Global Campus Caucasus

Policy Briefs 2020

Mane Torosyan

Traffic surveillance and human rights: How can states overcome the negative impact of surveillance technologies on the individual right to respect for privacy and personal data protection?

Supported by

Table Of Contents

Traffic surveillance and human rights: How can states overcome the negative impact of surveillance technologies on the individual right to respect for privacy and personal data protection?

Mane Torosyan

EXECUTIVE SUMMARY

The crucial role of surveillance technologies for the enforcement of traffic laws and prevention of traffic accidents, as well as for the development of modern traffic management systems and regulation of traffic jams, is acknowledged widely but so far little attention has been given to human rights concerns arising from traffic surveillance. However, traffic surveillance greatly affects several individual human rights, more specifically the individual right to private life and personal data protection.

In the case of traffic surveillance, interference by a public authority can be reasonably justified with the legitimate purpose of detecting traffic law violations, an action necessary 'in a democratic society' and for 'the prevention of disorder or crime'. In this regard, human rights concerns may arise not from the very fact of video monitoring, but the recording and processing of data which may create an unlawful interference with individual human rights. In the process of traffic surveillance and further proceedings in response to traffic law violations, general principles of personal data protection may be significantly affected, specifically the requirements of personal data being 'obtained and processed *fairly* and *lawfully*', 'processed for *specified and legitimate purposes* and not used in a way incompatible with those purposes'; '*not excessive* in relation to the purposes for which they are processed'; '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'.[1] The case study of traffic law enforcement in the Republic of Armenia (RA) reveals several examples of how protection of individual human rights may be challenged through traffic law enforcement policies and procedures and offers useful lessons for mitigating the negative impact of surveillance technologies on the right to respect for private life and personal data protection.

1 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (adopted 28 January 1981) CoE European Treaty Series - No. 108 <https://rm.coe.int/1680078b37> accessed 16 April 2020; Regulation (EU) on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (adopted 27 April 2016) European Parliament and Council 2016/679 <https://gdpr-info.eu/> accessed 20 April 2020 (emphasis added).

INTRODUCTION

The crucial role of surveillance technologies for the enforcement of traffic laws and prevention of traffic accidents is acknowledged widely. Such technologies are also applied for the development of modern traffic management systems and regulation of traffic jams. Thus, mass surveillance through traffic monitoring cameras is mainly justified due to its significant input in safeguarding against and the prevention of threats to public safety and protection of public interest.

Nevertheless, little attention has been given to the human rights concerns rising from the application of traffic surveillance technologies. Along with the red-light and speed cameras, detection technologies are already applied to determine whether drivers are wearing seatbelts or using cell phones and may be used to identify drivers.[2] Such development and growing application of mass surveillance technologies raises a number of crucial questions to be answered through further research and public debate. Specifically, what is the reasonable expectation of privacy in a private vehicle and may an individual claim similar private life guarantees for the vehicle as in the case of the home? To which extent do established legal and procedural mechanisms ensure the protection of personal data and the individual right to respect for privacy while collecting, processing and using the information on the violation of traffic rules and how those mechanisms may be improved? Who are the primary and exceptional users of the information acquired through the traffic cameras and what are the purposes other than traffic law enforcement it may be used for?

This policy paper strives to answer the above-mentioned questions and studies the ways traffic surveillance technologies affect personal data protection and the individual right to respect for privacy. It also comes up with the possible public policy alternatives of mitigating the negative impact of traffic surveillance on human rights with the specific focus on public policy debate and reforms in Armenia. Finally, it provides public policy recommendations for national and local governments, human rights defenders and civil society.

PUBLIC SAFETY CASTING A SHADOW ON INDIVIDUAL HUMAN RIGHTS: NEED FOR ACTION?

