UDK 343.123:004.8]:342.738
Preliminary communication

DATA PROTECTION, PRIVACY AND SECURITY IN THE CONTEXT OF ARTIFICIAL INTELLIGENCE AND CONVENTIONAL METHODS FOR LAW ENFORCEMENT

Simona Strmečki, M.Sc., Senior Lecturer
University of Applied Sciences in Criminal Investigation
and Public Security
Ministry of the Interior
Avenija Gojka Šuška 1, Zagreb, Croatia
sstrmecki@fkz.hr

Silvija Pejaković-Đipić, PhD, Lecturer
University of Applied Sciences in Criminal Investigation
and Public Security
Ministry of the Interior
Avenija Gojka Šuška 1, Zagreb, Croatia
spdjipic@fkz.hr

ABSTRACT

Unlike conventional methods and technologies of collecting, processing and analysing the personal data of natural persons as part of law enforcement activities, the broader use of different artificial intelligence methods brings into focus the need for specific rules regulating the application of various artificial intelligence methods to protect two independent fundamental rights as regulated by EU Charter of Fundamental Rights, Art. 7 and 8 – data protection and privacy.

Privacy, the protection of personal data and the security of their processing and transmission within law enforcement activities, whether it is non-automated, partially or fully automated, is prescribed by Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. When considering personal data protection in the context of Directive 2016/680 it is referred to the protection of information on the confirmed identity of a natural person (data protection) and the protection of all information by which identity can be confirmed

(privacy). Thus, this information should not be part of the defined personal data category, and all methods and technologies that can be used for direct and indirect confirmation of the identity of a natural person should be taken into account.

The paper aims to determine whether there is relationship between privacy and security and whether there are differences in the personal data collection, processing and analysis methods by law enforcement authorities, when used methods are conventional or artificial intelligence.

The first hypothesis emphasises causality between privacy and security when collecting, processing and analysing their personal data by conventional methods and artificial intelligence methods for law enforcement purposes. The second hypothesis implies a statistically significant difference in making personal data available to law-enforcement bodies in cases they are collected, processed and analysed by conventional methods and in cases they are collected, processed or analysed by artificial intelligence methods.

The methods used are: descriptive method for describing the process of collecting, processing and analysing personal data in law enforcement activities, as well as for describing the differences between conventional and artificial intelligence methods and evaluating hypotheses; induction for creating hypothesis; deduction for observing specific relations; content analysis and synthesis in the evaluation phase; survey method; statistical and comparative method in the testing phase and for determining the compliance with the hypotheses.

***Keywords**: artificial intelligence methods, data protection, law enforcement, privacy, security*

1. INTRODUCTION

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, and repealing Directive 95/46/EC (General Data Protection Regulation) determines that "the right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity." *Rodotà* stated that the right to personal data protection could be described as a result of widening of the right to privacy.[1] Similar to that, *Fuster* states that data protection could be interpreted as an ele-

[1] Rodotà, S., *Data Protection as a Fundamental Right*. In: Gutwirth, S., Poullet, Y., De Hert, P., de Terwangne, C., Nouwt, S. (eds) Reinventing Data Protection? Springer, Dordrecht, 2009, p- 79 [https://doi.org/10.1007/978-1-4020-9498-9_3], Accessed 7 July 2023.

ment of privacy, even in the context of EU Charter of Fundamental Rights.[2] This research takes into account that data protection could be interpreted as an element of privacy. Therefore, the personal data were the basis of the survey research in which respondents had to decide whether or not to give it and for what reason - security (personal and general) or privacy. For the purposes of this research general data protection issues such as principles of processing, legal basis and limitations of data processing right, confidentiality and integrity of data (GDPR Article 5f) were not specified. However, it was studied whether there is a difference in the respondents' attitude towards their personal data when it is collected using traditional methods and when it is collected using artificial intelligence methods. The difference was determined according to the particles that represented providing or non-providing of personal data for security (personal and general) and privacy reasons.

Relevant expert and scientific research (*Dragu*[3]; *Brandimarte*, *Acquisti* and *Loewenstein*[4]; *Goold*[5]; *Himma*[6]) focusing on the relationship between the right to security and the right to privacy are based on the axiomatic method, i. e. on an immediate increase in security by reducing privacy, as well as on an even more significant reduction of the right to privacy when using artificial intelligence methods to increase the right to security. The protection of the right to privacy when using artificial intelligence methods was recognised in 2015. At that time, the United Nations Special Rapporteur for the right to privacy compiled reports and recommendations to protect privacy and monitor relevant right-to-privacy trends in the context of new technologies, especially Open Data and Big Data.[7] In 2018, the EU recognised the need to regulate the field of artificial intelligence while respecting the right to privacy. The European Commission thus invited experts to create guidelines for the ethical development and the use of artificial intelligence based on the EU's fundamental rights under independent supervision by the European

---

2 Fuster, G. G., *The emergence of personal data protection as a fundamental right of the EU*, Springer Science & Business, Vol. 16, 2014, p. 260.

