PARTNERI SRBIJA

Овај пројекат финансира Европска унија

#ЕУ ЗА ТЕБЕ

Privacy and Personal Data Protection in Serbia

Reform and Implementation of the Legal Framework in the Selected Sectors (2021 -2022)

SHARE FONDACIJA

A 11 INICIJATIVA ZA EKONOMSKA I SOCIJALNA PRAVA

BOŠ BEOGRADSKA OTVORENA ŠKOLA

ATINA

DA SE ZNA

Privacy and Personal Data Protection in Serbia

Reform and Implementation of the Legal Framework in the Selected Sectors (2021 -2022)

Publisher: Partners for Democratic Change Serbia (Partners Serbia)
www.partners-serbia.org

For the publisher: Ana Toskić Cvetinović

Editor: Uroš Mišljenović

Authors: Nina Nicović
Ana Toskić Cvetinović
Milica Tošić
Milica Marinković
Vlada Šahović
Damjan Mileusnić
Uroš Mišljenović

Translation: Vera Gojković

Proofreading: Emily Wright

Belgrade, 2022.

This publication was published with the financial assistance of the European Union. The sole responsibility for the content of this publication lies with Partners for Democratic Change Serbia, SHARE Foundation, Da se zna! (Let It Be Known) Association, Belgrade Open School, ATINA NGO and A11 Initiative, and the content should not be construed as reflecting the official positions of the European Union.

***

All terms used in the text in the masculine gender refer to both masculine and feminine genders of the persons they refer to.

CONTENTS

INTRODUCTION

The right to privacy and personal data protection is one of those rights which, in addition to having value in itself, prevents the violation of other rights and freedoms. During its more than ten-year practice in this field, Partners Serbia has repeatedly encountered cases in which abuses or omissions in the handling of citizens' personal data resulted in the denial of citizens' social and economic rights, discrimination, threat to the freedom of speech or expression, etc., which frequently affect the most vulnerable among us.

With the idea of preserving citizens' dignity by protecting their privacy, six civil society organizations - Partners Serbia, SHARE Foundation, Da se zna! (Let It Be Known) Association, Belgrade Open School, Atina NGO and A11 Initiative - launched the *Protect Privacy - Resist Pressure* project in 2020. The project documented privacy violation cases, recording 149 such cases during the two-year monitoring process.

The frequency of privacy violations indicates how bad the situation in this area is. Violations range from inadequate legal framework, through underdeveloped practice of sanctioning violations of regulations, to the citizens' insufficient awareness about their own rights. In this context, the goal of this publication is to point to the challenges in connection with reforms and implementation of the existing privacy and personal data protection legal framework especially in areas which the authors recognized as significant in 2021 and 2022.

We will begin our overview of the situation by presenting the process of the development of a new Personal Data Protection Strategy, which should comprehensively determine the fields in which the situation, measures, and activities should be improved. After that, we will present the process of drafting a new Law on Internal Affairs, in which, because of the far-reaching consequences for the Serbian citizens' right to privacy, the issue of the Republic of Serbia's position towards the use of video surveillance systems with automatic facial recognition technology has a prominent place. Then, we will present the case law on the violation of the right to personal data protection developed by the Serbian courts' criminal departments in the previous year. We will continue with an overview of the international

standards regarding the child's right to privacy in the digital environment and place them in the context of their application in the Republic of Serbia. We will end the publication by presenting the situation in labor relations in the context of personal data protection in job applications.

This publication, like the one published a year ago, does not claim to offer a comprehensive overview of legal gaps or problems in the implementation of the legal framework on the protection of privacy and personal data in our country. In this context, we have to reiterate that during the previous year no progress has been registered regarding the obligation to carry out the "Analysis of sectoral regulations and development of a plan for their harmonization with the new Law on Personal Data Protection" referred to in the Action Plan for Chapter 23, nor has there been any significant progress in the harmonization of sectoral laws with the Law on Personal Data Protection, which is an obligation under the Law on Personal Data Protection.

Therefore, like a year ago, the analyses made within the *Protect Privacy - Resist Pressure* project, presented in this publication, support the civil sector in the process of reformation of the legal framework and improvement of its implementation. As an additional resource for the improvement of the legal framework, a Guide for Developing and Amending Sectoral Regulations Governing Personal Data Processing and Protection was made within the project, with the aim of supporting the authorities responsible for the development of sectoral regulations in carrying out these activities in a high-quality manner.