Video surveillance in public and private areas has attracted the attention of human rights defenders, national and local authorities, international development agencies, civil society organisations and media due to its potential harm to individual human rights. While there is a wide acknowledgement that an individual's private and family life, their home and correspondence should be protected from an unlawful interference, the debate on the nature and scale of privacy that individuals may reasonably expect in public places and the ways video surveillance in public places infringes the individual rights to respect for privacy and personal data protection is still ongoing. Moreover, the implication of traffic monitoring cameras has been mainly justified due to its significant input to public safety and prevention of disorder, thus casting a shadow on the concerns over any reasonable expectation of 'privacy in open roads'.[3] This fact, however, should not undermine states' obligations to set necessary policy and procedural mechanisms protecting individuals from unlawful and/or disproportionate interference with their private lives when processing and recording their personal data.

The national legislation in Armenia does not sufficiently regulate video surveillance in public places. The protection of personal data is stated at the constitutional level and further specified by the RA Law on Personal Data Protection and other legal acts. Further, the RA Law on Police and the RA Law on Administrative Proceedings in Response to Violations of Traffic Rules Detected through Traffic Monitoring Cameras set admin-

2 European Transport Safety Council (ETSC), 'New Spanish safety cameras to detect seat belt use' (*ETSC*, 4 April 2017) <https://etsc.eu/new-spanish-safety-cameras-to-detect-seat-belt-use/> accessed 23 March 2020; Li Tao, 'Shenzhen police can now identify drivers using facial recognition surveillance cameras' (*South China Morning Post*, 25 April 2018) <https://www.scmp.com/tech/china-tech/article/2143137/shenzhen-police-can-now-identify-drivers-using-facial-recognition> accessed 21 March 2020.

3 Dorothy J Glancy, 'Privacy on Open Roads' (2004) 30 Ohio Northern University Law Review 295.

istrative procedures for processing, recording and storing data on traffic law violations, ensuring some crucial safeguards for the personal data protection in this process. However, disproportionate collection and processing of personal data seem still possible under the established legislative framework and should be addressed carefully. Moreover, the National Assembly of Armenia has recently amended the existing RA Law on Administrative Proceedings in Response to Violations of Traffic Rules, giving the general public the right to record traffic violations through a mobile application. The law does not yet specify the types of violations that may be recorded by the general public and the mechanisms through which personal data protection and the right to respect for privacy will be ensured. Hence, this policy paper is a systematised effort to discuss the possible human rights concerns of the reform and perspectives to address them. The Armenian case study and relevant recommendations may also be helpful to human rights practitioners engaged in policy analysis, formation and advocacy in other countries.

IN WHICH WAY ARE INDIVIDUAL HUMAN RIGHTS AFFECTED BY TRAFFIC SURVEILLANCE?

In March 2007, the European Commission for Democracy through Law (Venice Commission) published an opinion on video surveillance in public places by public authorities and the protection of human rights.[4] Despite the scope of the study not dealing 'with video systems that automatically recognize license plates of moving vehicles, or systems that monitor traffic flow and catch people violating traffic laws', some of the mentioned concerns and recommendations can be still useful for the purposes of this policy paper.

The Venice Commission states that surveillance in public places affects several individual human rights, more specifically the individual right to privacy, personal data protection and the right to free movement. The latter concerns not only the right to move freely, but also the right to move without constantly being traced.

SHOULD THE RIGHT TO PRIVACY BE PROTECTED ONLY IN PRIVATE AREAS? WHAT ABOUT OPEN ROADS?

At the international level, the right to privacy is protected by the International Covenant on Civil and Political Rights[5] (ICCPR) and at the regional level by the European Convention of Human Rights[6] (ECHR). Article 17 of the ICCPR states that 'no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation'. Article 8 of the ECHR further specifies the conditions under which the individual right to respect for privacy may be restricted, stating that interference by a public authority shall be only:

> in accordance with the law and necessary in a democratic society in the interest of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

In the meaning of the ECHR, the concept of 'private life' is considered to be a broad term, which embraces (I) a person's physical, psychological or moral integrity, (II) his/her privacy and (III) his/her identity and autonomy. Video surveillance, systematic collection and storage of private data by public authorities also fall within the scope of 'private life'.[7] The European Court

4 European Commission for Democracy through Law (Venice Commission), 'Opinion on video surveillance in public places by public authorities and the protection of human rights' (Council of Europe Study No 404 / 2006 CDL-AD(2007)014).