3 Dragu, T., *Is there a trade-off between security and liberty? Executive bias, privacy protections, and terrorism prevention*, American Political Science Review, Vol. 105(1), 2011, pp. 64-78.

4 Brandimarte, L.; Acquisti, A.; Loewenstein, G., *Misplaced Confidences Privacy and the Control Paradox*, Social Psychological and Personality Science, Vol. 4, 2013, pp. 340-347.

5 Goold, B. J., *Privacy, Identity and Security* in: Goold. B. J.; Lazarus, L., eds, Security and Human Rights, Portland, Hart Publishing, 2007, p. 45.

6 Himma, K. E., *Privacy Versus Security: Why Privacy is Not an Absolute Value or Right*, 44 San Diego L. Rev., 2007, pp. 857-919.

7 United Nations Human Rights Office of the High Commissioner. Special Rapporteur on the right to privacy: Purpose of the mandate, 2023, [https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx], Accessed 15 March 2023.

Group on Ethics in Science and New Technologies.[8] In the same year, the European Commission introduced the AI Alliance to promote trust in using artificial intelligence methods. The idea was to encourage Trustworthy AI by sharing best practices among the members and help developers of AI to apply essential requirements through the ALTAI tool, a practical *Assessment List for Trustworthy AI*.[9] In 2020, *White Paper on Artificial Intelligence* listed substantial risks. The difficulty of tracing back potentially problematic decisions taken by AI systems referred to above in relation to fundamental rights applies equally to security and liability-related issues and specific requirements for remote biometric identification.[10] *White Paper* presented the basis for the Proposal for an AI Liability Directive[11], which intends to ensure that persons harmed by artificial intelligence methods enjoy the same level of protection as persons harmed by traditional technologies. General Data Protection Regulation (GDPR)[12] defines personal data protection and prohibits specific AI methods, such as the processing of biometric data, to uniquely identify a natural person. The Scientific Foresight Unit (STOA) of European Parliamentary Research Service in its study *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence* states:

"In particular, AI and big data systems can fall subject to cyberattacks (designed to disable critical infrastructure, or steal or rig vast data sets, etc.), and they can even be used to commit crimes (e.g., autonomous vehicles can be used for killing or terrorist attacks, and intelligent algorithms can be used for fraud or other financial crimes). Even beyond the domain of outright illegal activities, the power of AI can be used to purse economic interests in ways that are harmful to individuals and society: users, consumers, and workers can be subject to pervasive surveillance,

---

8 European Commission. Artificial intelligence: Commission kicks off work on marrying cutting-edge technology and ethical standards, 9.3.2018, [https://ec.europa.eu/commission/presscorner/detail/en/IP_18_1381], Accessed 22 March 2023.

9 European Commission. The European AI Alliance: Promoting Trustworthy AI, [https://digital-strategy.ec.europa.eu/en/policies/european-ai-alliance], Accessed 22 March 2023.

10 European Commission. White Paper On Artificial Intelligence - A European approach to excellence and trust. COM/2020/65 final, 19.2.2020, [https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0065&from=EN], Accessed 22 March 2023.

11 European Commission. Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), 28.9.2022 COM(2022) 496 final 2022/0303(COD), [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496], Accessed 22 March 2023.

12 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, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

controlled in their access to information and opportunities, manipulated in their choices."[13]

Law enforcement authorities also use AI methods, especially for predictive purposes. However, it is not the GDPR that applies to the law enforcement authorities, but the Directive 2016/680,[14] the so-called Police Directive, which determines the partial or complete automatic collection and processing of personal data for particular, explicit and lawful purposes and the explicit prohibition of their processing in a way that is not in accordance with these purposes. Identifying natural persons is allowed only as much as necessary for these purposes. *Kuziemski* and *Przemyslav* state the same and recommend the creation of permanent groups facilitating dialogue between different regulatory agencies and policy-making bodies.[15] There are three inter-related legal initiatives at the European legislative level promoting trust in AI based on a safe and innovation-friendly environment: a European legal framework for AI to address fundamental rights and security risks specific to the AI systems, a civil liability framework - adapting liability rules to the digital age and AI - and a revision of sectoral security legislation.[16]

In the Republic of Croatia, at the time of this research, there is an intention to improve trustworthy AI through clarifications of the regulations on data protection and in information security. *Katulić* emphasizes the benefits of AI methods "for the development of more efficient public services … by providing tools and services to ensure a higher level of security".[17] *Vojković* and *Katulić* note that GDPR also addresses the transfer of personal data outside the EU and EEA areas when required for electronic commerce, information society services such as cloud ser-

---

13 Sartor, G.; Lagioia, F, *The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence*, Scientific Foresight Unit (STOA), European Parliamentary Research Service EPRS, 2020, p. 19 [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf], Accesed 6 July 2023.

14 Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision2008/977/JHA [2016] OJ L 119/89.

