurate and, where necessary, kept up to date;[24] preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.[25] The most significant principles related to the retention of personal data are "purpose specification and limitation", "data minimization", and "fairness".[26] Essentially, law-enforcement bodies are not allowed to collect more data on individuals or to store data for longer than they need for crime prevention and/or prosecution. Finally, retention of personal data must be subject to accountability, which recalls the effective remedy requirement pursuant to Article 13 ECHR.

2.2. Case Law

According to well-established Court case law, "the storing of information relating to an individual's private life in a secret register and the release of such information come within the scope of Article 8 § 1 [ECHR]."[27] The Court has consistently held

19 Namely in the interest of protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences.

20 Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector Adopted by the Committee of Ministers on 17.09.1987 at the 410th meeting of the Ministers' Deputies.

21 Article 5 (a) Convention n°108.

22 Article 5 (b) Convention n°108.

23 Article 5 (c) Convention n°108.

24 Article 5 (d) Convention n°108.

25 Article 5 (e) Convention n°108.

26 Commissioner for Human Rights, The Rule of law on the Internet and in the wider digital world, Issue Paper, Council of Europe, at 89.

27 *Leander v. Sweden*, (ECHR, 26.03.1987), § 48; *Rotaru v. Romania*, (ECHR, 4.05.2000), § 43.

that storing personal data by police and criminal justice authorities constitutes interference with Article 8 ECHR,[28] and it is not necessary for a person to know about it or be inconvenienced by it. In short, European case law implies that any storage of data constitutes an interference with and infringement on the right to privacy, including exchanging already stored information in executing police cooperation requests.

Storing and exchanging personal data give rise to separate responsibilities under Article 8 ECHR,[29] and each step in the chain of data processing and data exchange is considered a separate interference. Hence, any release, storage or request of information concerning criminal investigations and their results in the course of international cooperation would also necessitate a separate justification.

As a consequence of the principle of legality, laws justifying these infringements must stipulate clearly and precisely the conditions for any infringement ranging from collecting to transferring data. Among many others, the Court addressed data retention within law-enforcement powers in the following four cases.

A first prominent example of this intricate relationship between databases and crime prevention is the leading case of *S. and Marper v. the United Kingdom*,[30] the relevant facts of which are as follows. Two men were arrested in 2001, and their fingerprints and DNA samples were taken; *S.* was a minor by then, and he was acquitted a few months later, and for *Marper*, the case was formally discontinued. Both asked for their fingerprints and DNA samples to be destroyed, arguing that the retention of their data created suspicion with respect of persons who had been acquitted, but in both cases the police refused.[31] Although the interference had a legal basis and retaining the information pursued the legitimate purpose of preventing crime by assisting in identifying future offenders,[32] under the core principles of the Council of Europe's instruments that require that data be retained in proportion to the purpose for their collection and limited in time, particularly in the police sector, the necessary conditions were not satisfied; the retention was not limited in time, and only limited possibilities existed for acquitted individuals to have their data removed

28 *B.B. v. France* (ECHR, 17.12.2000) ; *Gardel v. France* and *M.B. v. France* (ECHR, 17.12.2000) ; *Dimitrov-Kazakov v. Bulgaria* (ECHR, 10.02.2011) ; *M.M. v. the United Kingdom* (ECHR, 13.11. 2012).

29 *Leander v. Sweden, cited above*.

30 *S. and Marper v. the United Kingdom,* (ECHR, 4.12.2008).

31 Idem § § 9-12.

32 Idem § § 95-117.

from the nationwide database.[33] Moreover, the risk of stigmatization was of particular concern, with persons who had not been convicted of any offense and were entitled to the presumption of innocence finding themselves treated in the same way as convicted persons.

The second case, *Khelili v. Switzerland*,[34] concerned classifying the applicant as a "prostitute" in the Geneva police computer database for five years after a police search during which police officers found business card mentioning that she was looking for men to meet. Following that classification, Ms. Khelili requested multiple times that the mention be removed from the police database but with no results.