5 International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx> accessed 12 April 2020.

6 Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) (adopted 4 November 1950, entered into force 3 September 1953) <https://www.echr.coe.int/Documents/Convention_ENG.pdf> accessed 12 April 2020.

7 Council of Europe/ European Court of Human Rights, 'Guide on Article 8 of the European Convention on Human Rights. Right to respect for private and family life, home and correspondence' (Council of Europe/European Court

of Human Rights (ECHR) states that a person's reasonable expectations for privacy while being engaged in the activities that may be recorded or reported in a public manner can be a significant, although not necessarily conclusive, factor:

> A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain.[8]

The ECHR has also found that video surveillance of public places where the visual data are recorded, stored and disclosed to the public falls under article 8. In *Peck v the United Kingdom*,[9] for example, the disclosure of video footage of the applicant's suicide attempt to the media was found to be a serious interference with the applicant's private life, notwithstanding that he was in a public place at the time.

In the case of traffic surveillance, interference by a public authority, i.e. implication of traffic monitoring cameras, can be reasonably justified with the legitimate purpose of detecting traffic law violations, an action necessary 'in a democratic society' and for 'the prevention of disorder or crime' (as prescribed in the ECHR). In this regard, human rights concerns may arise not from the very fact of video monitoring, but the recording and processing of data which may create an unlawful interference with the right to respect for privacy and personal data protection.[10] Thus, more attention should be given to the proportionality of state actions undertaken for traffic law enforcement to exclude recording and processing of data not necessary for that legitimate purpose,[11] as well as potential infringement of personal data protection principles.

WHAT ABOUT PROCESSING AND RECORDING DATA ON TRAFFIC LAW VIOLATIONS?

Traffic surveillance touches personal data protection during the processing and recording of the collected data. Protection of personal data falls within the scope of private life in the meaning of article 8 of the ECHR. Video surveillance falls also under the scope of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[12] More thoroughly, personal data protection has been addressed in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation (GDPR)).[13]

The above mentioned documents elaborate identical principles relating to processing of personal data, stating that personal data should be: a) obtained and processed fairly and lawfully; b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; c) adequate, relevant and not excessive in relation to the purposes for which they are processed; d) accurate and, where necessary, kept up to date; e) kept in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are processed. GDPR sets addi-

of Human Rights 31 August 2019) <https://bit.ly/3dKn0OI> accessed 14 April 2020.

8 Ibid.

9 *Peck v UK* app. no. 00044647/98 (EHtCR, 28 January 2003).

10 European Commission for Democracy through Law (Venice Commission), 'Opinion on video surveillance in public places by public authorities and the protection of human rights' (Council of Europe Study No 404 / 2006 CDL-AD(2007)014).

11 Expert interview with Ara Khzmalyan, co-founder at ADWISE Business and Legal Consulting (20 April 2020).

12 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (adopted 28 January 1981) CoE European Treaty Series - No. 108 <https://rm.coe.int/1680078b37> accessed 16 April 2020.

13 Regulation (EU) on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (adopted 27 April 2016) European Parliament and Council 2016/679 < https://gdpr-info.eu/> accessed 20 April 2020.

tional principles, i.e. transparency of the processing in relation to the data subject and appropriate security of the personal data.

In Armenia, the protection of personal data is stated at the constitutional level and further specified by the RA Law on Personal Data Protection and other legal acts. On 9 May 2012, Armenia ratified the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the general principles of the personal data protection specified by the RA Law on Personal Data Protection is in compliance with international law. Further, GDPR is considered to set international standards on personal data protection and Armenia also seeks to comply with those standards.[14]

WHAT MAY GO WRONG? LESSONS LEARNT FROM THE ARMENIAN CASE STUDY

A number of important human rights concerns may arise in the process of traffic surveillance and further administrative proceedings, particularly in regard with the requirements of personal data being 'obtained and processed fairly and lawfully', 'processed for specified and legitimate purposes and not used in a way incompatible with those purposes'; 'not excessive in relation to the purposes for which they are processed'; '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'. And states can undertake different measures to address those concerns and mitigate the negative impact of surveillance technologies on the individual rights to respect for privacy and personal data protection. Here are some useful lessons learnt from the Armenian case study of traffic law enforcement.