THE PROCESS OF ADOPTION OF THE PERSONAL DATA PROTECTION STRATEGY

Authors: Ana Toskić Cvetinović, Damjan Mileusnić

Introduction

The new Law on Personal Data Protection was adopted in November 2018, but due to its complexity and the number of modifications, a 9-month period was left before the beginning of its implementation (August 2019). The Law was made on the model of the EU General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED).

However, the Law as such, cannot regulate this field in its entirety, and, therefore, numerous sectoral laws had to be adopted or amended in order to regulate specific features which the Law could not. The appropriate implementation of the legal framework is as important as the improvement of knowledge and raising of the awareness of citizens regarding their rights.

It has been nearly 12 years since the original Personal Data Protection Strategy was adopted. Even though the Government of the Republic of Serbia decided to establish a special working body to oversee the fulfilment of requirements and implementation of the Personal Data Protection Strategy and to adopt the Action Plan within 90 days from the date of publication of the decision, this process has never been properly initiated.[1]

Consequently, intensive discussions were held over the last year on the necessity of the adoption of a new Personal Data Protection Strategy, one that would comprehensively and coherently define the direction and method for improving the situation in this field, particularly regarding the reform and implementation of the legal framework.

[1] https://paragraflex.rs/dnevne-vesti/180216/180216-vest12.html

Establishment of a Working Group in Charge of Drafting the Personal Data Protection Strategy

In accordance with the June 2021 Serbian Government decision, a Working group in charge of developing a draft of the Personal Data Protection Strategy and the Action Plan was established. It was made up only of representatives of personal data controllers, specifically bodies of authority, e.g., the Government, ministries and the judiciary.

Since the representatives of social groups or citizens whose data are processed were not represented in the Working group, the civil society organizations Partners Serbia and Share Foundation expressed their interest in participating in the Working group. The formal invitation for the participation of these organizations in the Working group was sent in December 2021, and these organizations have since participated in the Working group on an equal footing.

In the period between December 2021 and when this report was written, two Working group meetings were held in addition to consultations between stakeholders and Working group members. The Working group prepared the initial drafts of the Strategy and the Action Plan, but the preparation of these documents was slowed due to the April 2022 elections. One of the proposed activities the Working group has agreed upon is the amendment of the Law on Personal Data Protection for the purpose of specifying or defining certain terms which cause difficulties in practice. Another conclusion of the Working group is that the Strategy and the Action Plan should recognize specific features of personal data protection in the implementation of new technologies, including artificial intelligence. The Working group, therefore, held a meeting in May 2022 and discussed the need for amending the Law, as well as the specific features of biometric data processing and personal data protection in the development and implementation of artificial intelligence systems.

Recommended Activities in the Action Plan for the Implementation of the Personal Data Protection Strategy

Through this process, Partners Serbia is committed to overcoming the key issues observed in the implementation of the Law on Personal Data Protection and other relevant regulations. So far, observations have shown that state authorities frequently violate the right to privacy and the case law on violations of the right to personal data protection has not been developed. In addition to this, the increasing frequency of information leaks (containing personal data) from institutions to the media is a cause for concern, especially when it comes to human trafficking and other cases in which the privacy of crime victims, including juveniles and children, is at stake. Another negative practice is reflected in the reluctance of some data controllers and processors to implement specific HR and organizational measures to ensure the implementation of data processing in those bodies in accordance with the law. These shortcomings are primarily reflected in the failure to appoint a person in charge of personal data protection, failure to publish privacy policies on websites through which managers would inform stakeholders about the type of collected data, the manner of collection, how long the data is stored, legal basis for collection etc., inadequate personal data protection (for the purpose of preventing data leaks) and insufficient use of digital protection measures at institutions during the processing of personal data.

Partners Serbia, together with a group of civil society organizations, submitted to the Working group a set of different activities that should be included in the Action Plan for the implementation of the Personal Data Protection Strategy. The proposals were made on the basis of information received from organizations that provide support to members of vulnerable groups whose privacy has been violated, on the basis of long-term experience of Partners Serbia in this field, information contained in the Commissioner's annual reports, case law analysis and data collected in the Database of Privacy Violations in which violations detected in the last two years were mapped.