In its ruling, the Court highlighted that the term "prostitute," which still appeared in all criminal files related to Ms. Khelili even though she regularly requested that the term be removed, could be harmful to her reputation and could also make her daily life more difficult given that the information could be transmitted to authorities. The Court therefore concluded that maintaining this personal information in the police database for several years was neither justified nor necessary in a democratic society and in fact violated Ms. Khelili's right to private life.[35]

Thirdly, in the case of *M.K. v. France*[36] the applicant, who had been the subject of two investigations concerning book theft—which ended in one case with his acquittal and in the other with a decision not to prosecute—complained of the fact that his data had been retained on a database by the French authorities. Specifically, he had been fingerprinted and photographed, and his personal data were stored on the police database, including his name, his father's name, his mother's name, his date and place of birth, and the offense that was being investigated. The applicant's request to have his private data deleted from the police database was rejected on the grounds that he was a suspect in an investigation and that the decision not to charge him was not grounds for deletion.

The Court considered that retaining the data in question had amounted to disproportionate interference with the applicant's right to respect for his private life, on the grounds that the storage of the private data of an innocent citizen on the police

33 Idem § 119.

34 *Khelili v. Switzerland*, (ECHR, 18.10.2011).

35 *Idem*, §§ 63-70.

36 *M.K. v. France*, (ECHR, 18.04.2013).

database for 25 years was not "necessary in a democratic society." The Court added that the judicial process to have the private data deleted was a "deceptive guarantee".[37]

The fourth case is *Brunet v. France*[38], in which the applicant complained in particular of interference with his private life as a result of being added to a police database—including information from investigation reports that listed the individuals implicated and the victims—after criminal proceedings against him had ended.

The Court held that there had been a violation of Article 8 (right to respect for private life) of the Convention, finding that the French state had overstepped its discretion to decide ("margin of appreciation") on such matters: The retention could be regarded as a disproportionate breach of the applicant's right to respect for his private life and was not necessary in a democratic society.

The Court considered in particular that the applicant had not had a real possibility of seeking the deletion from the database of the information concerning him and that the length of retention of that data, 20 years, could be construed to be if not indefinite then at least to a norm rather than to a maximum limit.[39]

Finally, the landmark ruling of the Court of Justice of the European Union (CJEU), *Digital Rights v. Ireland*[40] should be mentioned. Charged with giving a preliminary ruling on the validity of Directive 2006/24/CE, the CJEU held that the directive that mandated the retention of communications data by communications providers for law-enforcement purposes was incompatible with the right to privacy. The essence of the Court's reasoning rests on its finding that "(…) data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."[41] Noting that by allowing untargeted retention measures, the CJEU found that the data retention directive "affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained

37 *Idem*, § 44.

38 *Brunet v. France*, (ECHR, 18.09.2014).

39 *Idem*, § 43.

40 CJEU Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd and Seitlinger and others*, 8.03.2014, §65-68.

41 *Idem*, § 27.

being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy."[42]

Crucially, the CJEU ruled that the important objective of investigating serious crime did not in itself justify data retention. This was motivated by the broad scope of the directive as well as the lack of sufficient safeguards regarding the data retention period, the categories of data to be retained, and the absence of obligations to destroy the data or to retain the data within the EU only.

It should be pointed out that the legality of the EU's data retention directive has been assessed in the specific context of data retention for law-enforcement purposes. This judgment is of high importance because it strengthened data protection in this area by rejecting compulsory, suspicionless, untargeted data retention.