Lesson 1: Data minimisation

Video surveillance of public parking places has made it possible to identify not only vehicles that have violated parking rules, but also the surrounding buildings, vehicles and people. Thus, application of traffic monitoring cameras has not been strictly restricted to the necessity of detecting traffic law violations. The issue has invited the attention of the Agency for Protection of Personal Data of RA Ministry of Justice,[15] human right defenders and media. It has been addressed by a recent amendment to the RA Law on Administrative Proceedings in Response to Violations of Traffic Rules Detected through Traffic Monitoring Cameras, according to which before notifying that a traffic law violation has occurred, the figures of people in the relevant photo or video are obscured. Overall, one of the most effective technical solutions for 'data minimisation' is the low quality of the photo/video of a traffic violation ticket which makes it possible to identify only the licence plate of the vehicle through a 'zoom' function.[16]

Lesson 2: Issuing traffic tickets

Armenia applies one of the most common models of issuing red light and speed camera tickets: the tickets are issued to the owner of the car, not the actual driver, unless the owner has registered another person as the vehicle user. Hence, the tickets are sent to the postal address of the owner making personal data disclosure to third parties possible.[17]

The 'car owner is responsible' model is grounded on the overall concept and scope of rights and responsibilities of the property owner as prescribed by international law and national legislative acts.[18] The RA Constitution guarantees everyone's right to possess, use and dispose of legally acquired property at his or her discretion.[19]

14 Expert interview with Hayk Avetyan, lawyer at Leader and Co (15 April 2020).
15 Expert interview Gevorg Hayrapetyan, head of Agency for Protection of Personal Data of RA Ministry of Justice (7 April 2020).
16 Expert interview with Ara Khzmalyan (n 11).
17 RA Code on Administrative Offences (adopted 6 December 1985, entered into force 1 June 1986) <https://www.arlis.am/DocumentView.aspx?docid=73129> accessed 4 May 2020.
18 Expert interview with Sergey Ghazinyan, adviser to RA human rights defender (21 May 2020).
19 Constitution of the Republic of Armenia (adopted 5 July 1995, amended 2005 and 6 December 2015) <https://www.president.am/en/constitution-2015> art 60.1 accessed 5 May 2020.

The owner has the right, at their own discretion, to make any action in regard to their property, including alienating the property to the ownership of other persons, transferring to them the rights of possession, use and disposition of the property, if such action does contradict the law and does not violate the rights and legitimate interests of other persons.[20] According to RA Constitutional Court N1282 decision, as soon as a violation of traffic rules violates the rights and legitimate interests of other persons, the car owner is responsible for passing the right of use of the vehicle to the person who will not violate traffic rules. In this sense, the RA Constitutional Court states that for the purposes of preventing vehicle owners from not fulfilling their responsibilities arising from exercise of their rights of ownership, as well as ensuring the inevitability of the offender's responsibility, the vehicle owner takes the responsibility of a traffic law violation unless they provide evidence of another person having conducted the administrative offence.[21]

It should be noted, that according to some specialists, in the case of a traffic law violation the driver cannot reasonably expect sufficient level of privacy, as the disclosure of the personal data is the result of their unlawful action.[22] It is also about the technical equipment of the traffic surveillance system: cameras do not always allow identification of the driver, e.g. traffic violation photos may be taken from the back of the car.[23]

Nevertheless, some measures can be undertaken to minimise the risk of disclosing personal data to third parties, such as sending administrative acts to personal emails of the administrative act holders and/or strictly ensuring that a printed notification is received directly by the addressee to prevent personal data disclosure to family members. Another example of preventive measures is the recently amended RA road police procedural mechanism, according to which the police do not make a phone call to the car owner while removing their vehicle in order not to disclose the location of the actual driver.[24]