15 Kuziemski, M.; Przemyslaw, P., *AI Governance Post-GDPR: Lessons Learned and the Road Ahead*, European University Institute, 2019/07, p. 5, [doi:10.2870/470055].

16 European Commission. Shaping Europe's digital future: A European approach to artificial intelligence/A European approach to trust in AI, [https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence], Accessed 22 March 2023.

17 Katulić, T., *Towards the Trustworthy AI: Insights from Data Protection and Information Security Law*, Medijska istraživanja, 26 (2020), 2, p.13, [doi:10.22572/mi.26.2.1].

vices, on-demand streaming, and other content services or for more traditional purposes such as civil aviation traffic, cargo and passenger shipping etc.[18]

Croatian national framework in this area is based on the Act on the Protection of Natural Persons in Connection with the Processing and Exchange of Personal Data for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offenses or Execution of Criminal Sanctions from 2018.[19] In the national legislation of the Republic of Croatia, there is no strategy related to applying artificial intelligence methods that would include norms related to privacy protection. Therefore, this paper provides insight into the respondents' relation to their privacy and security when using artificial intelligence.

The causal relationship between the right to security and the right to privacy was tested to verify the internal validity by examining the relation of whether an increase in the right to security causes a decrease in the right to privacy and whether these rights vary consistently. It should be noted that in terms of the right to privacy, personal data (name and surname, personal identification number, credit card number, password), biometric data (fingerprint, face scan, pupil scan) and special categories of personal data (information about racial and ethnic origin, political viewpoint, religious belief, union membership, health data and data on criminal or misdemeanour proceedings) were considered. Data whose collection, processing and analysis may also significantly violate the right to privacy and related to behavioural characteristics, habits, social contacts and communication data were not considered. Control variables refer to providing personal data without possible initial perception of a threat to personal or general security (for commercial services, not law enforcement purposes).

The purpose of the research is to study whether there is a difference in the attitude of respondents in the Republic of Croatia towards the right to privacy and the right to security when it comes to conventional methods of collecting, processing and analyzing personal data and when law enforcement authorities use AI methods at a time when there is no national AI strategy.

The research question is whether there is a difference related to the right to security and the right to privacy when using conventional methods of collecting, processing and analysing personal data and when using artificial intelligence methods.

---

[18] Vojković, G.; Katulić, T., *Data Protection and Smart Cities*, in: Augusto, J.C. (eds) Handbook of Smart Cities. Springer, Cham, 2020, p. 1, [https://doi.org/10.1007/978-3-030-15145-4_28-1], Accessed 6 July 2023.

[19] Zakon o zaštiti fizičkih osoba u vezi s obradom i razmjenom osobnih podataka u svrhe sprječavanja, istraživanja, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, Official Gazette No 68/2018.

The assumption is that there is a causality between the relation to privacy and the relation to security of natural persons when collecting, processing and analysing their personal data using conventional and artificial intelligence methods.

The second assumption is that there is a statistically significant negative difference between providing personal data to law enforcement authorities when it is collected, processed and analysed by conventional methods and when it is collected, processed and analysed by artificial intelligence methods.

2. THE RELATIONSHIP BETWEEN PRIVACY AND SECURITY AS A RESEARCH SUBJECT

The measurement of the relationship between the right to privacy and the right to security was carried out based on personal data: personal identification number, name and surname, credit card number, password, biometric data (fingerprint, facial scan, pupil scan), and a special category of personal data (racial and ethical origin, political viewpoint, religious belief, union membership, health data and data on criminal or misdemeanour proceedings). It was measured in which situations the reasons for providing personal data were related to security and in which they were not. Data on behavioural characteristics, habits, communication data and the like, essential to privacy, especially when collected, processed and analysed using artificial intelligence methods, were not considered. Respondents had to decide in which situations and for what reasons they would provide their data or not provide it at all.

In cases the respondents have decided that they never provide personal data in certain situations or always provide it when someone asks for it, it was determined that their right to privacy is not affected by the level of their right to security. Namely, respondents were offered the option of choosing to provide personal data if it concerns their personal security or for general security, where security reasons imply that law enforcement authorities collect personal data. The situations were divided into conventional methods of data collection (airport, ship, earthquake, social contact, travel reservation, entering the cinema and theatre) and artificial intelligence data collection methods (autonomous vehicle, robot vacuum cleaner, facial recognition on social networks and personalised product and service recommendations).