The observation and knowledge about the right to personal data protection in all spheres of life has been recognized as one of the goals of the draft Strategy. As for the improvement of the legal framework in this field, civil society organizations have proposed amendments to the Serbian Criminal Code, specifically Article 146, which regulates the unauthorized collection of personal data (especially in view of the almost non-existent case law in this field – there have been just seven suspended sentences since 2015). To that end, it is necessary to improve the victims' court protection, to adopt a stricter sentencing policy in case of privacy violations, and to grant greater powers to the Commissioner for Information of Public Importance and Personal Data Protection.

In addition to this, the existing Serbian legal framework needs to be harmonized with the Law on Personal Data Protection. The Law on Public Information and Media needs to be improved in order to prevent media violations of privacy and punish the perpetrators. Better legal solutions also need to be adopted in order to protect the privacy of human trafficking victims, especially during court proceedings where they appear as victims or witnesses, which also includes the protection of privacy of representatives of organizations that provide legal aid or support to human trafficking and violence victims during court proceedings.

Additionally, for the purpose of improving the institutional framework in this field, it would be desirable to establish regional offices of the Commissioner throughout Serbia (which is already envisioned in the recent amendments to the Law on Free Access to Information of Public Importance) for the purpose of ensuring better territorial coverage and easier access to justice for persons in local communities. It is also necessary to organize trainings for the Commissioner Service employees on new trends in the field of personal data protection as well as to organize specialized trainings on personal data protection in the implementation of new technologies and artificial intelligence. It is important to improve cooperation with authorities dealing with personal data protection in other countries and with international organizations. More effective personal data protection would thus be secured for a wider circle of citizens. The Commissioner would also have to have a more active role in the criminal and misdemeanour proceedings against perpetrators of privacy offenses.

As for the improvement of mechanisms for the protection of the right to privacy and personal data protection, the Commissioner will have to

draft recommendations that will specify the internal documents which data controllers and processors should develop since this issue has not yet been regulated by the Law on Personal Data Protection. It is also very important to require all foreign data controllers to register their representatives in Serbia in charge of personal data protection, as well as to create guidelines for the development of a personal data protection impact assessment study and guidelines for the personal data protection of human trafficking victims during court proceedings (including persons who provide them with legal aid and psychosocial support). The guidelines are also necessary for employees in the social protection system, who very frequently handle large quantities of personal data, for the purpose of ensuring that they are trained for this kind of work and able to implement appropriate protection measures when they handle the personal data of a wider circle of citizens. It is also necessary to establish the disciplinary responsibility of employees/responsible persons if privacy violations occur in the social protection system.

Regarding curriculum improvement, it is essential to include the topic of personal data protection and digital literacy of young people in the curriculum of civic education to enable new generations to acquire knowledge about the importance of these rights.

It is especially important to raise the capacity of public prosecutors, judges and police officers who act in privacy violation cases (both in civil and criminal matters), train them to adequately protect the privacy of all participants in the proceedings and prevent them from contributing to further victimization of participants in the proceedings.

Moreover, it is also necessary to raise citizens' awareness of the importance of privacy and personal data protection through different workshops with young people and marginalized group members, to broadcast educational campaigns on the importance of privacy in the national media. as well as to train media representatives on how to handle such situations. The media would thus receive education on the consequences of personal data disclosures resulting from negligence in reporting and would pay more attention to the protection of privacy in the future. In this regard, it would be useful to develop a brief guide for the implementation of the Serbian Journalists' Code of Ethics in the field of media reporting, where the right to privacy would be explained in greater detail. In addition to the right to privacy, it would also be necessary to implement different educational campaigns for citizens about the responsible use of artificial intelligence

and new technologies and their rights regarding personal data protection in artificial intelligence systems.

In order to prevent further information leaks from state authorities and to facilitate the determination of the responsible employees in cases of personal data disclosure, it is necessary to improve the capacity of staff at these authorities and to establish a system for controlling the access to databases (thus making it possible to determine easily and quickly who, when and how has accessed certain personal data of users).