3. Switzerland

3.1. Legal Framework

The right to privacy as enshrined in Article 13 (2) of the Federal Constitution of the Swiss Confederation[43] states that "every person has the right to be protected against the misuse of their personal data." This right includes the right to self-determination with respect to personal data. According to the case-law of the Federal Court, collecting, retaining, and processing identification data infringe on the right to respect for private life.[44] In its recent findings, the Federal Court confirms that "the retention of personal data in criminal investigation files constitutes at least a virtual infringement of the concerned person's privacy, whose protection is guaranteed under Articles 8 ECHR and 13 Cst.[45] In order to be admissible, such infringement must have a legal basis justified by a public interest or the protection of a fundamental right of another individual and must be proportionate to the aim pursued according to Article 36 Cst.[46]

42 *Idem*, § 58.

43 Federal Constitution of the Swiss Confederation of 18 April 1999, RS. 101.

44 ATF 120 Ia 147 para. 2a; JdT 1996 IV 61.

45 ATF 126 I 7 para. 2a ; ATF 138 I 256, para. 4 ; TF 1C_51/2008, para. 3.1.

46 TF 1C_363/2014, para.2

With regard to databases, "the retention of personal data in judicial police files pursues legitimate aims relating to the prevention of disorder or crime and the retention of data relating to a convicted person on the grounds that the person could be re-offend complies with the principle of proportionality."[47] However, this is not the case for retaining personal data relating to criminal proceedings terminated by a final disqualification on grounds of law, acquittal, or withdrawal of a complaint.[48]

Thus, Article 13 (2) Cst. protects individuals against abusive use of their personal data, especially those data related to judicial procedures that would undermine their social consideration.[49]

With regard to the Federal Data Protection Act (FDPA),[50] the scope of federal (and also cantonal) legislation on data protection does not extend to the processing of personal data in the context of pending criminal proceedings, including proceedings that require international legal assistance. [51] Therefore, this legislation does not apply to data that the police collect for judicial inquiry under the direction of a criminal judicial authority.[52] In such cases, data processing is governed by the specific provisions of the Swiss Criminal Procedure Code (CPC)[53] to protect the persons involved in the proceedings.

From the moment a criminal proceeding begins until it ends, specific provisions set out in Section Eight of the Swiss Criminal Procedure Code on data processing apply. Personal data are "all information relating to an identified or identifiable person."[54] Article 95 CPC addresses obtaining personal data, and it states in par. 1 that "Personal data must be obtained from the person concerned or with that person's knowledge unless the proceedings would be otherwise be prejudiced or unreasonable inconvenience or expense would be incurred." That is, it is in the nature of law enforcement that information is collected without the knowledge of those concerned

47 *Khelili*, cited above, § 66

48 TF 1P.46 / 2001 of 2.03.2001 para. 2a, 2b and 2c.

49 ATF 137 I 167 para. 3.2 ; 135 I 198 para.3.1. ; TF 2P.83/2005 para.2.1.

50 Federal Act on Data Protection (FADP), 19.06.1992, R.S. 235.1.

51 RJJ 1999, p. 117, para. 1b, p. 121 and 122.

52 Frédéric Gisler, La coopération policière internationale de la Suisse en matière de lutte contre la criminalité organisée, Schultess, 2009, p. 86.

53 Swiss Criminal Procedure Code of 5 October 2007, RS 312.

54 Article 3 FADP lit. a.

and must be collected for criminal offenses.[55] This leads to the requirement of subsequent information as provided for by Article 95 par. 2 CPC: "If personal data is obtained without the knowledge of the person concerned, that person must be notified thereof immediately. Where overriding public or private interests so require, notification may be dispensed with or postponed." Thus, if the information has been collected without the knowledge of those concerned, which is often the case for criminal offenses, Article 95 par. 2 CPC requires that the concerned person be notified immediately.

Regarding the period following the conclusion of the proceedings, Article 99 CPC provides that "The processing of personal data, procedures, and legal protection are governed by the provisions of federal and cantonal data protection law." The storage period for personal data after conclusion of proceedings is governed by Article 103 CPC: "The case documents must be preserved at least until conclusion of the time limits for prosecution and for the execution of the sentence have expired." Retention and use of identifying documents are further regulated under Article 261 CPC, which allows retention for a maximum period of 10 years if there is a re-offense risk.