3. RESEARCH METHODS AND SAMPLE DESCRIPTION

The research on providing personal data when using conventional methods and artificial intelligence methods from the aspect of the right to privacy and the right

to security was carried out with a closed questionnaire as a means of measuring the frequency of choosing the right to security in situations when there is a greater need for general and personal security. Situations related to consumer services were taken as control ones. The testing was completely anonymous and voluntary, and a positive opinion of the Ethics Committee of the University of Applied Sciences in Criminal Investigation and Public Security was obtained. The correlation between the right to privacy and the right to security was examined with regard to the correlation coefficient (r). By virtue of induction, assumptions were made that there is a negative correlation between the right to privacy and the right to security and the assumption that there is a statistically significant negative difference between the providing of personal data to law enforcement authorities in the case when they are collected, processed and analysed by conventional methods and in the case when they are collected, processed or analysed by artificial intelligence methods. The deduction method was used to observe the specificity of the relationship between the right to privacy and the right to security regarding the type of personal data, but not the category. The obtained results were interpreted through analysis and synthesis. MS Excel statistical tools were used for statistical methods. The questionnaire did not examine respondents' attitudes but measured in which situations and in relation to which personal data the respondents decided to provide personal data ("giving privacy") to exercise the right to security. Collected empirical data were tested by comparative analysis to determine compliance with conditional hypotheses.

The measurement was conducted on 309 subjects (N=309) from the Republic of Croatia, and the sample was probabilistic. The majority of respondents (35%) were between the ages of 26 and 35, and the least (10%) were over 55 (Table 1). Respondents were informed about the research objectives and their voluntary and anonymous participation, and the results were presented cumulatively.

Table 1: Distribution of respondents by age (N=309)

Age	N	%
less than 25 years	66	21
26 - 35 years	109	35
36 - 45 years	59	19
46 - 55 years	45	15
more than 55 years	30	10

Regarding the distribution of respondents by gender, 58% were female, and 42% were male (Table 2).

Table 2: Distribution of respondents by gender (N=309)

Gender	N	%
female	179	58
male	130	42

According to the level of education, most respondents (54%) have completed high school, and the least (2%) have a doctorate (Table 3).

Table 3: Distribution of respondents by the level of education (N=309)

Level of education	N	%
high school	170	54
undergraduate studies	38	12
graduate studies	76	24
master of science	18	6
doctorate of science	7	2

4. RESULTS OF THE RESEARCH

In the questionnaire, respondents could choose in which situations they would provide personal data due to the right to security (personal and general) and when that right does not determine the reason for providing personal data. Thirteen different situations were offered, five of which implied the need to exercise a greater right to personal or general security (at the airport, when boarding a ship, after an earthquake, when driving an autonomous vehicle and when recognising faces using artificial intelligence methods), five of those related to various service activities (getting a discount in a store, booking a trip, in the cinema, social contacts on the Internet and using a robot vacuum cleaner) and the final three related to product recommendations, personalised content recommendations and communication with the robot. The situations were classified into two groups: seven were collected by conventional methods, and six were collected, processed and analysed by artificial intelligence methods.

Table 4 shows that 79% (31,811) of responses did not refer to providing individual personal data to law enforcement authorities for personal or general security reasons but that they would **always** or **never** be provided when requested by anyone, regardless of personal or general security. Security-related privacy was determined in 21% of cases (8,359 responses), i. e. providing personal data was related to security.

Table 4: Providing of personal data with regard to the right to security

Right to security	N	%
yes	31811	79%
no	8359	21%

As regards the distribution of situations in which personal data can be collected, the data from Table 5 show that if the situation does not imply the need for security, less (0.64 : 1) personal data would be provided for the right to security reasons.

Table 5: Providing of personal data with regard to the implication of the right to security

Situation	privacy regardless of security	privacy with respect to security
implies the right to security	14628	5457
does not imply the right to security	17183	2902

The results presented in Table 6 show the relationship between the right to privacy and the right to security with regard to the methods of collection, processing and analysis of personal data. There is a fairly strong positive correlation (r = 0.87) in the respondents' attitude towards the right to privacy and the right to security if personal data is collected, processed and analysed using conventional or artificial intelligence methods. So it is evident that there is a willingness to provide more personal data if conventional methods are used.

Table 6: Providing of personal data with regard to the collecting methods

Right to security	conventional methods	methods of AI
no	21181	21705
yes	6938	2397

The distribution of the results according to the type of personal data and respondents' commitment to security is shown in Table 7. Concerning the type of data, the personal data the respondents were least willing to provide in situations where their personal or general security was in question was the password (2%). The personal data they chose most likely to provide in personal and general security cases was their name and surname (17%). After that, personal identification numbers and health data (12%) followed. Interestingly, the subsequent data respondents were least likely to share was their political viewpoint (3%).