Further Steps

The Law on Personal Data Protection itself is a step forward in improving the Serbian citizens' right to privacy protection. However, on its own, the Law is insufficient, since even the best written laws are not worth much unless appropriate conditions for their full implementation have been created. For that very reason, the Strategy drafting process is an important step in the development of an institutional and wider social infrastructure for the implementation of standards important for the effective protection of Serbian citizens' privacy.

It is important to point out that the process of Strategy development should not affect the already existing processes aimed at improving the situation in this field. There is no reason for further postponement of an analysis of shortcomings in the legal framework in this field or for waiting for the improvement of regulations that have been found to contain certain shortcomings.

The field of personal data protection is constantly developing, improving and evolving. However, the Serbian legal framework in this field is constantly lagging. It is, therefore, necessary for us as a society to define the strategic direction in which the legal regulation will develop, in order to preserve citizens' privacy and ensure appropriate protection measures for the purpose of preventing future disclosures of citizens' personal data.

Only if citizens have appropriate privacy protection mechanisms at their disposal and if the offenders receive appropriate punishments can we say that the level of personal data protection in Serbia is appropriate.

INCLUDING VIDEO SURVEILLANCE WITH FACIAL RECOGNITION TECHNOLOGY IN THE LEGAL FRAMEWORK

Authors: Milica Tošić and Ana Toskić Cvetinović

Introduction

In late August 2021, the Ministry of Interior (MoI) posted the Draft Law on Internal Affairs[2] on its website without any prior announcement and without informing the professional and general public that the drafting of this law had been planned. Within the same post, the public was informed that the public debate would last for 20 days and that all stakeholders could submit their comments in this period. The development of the draft in secrecy and the shortest statutory deadline for a public debate were not the only problems in this process - the adoption of this Law would seriously undermine the achieved level of rights and freedoms in our country, especially the right to privacy.

The professional public and civil society organizations had numerous negative comments[3] to the Draft as well as suggestions for its amendment and adequate formulation. Complaints mainly referred to new authorizations for the processing of citizens' personal data, strict penal provisions, new rules on the use of the term "police", disclosure of identities of authorized persons, identification of police officers, etc. The strongest reactions were triggered by the provisions on the indiscriminate, mass video surveillance of public areas using biometric facial recognition systems without any previous analysis of potential risks to citizens' rights.

[2] http://www.mup.gov.rs/wps/wcm/connect/c8c5d780-fcb1-46b2-96be-650dbb3ef94e/NACRT+ZAKONA+O+UNUTRASNJIM+POSLOVIMA-cir.pdf?MOD=AJPERES&CVID=nKmncZs

[3] Komentari-na-Nacrt-zakona-o-unutrasnjim-poslovima-SHARE-Fondacija.pdf (sharefoundation.info)

A few days after the end of the public debate, the minister of interior announced[4] that he was withdrawing the draft from the procedure following the Serbian president's request. The reason for withdrawal was said to be "formal" as there were just six months left before the parliamentary and presidential elections, which was described as bad timing for the adoption of this law.

Although all those who commented on the draft had welcomed this step, citizens were still left with numerous unresolved issues. What will happen once a good political moment to pass this law arrives? What are the possibilities of video surveillance and associated technology? Who will be able to use the collected data and for which purpose? Do we really need video surveillance with facial recognition technology to keep us safer, or will it bring us to completely different position?

Publication of the Draft and Reaction of the Professional Public and CSOs

The new Law on Internal Affairs was supposed to replace the current Law on Police (Official Gazette of the RS, No. 6/2016, 24/2018 and 87/2018). The Ministry explained[5] that the draft was made in view of the need for a more precise definition, adaptation and harmonization of certain provisions with the practical needs of the MoI, in order to help improve the quality of policing and other tasks within the competence of the Ministry. A conclusion[6] was attached to the Draft saying that the public debate was to last between August 30, 2021, and September 18, 2021, which is the statutory minimum for public debates under the Government Rules of Procedure.