Lesson 3: Publishing data acquired through traffic cameras

In 2017, RA Road Police published video footage taken by a policeman's mobile camera where a person refused to comply with the lawful demand of the policeman to present the legal documents and drove away. In response to the disclosure, an administrative proceeding was initiated by the Agency for Protection of Personal Data of RA Ministry of Justice. As a conclusion of the proceeding, it was determined that video publishing contradicted the principle of lawfulness stated in article 6 of the RA Constitution, i.e. that 'state and local self-government bodies and officials shall be entitled to perform only such actions for which they are authorised under the Constitution or laws'.[25] Despite the official response of the road police that the video was published with the consent of the data subject, there was no legal foundation of providing such consent. The video has been removed and current legislation directly prohibits publishing the photos and videos acquired through police surveillance technologies.[26]

Lesson 4: Storing and destroying data

In 2018, the RA Law on Police was amended, inter alia, to set a certain period for maintenance of photos and videos acquired through police surveillance cameras. According to the amended law,

20 RA Civil Code (adopted 5 May 1998, entered into force 1 January 1999) <https://www.arlis.am/documentview.aspx?docid=141434> accessed 5 May, 2020.

21 RA Constitutional Court N1282 Decision on the Case of Lilit Museyan's claim on determining compliance of Section 3 of Article 32 of RA Law on Administrative Offences to RA Constitution (adopted 21 June 2016, entered into force 21 June 2016) <https://www.arlis.am/DocumentView.aspx?docID=106908> accessed 12 May 2020.

22 Expert interviews with Gevorg Hayrapetyan (n 15), Hayk Avetyan (n 14), Ara Khzmalyan (n 11).

23 Expert interview with Sergey Ghazinyan (n 18).

24 Ibid.

25 Constitution (n 19).

26 RA Law on Police (adopted 16 April 2001, entered into force 10 June 2001) <https://www.arlis.am/DocumentView.aspx?docid=137948> art 22 accessed 10 May 2020.

data should be removed after seven days of being recording by police officers' mobile cameras, unless (I) crime or public disorder, including a traffic law violation, has been detected, (II) the actions of the police officers have been appealed or (III) persons have applied to the police for the protection of their rights and legitimate interests.[27] In the above-mentioned cases, the period for data storage is determined by the head of the RA police territorial unit or the head of RA road police.[28] Given such regulation, concerns may arise in regard to the compliance with the principle of 'storage limitation', as the exact period of data preservation on traffic law violations is not prescribed by the law. In the case of fixed traffic cameras, videos are kept for 48 hours, after which they are automatically removed from the server due to technical memory limits. The video excerpts detecting traffic law violations are stored and kept for one year if the administrative proceeding is finished and for an uncertain period if the decision on issuing a traffic ticket has been appealed. Despite the fact that timeframes for storing and destroying data acquired through fixed traffic cameras seem reasonable for traffic law enforcement, the transparency of those measures in relation to data subjects are still insufficient to comply with another key principle of personal data protection.

Lesson to be learnt: Citizens detecting traffic law violations

Finally, in 2019 the National Assembly of RA amended the existing RA Law on Administrative Proceedings in Response to Violations of Traffic Rules, giving the general public the right to record traffic violations through a mobile application. The law does not yet specify the types of violations that may be recorded by the general public and the mechanisms through which personal data protection and the right to respect for privacy will be ensured. Hence, there are number of human rights concerns that should be elaborated.