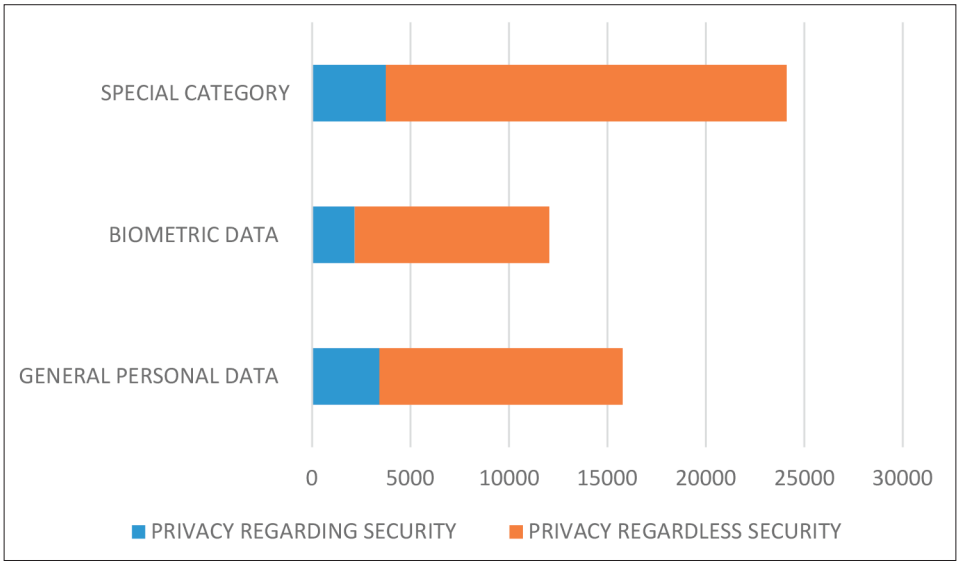
Regarding the distribution of results in situations that are not perceived as security-related, the respondents were equally inclined to provide their personal data, whether general personal, biometric or a special category of personal data are in question (range from 6 to 9%).

Table 7: Distribution of results according to the type of data and respondents' commitment to security

Data category	**Type of personal data**	**Privacy, regardless of security**		**Privacy with respect to security**	
general personal data	personal identification number	2855	7%	1162	12%
	name and surname	2385	6%	1632	17%
	credit card number	3554	8%	463	5%
	password	**3564**	8%	**163**	**2%**
biometric data	fingerprint	3301	8%	716	8%
	face scan	3120	7%	897	10%
	pupil scan	3460	8%	557	6%
special category of personal data	racial and ethnic origin	3187	7%	830	9%
	political viewpoint	3697	9%	320	3%
	religious belief	3580	8%	437	5%
	union membership	3581	8%	436	5%
	health data	2935	7%	1082	12%
	data on criminal or misdemeanour proceedings	3377	8%	640	7%
TOTAL		42596		9335	100%

Providing personal data with regard to the category and security or non-security reasons is shown in Chart 1.

Chart 1: Providing of personal data with regard to the category



5. DISCUSSION

The research shows that most personal data in the majority of observed situations (79%) would not be provided to law enforcement authorities to exercise a greater right to personal or general security. This is supported by the results that show that the slightest concern for the right to privacy will be in situations that do not imply the need for a greater right to security. The said reveals that the regulatory authorities have a greater responsibility when establishing a collection, processing and analysis system of personal data, which should include privacy protection. Prediction is mentioned as one of the most important areas of regulating the use of AI methods by law enforcement authorities. Thus *Chen*, *Ahn* and *Wang* state:

"Predictive analytics is another popular use of AI that helps prioritize resource allocation in the public sector for services such as public safety and the prevention of fraud. Humans are still responsible for enforcing public safety rules and determining the subjects of fraud investigations. In the cybersecurity area, AI can fulfill the functions of security analytics and threat intelligence, while humans exercise judgment on the parameters of threat analysis and responses."[20]

[20] Chen, Y.-C.; Ahn, M.; Wang, Y.-F., *Artificial Intelligence and Public Values: Value Impacts and Governance in the Public Sector*, Sustainability 2023, 15, 4796, p. 4, [https://doi.org/10.3390/su15064796], Accessed 6 July 2023.

Kingston stands out that area where AI technology might be of use to organisations during their data processing activities is in the identification and assessment of potential or actual breaches.[21] He states that the monitoring of data security is a key task.

Results in this research show a greater willingness to provide personal data when collected using conventional methods compared to artificial intelligence methods, it is imperative to protect the right to privacy with adequate legal regulation regarding the use of artificial intelligence methods. Also, a fairly strong positive correlation (r = 0.87) in respondents' attitudes toward the right to privacy and the right to security in situations where personal data is collected using conventional and artificial intelligence methods shows that the decision to provide personal data depends more on the type of personal data than on collecting method. This indicates that the particular focus of regulatory authorities should be on situations that do not imply the need for privacy protection. This particularly applies to private or public services, including artificial intelligence methods most people use. Legal regulation of the use of artificial intelligence methods in individual areas of its application should also exist at the national level. At the national level, there is no specifically regulated privacy protection in the context of artificial intelligence methods at the strategic level. There is no assessment of the effects of systems using artificial intelligence methods on human rights. In his recommendations, the *Commissioner for Human Rights of the Council of Europe* assumes that in circumstances where a risk of violating human rights has been identified in relation to an AI system that has already been deployed by a public authority, its use should be immediately suspended and where it is not possible, the AI system should not be deployed or otherwise used by any public authority.[22] *Etzioni* points out that nations face several entirely legitimate, competing claims regarding privacy and security, which cannot be mutually maximised.[23] He also advocates balancing individual rights with social responsibilities and individuality with community.[24] The exact position took *Stalla-Bourdilon, Philips and Ryan*: "To engage in the balancing of privacy and security interests, it is crucial to start with defining the concepts at stake…What remains is to clarify the notion of security and distinguish

---

21 Kingston, J., *Using Artificial Intelligence to Support Compliance with the General Data Protection Regulation*, Artificial Intelligence and Law, 2018, p. 10.