The public was not aware that the Draft was being developed, and even after its publication, many issues remained open. It is still unknown who was in the working group that developed the text, whether professional organizations were consulted during the preparation of the draft, or how

[4] Vulin: Na molbu Vučića, povučen Nacrt zakona o unutrašnjim poslovima (slobodnaevropa.org)

[5] http://www.mup.gov.rs/wps/wcm/connect/b142a791-747e-45a7-9915-4f6c08bbf3cd/OBRAZLOZENJE.pdf?MOD=AJPERES&CVID=nKmiY8X

[6] http://www.mup.gov.rs/wps/wcm/connect/e764195b-60dc-4258-bc32-b16159f9a55f/Zakljucak.pdf?MOD=AJPERES&CVID=nKmjAZR

long the preparation itself lasted. It is unknown why an impact assessment of the introduction of non-selective biometric surveillance system (envisioned by the draft) has not been prepared, like it should have been in keeping with Article 54 of the Law on Personal Data Protection (LPDP), despite the fact that this is an act of processing which is likely to result in high risks for the rights and freedoms of citizens.

A quick reaction of the professional public and civil society organizations prevented the public debate from passing unnoticed. Numerous organizations submitted their comments on disputable provisions, thus helping the public to be informed about the proposed changes and possible consequences of their implementation as well as to bring into question of the Draft's compliance with the Constitution, ratified international conventions, laws and established standards.

The public hearing was not formally concluded, and the proponent of the Draft did not publish a report addressing all suggestions put forward by stakeholders. In the absence of a formal source, the comments we will refer to in the text rely on those that could be heard in public.

Disputable Provisions of the Draft

Numerous changes were announced in the Draft's 365 articles. In this text, we will focus on the provisions that caused the greatest reactions among the stakeholders.

Article 59 and Article 355

Article 59 envisions several innovations. Under the Draft, instead of a police officer's name and family name, a "combination of letters and/or numbers serving the purpose of identification" should be displayed on police officers' uniforms. This Article also prohibits the "disclosure of information on the identity of an authorized official person who is enforcing police powers", while Article 355 envisions fines between RSD 30,000.00 and RSD 1,500,000.00 for the violation of this prohibition.

Although it is indisputable that the identity of police officers performing special police tasks during criminal investigations needs to be protected, the implementation of a provision that makes it difficult (and often impossible)

to identify all police officers provides those who exceed their powers and violate the law with complete protection from liability.

Moreover, this Article is not in accordance with the systemic law regulating information disclosure (the Law on Public Information and Media), which, in Article 82, says explicitly that private information and personal recordings may be published without the consent of the person to whom they refer if, in that specific case, the interest of the public to know outweighs the interest to prevent disclosure, and especially if the information refers to a public official and is published for the purpose of protecting the rights and freedoms of others.

The problematic nature of these Articles becomes additionally prominent if observed in the context of behavior of individual police officers towards participants in the July 2020 protests[7].

▸ Article 44

Although Serbia has the legal framework on the use of video surveillance in public areas (Law on Police, Law on Private Security), this draft is the first document envisioning the connection of cameras and biometric facial recognition systems and this type of processing of citizens' personal data.

Article 44 regulates data processing systems, e.g., audio and video surveillance systems, which consist of a set of fixed and mobile cameras and software/hardware solutions with analytical tools, which are used for automatic face detection, "including the processing of biometric data on the basis of detected facial and physical features, time and location and the person's participation in the event, automatic vehicle detection, recognition of license plates and other markings on the vehicle and detection of violations."

According to the rationale of the Draft, giving the police legal grounds to use "numerous data processing systems, and primarily video surveillance systems for the automated face and license plate recognition" should help to prevent crime and ensure greater detection of criminal offenses and arrest of their perpetrators. However, these claims were not accompanied

[7] http://www.bgcentar.org.rs/bgcentar/wp-content/uploads/2020/11/izvestaj-protesti_compressed.pdf

by data on the level of efficiency of these systems in the prevention and prosecution of criminal offences. In fact, comparative experiences show that their achievements are limited, that facial recognition algorithms are often imprecise and can result in the misidentification of persons, and violation of other rights and freedoms (such as wrongful convictions, discrimination, etc.).[8]

Although this Article envisions the introduction of non-selective video surveillance, connected to biometric facial recognition systems, the proponent of the Law did not prepare an impact assessment of the proposed processing on personal data protection. An impact assessment would have been in accordance with Article 54 of the Law on Personal Data Protection, although this act of processing is likely to result in a high level of risk to the rights and freedoms of natural persons. Under the LPDP, the assessment must contain a comprehensive description of the planned processing activities, an assessment of risks to the rights and freedoms of data subjects, and a description of measures to be taken to prevent risks (protection mechanisms and technical, organizational and staffing measures aimed at protecting personal data). However, the rationale of the Draft neither refers to such a document nor does it provide answers to the above-mentioned questions.