The national legislation does not prohibit the public from recording crimes and public disorder and providing relevant information to law enforcement bodies.[29] In this sense, the main human rights concerns may arise not from the fact of using a mobile application to report on traffic law violations but the technical design of the application allowing preservation of the photo/video footage in a mobile device. The violation should be recorded through a mobile application and directly submitted to the road police with no saving option.[30] The other concern that should be taken carefully is the appropriate technical security of collected data.[31] Finally, given the public interest in the proposed amendment, frequently clashing advantages and disadvantages, there is an obvious need to design and implement appropriate policy communication ensuring public participation, inter alia, in policy reforms on personal data protection mechanisms. According to a RA Road Police representative, the proposed RA government decision draft will be soon available for public discussion and envisages the above-mentioned technical design of the mobile application, as well as procedures to prevent potential misuse of the application by setting limits on the number of traffic law violations that may be reported in a certain period of time from the same person and on misconduct of the same vehicle, as well as denying access to the system for users who have submitted information other than traffic law violation.[32]

POLICY RECOMMENDATIONS

Below, some general recommendations are provided for national and local authorities, as well as human rights practitioners engaged in policy analysis, formation and advocacy, to mitigate the negative impact of traffic surveillance on the protection of the individual right to privacy and personal data:

27 Ibid.
28 Ibid.
29 Expert interview with Gevorg Hayrapetyan (n 15).
30 Ibid.
31 Expert interview with Ara Khzmalyan (n 11).
32 Expert interview with Hayk Vardanyan, head of Law Department of RA Road Police(29 April 2020).

- The implication of traffic monitoring cameras should be sufficiently regulated by national legislations, allowing their exceptional use to be for the purposes of detecting traffic law violations and excluding the processing and storage of the data that are not necessary for detecting and reporting traffic law violations; safeguards should be established against constant video surveillance and data collection;
- People should be notified of their being watched or at least monitoring cameras should be obvious, which would also serve for prevention purposes;
- People should have access to the data collected about them and be informed about the collection, processing and use of those data. Such access may be restricted, if it would endanger the prevention or prosecution of crimes, the protection of safety or the (privacy) rights of others;
- The collected data should be preserved in a form which permits identification of the data subjects for no longer than is required for the purposes for which this data is stored. Data maintaining and destroying procedures should be clearly defined by legislation and communicated with general public and human rights practitioners;
- Publication of the photos and videos acquired through traffic cameras, as well as their usage by public authorities for the purposes other than traffic law enforcement, should be strictly restricted by national legislations; sufficient measures should also be undertaken to prevent the disclosure of personal data to third parties in the process of issuing traffic tickets;
- By giving the general public the right to record traffic violations through a mobile application, necessary technical measures should be undertaken not to provide an opportunity to save the photo/video footage in a mobile device and photo/video recording should directly submitted to the road police; the appropriate technical security of data should be ensured;the proposed mechanisms of personal data protection should be effectively communicated with general public and human rights practitioners.

REFERENCES

Alghnam S and others, 'The effectiveness of introducing detection cameras on compliance with mobile phone and seatbelt laws: a before-after study among drivers in Riyadh, Saudi Arabia'(2018) 5 Injury Epidemiology 31 <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6081868/> accessed 21 March 2020

Constitution of the Republic of Armenia (adopted 5 July 1995, amended 2005 and 6 December 2015) <https://www.president.am/en/constitution-2015> accessed 5 May 2020

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (adopted 4 November 1950, entered into force 3 September 1953) <https://www.echr.coe.int/Documents/Convention_ENG.pdf> accessed 12 April 2020

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (adopted 28 January 1981) CoE European Treaty Series - No. 108 <https://rm.coe.int/1680078b37> accessed 16 April 2020;

Council of Europe/European Court of Human Rights, 'Guide on Article 8 of the European Convention on Human Rights. Right to respect for private and family life, home and correspondence' (Council of Europe/European Court of Human Rights 31 August 2019) <https://bit.ly/3dKn0OI> accessed 14 April 2020

Eurasia Partnership Foundation (EPF), 'Protection of human rights: Video surveillance in Armenia' (*EPF*, 13 September 2017) <https://epfarmenia.am/hy/node/701> accessed 15 March 2020

European Commission for Democracy through Law (Venice Commission), 'Opinion on video surveillance in public places by public authorities and the protection of human rights' (Council of Europe Study No 404 / 2006 CDL-AD(2007)014)