22 Council of Europe: Commissioner for Human Rights. Unboxing Artificial Intelligence: 10 steps to protect Human Rights, May 2019, p. 8, [https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64], Accessed 6 April 2023.

23 Etzioni, A., *Privacy in a Cybver Age: Policy and Practice*, New York, NY, Palgrave Macmillan, 2015, p. 101.

24 Etzioni, A., *The Limits of Privacy*, New York, NY, Basic Books, 2008, p. 198.

between distinct but closely related terms such as national security, public security, the prevention of crimes and cybersecurity."[25]

The results of this research show that respondents are the least inclined to provide biometric data for security reasons (personal and general security). The correlation between its providing when collected by conventional methods and methods of AI is fairly strong positive (r = 0.87). This indicates that the type of personal data, not the collecting method, is decisive for people in terms of privacy and security. This can also be interpreted as insufficient knowledge of possible privacy implications when using artificial intelligence methods. In general, the results point to the great responsibility of regulatory bodies in the field of privacy protection when applying artificial intelligence methods. When it comes to AI methods for law enforcement activities, the results support *Mironenko Enerstvedt's* point that it is crucial that "both the regulation and the technologies can protect both security – and the right to life – along with other rights of the individual and that the law has a potential to define both the amount of desired privacy as well as data protection requirements and the amount limits of the security measure involved".[26] *Mironenko Enerstvedt* further states: "… if no proper limits on surveillance are set in the earlier stages, privacy and other human rights may ultimately be affected to an undesirable extent."[27]

As for the protection of individual personal data, there are different approaches. Some authors look at protecting personal data in their totality, which is the speciality of the legal approach. In contrast, technology experts approach them from the aspect of collecting technology. *Solova* considers that we do not need to accept the claim that information is inherently public or private.[28] However, he also states that "the interests aligned against privacy – including national security – are often cached out in larger social terms".[29] A similar approach has *Floridi,* who considers that agents do not need to be persons; they can be organisations, artificial constructs, or hybrid syntheses.[30]

---

25 Stalla-Bourdillon, S.; Phillips, J.; Ryan, M. D., *Privacy vs. Security*, Springer London, Springer Briefs in Cybersecurity, 2014, p. 65.

26 Mironenko Enerstvedt, O., *Aviation Security, Privacy, Data Protection and Other Human Rights: Technologies and Legal Principles,* Law, Governance and Technology Series Sub-series: Issues in Privacy and Data Protection, Vol. 37, 2017, p. 422.

27 *Ibid.*

28 Solove, D. J., *The Meaning and Value of Privacy*, Social Dimensions of Privacy, Cambridge, Cambridge University Press, 2015, p. 75.

29 Solove, D. J., *Understanding Privacy*, Cambridge, MA., Harvard University Press, 2008, p. 89.

30 Floridi, L., *Four Challenges for a Theory of Informational Privacy*, Ethics and Information Technology, Vol. 8, No. 3, 2006, p. 115.

6. PERSONAL DATA AND RIGHT TO PRIVACY IN THE CASE LAW OF THE EUROPEAN COURT OF HUMAN RIGHTS

When it comes to the right to privacy and the use of personal data, regardless of what type of personal data is in question and what method of collection is involved, some case law of the European Court of Human Rights has been studied. Namely, misuse of personal data in the context of the right to privacy violates Article 8 of the European Convention on Human Rights.[31] In the *Case of S. and Marper v. the United Kingdom,* the Court finds 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 of the Convention. 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. Domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored and 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 … The domestic law must also afford adequate guarantees that retained personal data was efficiently protected from misuse and abuse … ."[32]

In the *Case of Big Brother Watch and Others v. The United Kingdom*, the Court clearly stated that "even the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 … and that the need for safeguards will be all the greater where the protection of personal data undergoing automatic processing is concerned." The Court further stated that the fact that the stored material is in coded form, intelligible only with the use of computer technology and capable of being interpreted only by a limited number of persons, has no effect on that finding. If information about a person are analysed or if the content of the communications is being examined by an analyst, the need for safeguards is the greatest.[33]

In the *Case of Breyer v. Germany,* the Court stated that private life is a broad term and that Article 8 protects as well as "the right to identity and personal devel-

---

31 European Convention on Human Rights (Convention for the Protection of Human Rights and Fundamental Freedoms) as amended by Protocols Nos. 11 and 14, 4 November 1950.