An additional problem lies in paragraph 8 of this Article, under which these systems can be connected to the similar systems of other state authorities, bodies of autonomous provinces, local self-government units and legal entities. This provision does not specify the authorities and legal entities concerned, situations in which the connection of the system would be allowed, or the way in which the applied personal data processing would be examined. If implemented, this provision would have the capacity to make citizens' biometric data available to a wide range of users and it would be nearly impossible to check how they are used and protected.

- Article 57

Paragraph 2. 4 of this Article envisions a new area of competency for official persons in policing – biometric identification based on physical characteristics.

[8] https://www.sharefoundation.info/wp-content/uploads/Analiza_procene_uticaja_SHARE_Partneri-Srbija_BCBP.pdf

Such a solution is in contravention with the Criminal Procedure Code (CPC) under which police engage in identification as an evidentiary action at the order of the prosecution or the court in connection with a relevant criminal procedure.

Another problem is that the CPC, as the law that regulates the entire criminal prosecution procedure, does not envision biometric identification on the basis of a person's physical characteristics as an evidentiary action. In view of the above, the Law on Internal Affairs would have to be harmonized with the CPC.

Article 58

Under this Article, an authorized official person may exercise police powers, *inter alia*, "at his own initiative". This wording enables authorized official persons to carry out actions, including those related to biometric facial recognition, without any control of the prosecution and the court. This results in the same problem as in Article 57 - discrepancy between this regulation and the Criminal Procedure Code.

The provision that allows authorized persons to act at their own initiative, without any restrictions pertaining to situations and scope of application of this right, paves the way to the possibility of the legalization of the abuse of office for private purposes.

Article 71

Under Article 71, the biometric facial recognition and data processing system may be used by authorized official persons to find perpetrators of criminal offenses who are prosecuted *ex officio*, to find persons for whom there are grounds to suspect that they are preparing the commission of a criminal offense, as well as to find wanted persons.

This provision gives an overly broad description of situations in which biometric recognition systems may be used making any control over the use of these systems impossible. If this provision were applied, there would be no way to limit these surveillance and recognition systems to potential offenders alone; rather, they would rather target all citizens who find themselves in the areas covered by the cameras.

International Recommendations for the Use of Biometric Facial Recognition Systems and Standards of National Legislation

Biometric facial recognition systems use a new, still developing technology whose characteristics are not fully known by the interested public. However, it is clear that the application of those systems (in the manner envisioned by the draft) is extremely intrusive when it comes to privacy with unforeseeable consequences for citizens' rights and freedoms. Therefore, bans of, or restrictions on the use of such systems is a global trend, supported and encouraged by numerous international organizations.

In January 2021, the Council of Europe published Guidelines on Facial Recognition[9], which contains instructions for the legislators, manufacturers of facial recognition equipment, and user organizations. According to the guidelines, the legal framework applicable to the biometric data processing through facial recognition should provide a detailed explanation of the specific use and intended purpose, an assessment of the reliability and accuracy of the algorithm used, retention duration of the photos used, possibility of auditing these criteria, the traceability of the process and the safeguards.

The United Nations has called for a moratorium on the acquisition and use of such technologies until it is determined that the use of smart video surveillance does not have a negative impact on democracy and that these systems are in line with the protection of citizens' privacy and personal data.[10].

The European Data Protection Board shares this position, explaining that a comprehensive ban on the use of these technologies for biometric facial recognition is necessary if we want to preserve our freedom and create a humane legislative framework for the use of artificial intelligence.[11] A regulation on artificial intelligence, which should govern the field of automated facial recognition, is being drafted.