The situation differs slightly with respect to retaining personal data in police files over a criminal procedure. Pursuant to Article 18 of the Geneva Police Act, "Police officers can undergo identification measures such as taking photographs or fingerprints of persons if their identity is in doubt and cannot be established by any other means," and "unless the law authorizes conservation for the needs of another procedure, photographic, fingerprint, or another collected data is destroyed as soon as the identity of the person concerned is established."[56]

Regarding the police records, Article 1 of the Information Act and Police records issuing certificates of good life and morals in Geneva states that "The police organize and manage folders and files related to the tasks incumbent upon them, thus can process sensitive personal data and establish personality profiles for the prevention or prosecution of crimes." The storage period is again determined under the provisions of FDPA.

55 Daniela Brüschweiler, Kommentar zur Schweizerischen Strafprozessordnung, 2014, at 457.

56 Loi sur la Police (Lpol), 9.9.2014, F 105.

3.2. Case Law

In its recent finding of November 26, 2015, the Federal Court ruled about the legality of retaining personal data after proceedings are discontinued.[57] The appeal was directed against a decision on a request for the deletion of data entered in a criminal investigation file, and the facts can be summarized as follows: A complaint was filed against A. for fraud and forgery in 2012, and the Public Prosecutor of the Republic and Canton of Geneva ordered the discontinuation of the proceedings in January 2014. In April 2014, A. requested the cancellation of data entries in connection with the criminal proceedings filed against him. By decision of June 2014, the Head of Police of the Republic and Canton of Geneva proceeded to cancel some documents but refused to withdraw other data because the infringements in question concerned serious events occurred less than five years previously and that the proceedings could very likely resume in the event of the discovery of new evidence or facts.

The Federal Court admitted that the police retained personal data in their files for their potential utility in preventing or prosecuting crimes.[58] That is, the legitimate aim was to allow for identifying the perpetrators of serious crimes and preventing disorder or crime. Nonetheless, the Federal Court argued that the storage of personal data in police records should comply with the proportionality requirement where security must be balanced against the seriousness of the interference with an applicant's right to respect for his or her private life[59].

In this specific case, the Federal Court held that the fact that the police records did not contain the ranking order of the prosecution contravened the requirement of completeness as required by Article 36 para. 1 of the Geneva Data Protection Act.[60] Furthermore, the likelihood that the data could be used for future investigations was purely theoretical and the fact that the concerned person was never convicted or prosecuted beforehand led the Federal Court to conclude that this storage was not justified. [61]

57 TF 1C_307/2015. see also, ATA/636/2016 (26.07.2016, Geneva Court of Justice)

58 Article 1 para. 3 of the Geneva Information Act and Police Records Issuing Certification of Good Life and Morals (la loi genevoise sur les renseignements et les dossiers de police et la délivrance des certificats de bonne vie et moeurs) (LCBVM; RS/GE F 1 25).

59 TF 1C_307/2015, para. 2.

60 Loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD), 5.10.2001, A 208.

61 See also, Ursula Uttinger, Öffentliches Interesse an Polizeidaten höher als Interessen der betroffenen Person, in: Commentaire de jurisprudence numérique publié le 15 août 2012.

4. Turkey

4.1. Legal Framework

The right to privacy and the right to data protection are enshrined in Article 20 of the Constitution of the Republic of Turkey (Cst.)[62]. Regarding personal data, a constitutional guarantee of protection against unlawful use was introduced in 2010, in Article 20, paragraph 3 Cst.: "Everyone has the right to request the protection of his/her personal data," including being informed of, having access to, and requesting the correction and deletion of personal data as well as being informed whether these data are being used consistently with the purpose for their collection. Thus, under these principles, personal data can only be processed with a data subject's explicit consent or with any of the conditions envisaged by law.