32 Judgement S. and Marper v. the United Kingdom, Applications nos. 30562/04 and 30566/04, Strasbourg, 4 December 2008, Art. 103.

33 Judgement Big Brother Watch and Others v. The United Kingdom, Applications nos. 58170/13, 62322/14 and 24960/15, Strasbourg, 25 May 2021, Art. 330.

opment and the right to establish and develop relationships with other human beings and the outside world". When it comes to the use of personal data, the Court further stated "that the term 'private life' must not Be Interpreted Restrictively".[34] When data has been collected on a specific person, the processing or use of personal data or its publication to the degree beyond what is usual, considerations of private life arise. In that way, Article 8 provides for "the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged".[35] The same Court views can be found in the *Case of M. L. and W. W. v. Germany*[36] and the *Case of Satakunnan Markkinapörssi oy and Satamedia oy v. Finland.*[37]

In the *Case of Magyar Helsinki Bizottság v. Hungary,* the Court, inter alia, specified personal data relating to the most intimate and personal aspects of an individual, such as health status, attitude to religion and sexual orientation, stating that "such categories of data constituted particular elements of private life falling within the scope of the protection of Article 8 of the Convention".[38]

7. CONCLUSION

This research did not confirm the first conditional hypothesis that there is a causality between the perception of privacy and the perception of security of natural persons when collecting, processing and analysing their personal data using conventional and artificial intelligence methods. Namely, no negative correlation was found between providing personal data for security reasons and those unrelated to security, so causality could not be measured in the experiment. A recommendation for further research is to create a preliminary questionnaire in which respondents would be individually asked which specific situations they consider sufficiently security relevant and in which they would consider their privacy from the aspect of security. It is also recommended that, in future research, the situations in which "giving privacy" for security reasons is measured are divided into those that are

[34] Judgement Breyer v. Germany, Application no. 50001/12, Strasbourg, 30 January 2020, Art. 73-76

[35] *Ibid.*

[36] Judgement M. L. and W. W. v. Germany, Applications nos. 60798/10 and 65599/10, Strasbourg, 28 June 2018, Art. 87.

[37] Judgement Satakunnan Markkinapörssi oy and Satamedia oy v. Finland, Application no. 931/13, Strasbourg, 27 June 2017, Art. 137.

[38] Judgement Magyar Helsinki Bizottság v. Hungary, Application no. 18030/11, Strasbourg, 8 November 2016, Art. 192.

extremely dangerous (terrorism, epidemics and disasters) and those that are not perceived as huge security threats (common crime).

The second conditional hypothesis that there is a statistically significant negative difference between providing personal data to law enforcement authorities in the case when it is collected by conventional methods compared to those cases when artificial intelligence methods collect it was rejected because a fairly strong positive correlation (r = 0.87) was found when providing personal data for security reasons using conventional methods and artificial intelligence methods. It follows from this that the respondent's decision to provide personal data to law enforcement authorities was based on the type of personal data and not on the method of its collection. Given that at the time of the research, there is no legally regulated privacy protection in the context of artificial intelligence methods at the national level of respondents, there is a possibility that the wider population is not aware of the possible effects of artificial intelligence methods on the right to privacy. There is also the possibility that respondents consider privacy protection solely with regard to the type of personal data that may be compromised and its consequences.

The answer to the research question of whether there is a difference in the relation to the causality of the right to security and the right to privacy when using conventional methods of collecting personal data in relation to the use of artificial intelligence methods conditionally is that in the territory of the Republic of Croatia at the time of the research, there is not.

REFERENCES

BOOKS AND ARTICLES

1. Brandimarte, L.; Acquisti, A.; Loewenstein, G., *Misplaced Confidences Privacy and the Control Paradox*, Social Psychological and Personality Science, Vol. 4, 2013, pp. 340-347
2. Chen, Y.-C.; Ahn, M.; Wang, Y.-F., *Artificial Intelligence and Public Values: Value Impacts and Governance in the Public Sector*, Sustainability 2023, 15, 4796, [https://doi.org/10.3390/su15064796], Accessed 6 July 2023
3. Dragu, T., *Is there a trade-off between security and liberty? Executive bias, privacy protections, and terrorism prevention*, American Political Science Review, Vol. 105(1), 2011, pp. 64-78
4. Etzioni, A, *Privacy in a Cyber Age: Policy and Practice*, New York, NY, Palgrave Macmillan, 2015
5. Etzioni, A., *The Limits of Privacy*, New York, NY, Basic Books, 2008
6. Floridi, L., *Four Challenges for a Theory of Informational Privacy*, Ethics and Information Technology, Vol. 8, No. 3, 2006, pp. 109-119
7. Fuster, G. G., *The emergence of personal data protection as a fundamental right of the EU*, Springer Science & Business, Vol. 16, 2014