European Transport Safety Council (ETSC), 'New Spanish safety cameras to detect seat belt use' (*ETSC*, 4 April 2017) <https://etsc.eu/new-spanish-safety-cameras-to-detect-seat-belt-use/> accessed 23 March 2020

Glancy DJ, 'Privacy on Open Roads' (2004) 30 Ohio Northern University Law Review 295

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx> accessed 12 April 2020

Li T, 'Shenzhen police can now identify drivers using facial recognition surveillance cameras' (*South China Morning Post*, 25 April 2018) <https://www.scmp.com/tech/china-tech/article/2143137/shenzhen-police-can-now-identify-drivers-using-facial-recognition> accessed 21 March 2020

RA Civil Code (adopted 5 May 1998, entered into force 1 January 1999) <https://www.arlis.am/documentview.aspx?docid=141434> accessed 5 May, 2020

RA Code on Administrative Offences (adopted 6 December 1985, entered into force 1 June 1986) <https://www.arlis.am/DocumentView.aspx?docid=73129> accessed 4 May 2020

RA Constitutional Court N1282 Decision on the Case of Lilit Museyan's claim on determining compliance of Section 3 of Article 32 of RA Law on Administrative Offences to RA Constitution (adopted 21 June 2016, entered into force 21 June 2016) <https://www.arlis.am/DocumentView.aspx?docID=106908> accessed 12 May 2020

RA Law on Administrative Proceedings in Response to Violations of Traffic Rules (adopted 26 December 2008, entered into force 1 January 2009) <https://www.arlis.am/DocumentView.aspx?docid=138993> accessed 14 May, 2020

RA Law on Personal Data Protection (adopted 18 May 2015 , entered into force 1 July 2015) <https://www.arlis.am/DocumentView.aspx?docid=132745> accessed 25 April, 2020)

RA Law on Police (adopted 16 April 2001, entered into force 10 June 2001) <https://www.arlis.am/DocumentView.aspx?docid=137948> art 22 accessed 10 May 2020

Regulation (EU) on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (adopted 27 April 2016) European Parliament and Council 2016/679 <https://gdpr-info.eu/> accessed 20 April 2020

Sayadyan L, 'Attention: You are monitored by video surveillance' (*trace*, 8 July 2016) <https://hetq.am/hy/article/69060> accessed 5 April 2020

Participants of expert interviews

Avetyan H, lawyer at Leader and Co (15 April 2020)

Ghazinyan S, adviser to RA human rights defender (21 May 2020)

Hayrapetyan G, head of Agency for Protection of Personal Data of RA Ministry of Justice (7 April 2020)

Karapetyan Z, deputy head of Department for Investigation of Offenses Revealed by Technical Devices of RA Road Police (29 April 2020)

Khzmalyan A, co-founder at ADWISE Business and Legal Consulting (20 April 2020)

Vardanyan H, head of Law Department of RA Road Police (29 April 2020)

Global Campus of Human Rights

Monastery of San Nicolò
Riviera San Nicolò, 26
I-30126 Venice Lido (Italy)

gchumanrights.org

Global Campus of Human Rights

The Global Campus of Human Rights is a unique network of more than one hundred participating universities around the world, seeking to advance human rights and democracy through regional and global cooperation for education and research. This global network is promoted through seven Regional Programmes which are based in Venice for Europe, in Sarajevo/Bologna for South East Europe, in Yerevan for the Caucasus, in Pretoria for Africa, in Bangkok for Asia-Pacific, in Buenos Aires for Latin America and the Caribbean, and in Beirut for the Arab World.

The Global Campus Policy Observatory

The Observatory is a 'virtual hub' which comprehends a team of seven researches from the regional programmes to produce, publish and publicly present seven different policy analyses in form of policy briefs, with the aim of making of each regional programme a solid focal point for policy expert advisory in human rights issues.

This document has been produced with the financial assistance of the European Union and as part of the Global Campus of Human Rights. The contents of this document are the sole responsibility of the authors and can under no circumstances be regarded as reflecting the position of the European Union or of Global Campus of Human Rights.