With regard to Law n° 6698 on Protection of Personal Data[63], exclusions from its scope are similar to those in Swiss data protection law. Article 28 § 1 of the law excludes processing personal data outside of scope where the processing is within the scope of preventive, protective, and intelligence-related activities by public institutions and organizations who are assigned and authorized to provide national defense, national security, public safety, public order, or economic safety as well as where the processing is for criminal investigations, prosecutions, or cases performed by judicial bodies and execution offices.

One can observe a substantial difference between the two national frameworks: Swiss data protection law applies to the pre- and post-trial period, whereas the Turkish legal framework is regulated under different legislation.

With regard to identification under the Criminal Procedure Code (CPC Law n°5721,)[64] Article 81 provides that "If the committed crimes requires a maximum prison term of two years or a heavier punishment, upon the order of the public prosecutor, a picture shall be taken, measurement of the body shall be made, fingerprints or palm prints shall be taken, special marks on the body, that would enable the recognition of the suspect or the accused shall be registered; and a voice sample and a video film shall be produced as well, and inserted into the file where the interactions related to the investigations and prosecutions are kept."

62 Constitution of the Republic of Turkey, of 18 october 1982.

63 Published in Official Gazette n° 29677, 7.4.2016.

64 Law n° 5721, published in the Official Gazette n° 25673, 17.12.2004.

Nevertheless, Article 81 § 2 CPC foresees that in cases in which the time limit is exhausted for opposing a decision on no grounds for prosecution, the opposition has been overturned, the court gives a final judgment on acquittal, or a judgment is rendered on not punishing the accused and the judgment is made final, "related records shall be destroyed in the presence of the public prosecutor and this fact shall be documented." Thus, with the respect to the defense's rights, privacy is equally respected in this regulation.

However, Article 5 of Law n° 2559 on Duties and Powers of Police[65] authorizes collecting and storing fingerprints and photographs of arrested persons, and these data can be used to prevent or investigate by the courts, prosecutors, and law-enforcement bodies. If the storage can be deemed to satisfy a legitimate aim, the problematic part of this regulation remains in the fact that all data included will be erased only after 80 years except when the concerned person passes away, in which case the data will be deleted 10 years after death. The question is raised of whether such a long period can be deemed to be proportionate to the legitimate aim.

From this, it follows that cancelling the fingerprints and photographs that law enforcement authorities collect is subject to different rules: Even if the data have to be deleted in accordance with Article 81 CPC, Article 5 (4) of the Police Law allows for their storage for the purpose of preventing an offense.

4.2. Case Law

The existing dichotomy in the legal framework can also be found in the case law of the Turkish Council of State of 6 December 2010.[66] Ruling on a claimant's infringement claim of, among other matters, the right to privacy, for having had an application rejected for cancelling the registration of the claimant's fingerprints and photos following his acquittal, the Council of State held that keeping this record for identification purposes was in accordance with Law n° 2559.

Another prominent example of the constitutionality of such databases is found in a recent Ombudsman's decision of 3 December 2014.[67] In *F.D. v. Ministry of Justice*, the claimant challenged the validity of his records because he had been accused of a theft in 2009 and acquitted in 2010, but the National Judiciary Informatics System

65 As amended on 27.03.2015, published in the Official Gazette n° 2751, 04.07.1934.

66 Danistay 10 Daire 2007/4364 E.N., 2010/10458 KN of 06.12.2010.

67 Ombudsman decision *F.D. v. Ministry of Justice*, 03.12.2014.

was never rectified, and his charge was still on record by 2014. With reference to international and national legal frameworks for protecting personal data, the Ombudsman held that storage of such information for an unknown period was disproportional and undermined the private life of the claimant.[68]

5. Conclusion

To conclude, the practical implications of these distinctive legal frameworks requires an assessment with regard to trans-border flows of personal data with reference to The European Union Agency for Law Enforcement Cooperation (Europol).[69]

Europol's main purpose is the exchange of police information with a view to preventing and combating organized crime; it analyzes and makes available information it obtains from the various countries.