8. Goold, B. J., *Privacy, Identity and Security* in: Goold. B. J.; Lazarus, L., eds, Security and Human Rights, Portland, Hart Publishing, 2007, pp. 45-72
9. Himma, K. E., *Privacy Versus Security: Why Privacy is Not an Absolute Value or Right*, 44 San Diego L. Rev., 2007, pp. 857-919
10. Katulić, T., *Towards the Trustworthy AI: Insights from Data Protection and Information Security Law*, Medijska istraživanja, 26 (2020), 2; p. 9-28, doi:10.22572/mi.26.2.1
11. Kingston, J., *Using Artificial Intelligence to Support Compliance with the General Data Protection Regulation*, Artificial Intelligence and Law, 2018
12. Kuziemski, M., Przemyslaw, P., *AI Governance Post-GDPR: Lessons Learned and the Road Ahead*, European University Institute, 2019/07, doi:10.2870/470055
13. Mironenko Enerstvedt, O., *Aviation Security, Privacy, Data Protection and Other Human Rights: Technologies and Legal Principles,* Law, Governance and Technology Series Sub-series: Issues in Privacy and Data Protection, Vol. 37, 2017
14. Rodotà, S., *Data Protection as a Fundamental Right,* in: Gutwirth, S., Poullet, Y., De Hert, P., de Terwangne, C., Nouwt, S. (eds) Reinventing Data Protection? Springer, Dordrecht, 2009 [https://doi.org/10.1007/978-1-4020-9498-9_3], Accessed 7 July 2023
15. Solove, D. J., *The Meaning and Value of Privacy*, Social Dimensions of Privacy, Cambridge, Cambridge University Press, 2015
16. Solove, D. J., *Understanding Privacy*, Cambridge, MA., Harvard University Press, 2008
17. Stalla-Bourdillon, S.; Phillips, J.; Ryan, M. D., *Privacy vs. Security*, Springer London, Springer Briefs in Cybersecurity, 2014
18. Vojković, G., Katulić, T., *Data Protection and Smart Cities*, in: Augusto, J.C. (eds) Handbook of Smart Cities. Springer, Cham, 2020, [https://doi.org/10.1007/978-3-030-15145-4_28-1], Accessed 6 July 2023

ECHR

1. *Big Brother Watch and Others v. The United Kingdom*, Applications nos. 58170/13, 62322/14 and 24960/15, Strasbourg, 25 May 2021
2. *Breyer v. Germany*, Application no. 50001/12, Strasbourg, 30 January 2020
3. *M. L. and W. W. v. Germany*, Applications nos. 60798/10 and 65599/10, Strasbourg, 28 June 2018
4. *Magyar Helsinki Bizottság v. Hungary*, Application no. 18030/11, Strasbourg, 8 November 2016
5. *S. and Marper v. the United Kingdom*, Applications nos. 30562/04 and 30566/04, Strasbourg, 4 December 2008
6. *Satakunnan Markkinapörssi oy and Satamedia oy v. Finland*, Application no. 931/13, Strasbourg, 27 June 2017
7. European Convention on Human Rights (Convention for the Protection of Human Rights and Fundamental Freedoms) as amended by Protocols Nos. 11 and 14, 4 November 1950

EU LAW

1. Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision2008/977/JHA [2016] OJ L 119/89
2. 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, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1
3. EU Charter of Fundamental Right

LIST OF NATIONAL REGULATIONS, ACTS AND COURT DECISIONS

1. Zakon o zaštiti fizičkih osoba u vezi s obradom i razmjenom osobnih podataka u svrhe sprječavanja, istraživanja, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, Official Gazette No 68/2018

WEBSITE REFERENCES

1. Council of Europe: Commissioner for Human Rights. Unboxing Artificial Intelligence: 10 steps to protect Human Rights, May 2019, [https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64], Accessed 6 April 2023
2. United Nations Human Rights Office of the High Commissioner. Special Rapporteur on the right to privacy: Purpose of the mandate, 2023, [https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx], Accessed 15 March 2023
3. European Commission. Artificial intelligence: Commission kicks off work on marrying cutting-edge technology and ethical standards, 3 April 2018, [https://ec.europa.eu/commission/presscorner/detail/en/IP_18_1381], Accessed 22 March 2023
4. European Commission. Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), 28.9.2022 COM (2022) 496 final 2022/0303(COD), [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496], Accessed 22 March 2023
5. European Commission. Shaping Europe's digital future: A European approach to artificial intelligence/A European approach to trust in AI, [https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence], Accessed 22 March 2023
6. European Commission. The European AI Alliance: Promoting Trustworthy AI, [https://digital-strategy.ec.europa.eu/en/policies/european-ai-alliance], Accessed 22 March 2023
7. European Commission. White Paper on Artificial Intelligence - A European approach to excellence and trust. COM/2020/65 final, 19.2.2020, [https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0065&from=EN], Accessed 22 March 2023
8. Sartor. G., Lagioia, F., *The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence*, Scientific Foresight Unit (STOA) EPRS, European Parliamentary Research Service 2020, [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf], Accessed 6 July 2023