Switzerland and Europol concluded a cooperation agreement that came into force on March 1, 2006,[70] that enables the exchange of strategic, operative, and other specific information.[71] The cooperation agreement comprehensively covers data processing. Articles 7 to 13 govern data transmission, source and information classification, data correction and deletion, and classification or confidentiality of information. These fulfill the constitutionality requirements regarding privacy protection under Article 13 of the Swiss Constitution and Article 8 of the Convention on Human Rights.

With regard to Turkey, a cooperation agreement with Europol came into force in 2004.[72] The agreement is a strategic one, which "means an agreement allowing for the exchange of information, excluding personal data."[73] In other words, "this agreement does not authorize the transmission of data related to an identified individual or identifiable individuals."[74] A further liaison agreement was concluded

68 Following the Ombudsman's recommendation, the Ministry of Justice declared it necessary to end this practice.

69 See Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation, OJ L 135, 24.05.2016, p. 53-114.

70 Agreement between The Swiss Confederation and Europol, 24.07.2004, RO 2006, 1019.

71 Article 1 and 4 CH-Europol Agreement. The scope of this cooperation was extended on January 1, 2008, to embraces 25 areas of crime.

72 Strategic Agreement on Cooperation Between The European Police Office and the Republic of Turkey.

73 See Article 1 (g) of the Council Decision 2009/934/JHA.

74 Article 1 TR-Europol Agreement.

between Turkey and Europol in 2016 in order to enhance cooperation with Turkish law enforcement to strengthen the fight against organized crime and terrorism.

Article 1 of the "main" cooperation agreement of 2004 aims to "enhance the cooperation of the Member States of the European Union, acting through Europol and the Republic of Turkey in preventing, detecting, suppressing, and investigating serious forms of international crime within the respective competence of each Party, (…) in particular through the exchange of strategic and technical information," which are "of mutual interest."[75] Note that it is of crucial importance to specify that "this agreement does not authorize the transmission of data related to an identified individual or identifiable individuals."[76] The reasoning of such a limited scope relies on the fact that at the time of this cooperation agreement, there was not yet a specific data protection law in Turkish legislation. Or, in order to satisfy the requirement for a data exchange, the Europol Convention requires an equivalent framework that will ensure proper use and storage of personal data, and because Turkey only ratified CV n°108 in 2016, it was not possible to speak about an equivalent level of protection within the Turkish legal order. To sum up, an effective application of data protection in Turkey is required in order to enable closer cooperation with Europol, and indirectly with Switzerland, in law-enforcement cooperation.[77]

Bibliography

Brüschweiler D. in *Kommentar zur Schweizerischen Strafprozessordnung*, Donatsch A., Hansjakob T., Lieber V. Schulthess, 2014.

Claes E., Duff A., Gutwirth S., *Privacy and the Criminal Law*, Intersentia, 2006.

Hoven van Genderen R., *Cybercrime investigation and the protection of personal data and privacy,* Council of Europe Publications, 2008.

Güntürk M. S., *Türk Yüksek Mahkemeleri ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Özel Hayatın Gizliliğinin Korunması*, Seçkin, 2012.

Gisler F., *La coopération policière internationale de la Suisse en matière de lutte contre la criminalité organisée*, Schultess, 2009.

Uttinger U., "Öffentliches Interesse an Polizeidaten höher als Interessen der betroffenen Person", Commentaire de jurisprudence numérique publié le 15 août 2012.

75 Article 3 TR-Europol Agreement.

76 Article 1 TR-Europol Agreement.

77 It should be noted that at the bilateral level of data exchange between Switzerland and Turkey, the latter is not deemed to ensure an equivalent level of data protection by the former.