[9] https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3

[10] https://news.un.org/en/story/2021/09/1099972

[11] https://edps.europa.eu/press-publications/press-news/press-releases/2021/edpb-edps-call-ban-use-ai-automated-recognition_en

It is unknown whether these guidelines and recommendations have been taken into account during the development of the relevant provisions of the Draft, but they were obviously not implemented.

In our country, the umbrella law in the field of personal data protection is the Law on Personal Data Protection. This act prescribes the relevant standards that public authorities have to observe in the introduction of new technologies and adoption of new regulations. Therefore, the Draft Law on Internal Affairs had to be harmonized with the standards provided for by the LPDP and ensure the same or even higher level of data protection in its provisions. If provisions of the Draft were applied, though, these standards would be significantly lower.

Withdrawal of the Draft from the Procedure and Informal Consultations

A few days after the end of the public debate, the Minister of the Interior announced that the draft had been withdrawn from the procedure.

In late September, the Ministry of Interior sent an invitation to informal consultations on the further development of the Draft Law to interested civil society organizations (including Partners Serbia). By the time when this text was written, five meetings were held with the participation of representatives of the Ministry of Interior and other relevant public institutions, representatives of the civil sector, scientific community and trade unions of MoI employees.

The meetings focused on topics related to video surveillance systems with biometric facial recognition software, technical characteristics and capabilities of the technology, legal basis for the introduction and use of such a system, impact assessment analysis of these technologies on citizens' rights and freedoms, compliance of the proposed provisions with applicable laws in other areas (personal data protection, informing, access to information of public importance, criminal procedure).

Conclusion and Recommendations

The Ministry of Interior has yet to state its position on the future course of action concerning amendments to the legal regulations in this area, i.e.,

on future steps in the development of a new or amendment of the existing Draft.

The Ministry has so far repeatedly emphasized that the new Draft Law will not be written "from scratch" and that the withdrawn Draft will be taken as the basis for the preparation of the new Draft, announcing that the comments and information presented in the current informal consultations will be taken into account.

Before developing a new draft, the Ministry of Interior should:

- substantiate the claims that Serbia needs to establish a video surveillance system with facial recognition capabilities. This should be done through the development of analyses that would identify the problems in the society which are addressed through video surveillance and define how video surveillance will help resolve these problems. Also, the necessity of introduction of such systems needs to be analyzed for the purpose of determining whether the same goal can be achieved using less intrusive means;
- In connection with the previous recommendation, the Ministry of Interior should publish all analyses either developed within this process or prepared by other public institutions, i.e., it should present to the public, in the integral form, all relevant information that corroborates or denies the MoI position that the introduction of a video surveillance system with facial recognition capabilities is necessary at this day and age;
- Develop an impact assessment of data processing on data protection, in the manner prescribed by the LPDP;
- Make available to the public all contracts and/or international treaties on the basis of which biometric surveillance projects are planned or implemented;
- Make available all information on the past procedures of procurement of equipment that can be used for biometric surveillance, as well as plans for future procurement of such equipment;
- - Proactively and adequately inform citizens about plans for the introduction of biometric surveillance, and include the wider community (academic community, civil sector, economic entities, etc.) in the discussion on the needs for the introduction of such a system.

SERBIAN CASE LAW IN THE FIELD OF PERSONAL DATA PROTECTION

Authors: Nina Nicović and Uroš Mišljenović

In 2021, Partners Serbia conducted a detailed research on the work of public prosecutors' offices and courts in cases referred to in Article 146 of the Criminal Code – Unauthorized Collection of Personal Data. Last year's conclusions did not offer grounds for optimism. It was observed that the case law had not been developed; between 2015 and August 2020, judgments of conviction were rendered in just two court cases, both of which ended with suspended sentences. The main reason for such a small number of judgments in which violations of the right to personal data protection are found lies in the fact that the Commissioner's criminal reports do not get an epilogue, that is, that prosecutor's offices rarely file indictments (only two in the relevant period). In view of a large number of violations of the right to personal data protection and incidents such as unauthorized access to public records and leakage of data from institutions to the media, and simultaneously a small number of cases that reach the court at all, the conclusion was made that Serbia currently did not ensure adequate legal protection to injured parties - victims of abuse of personal data.

This year's research focuses on case law in an attempt to determine whether any progress has been made in sanctioning the perpetrators of the above-mentioned criminal offense, which should serve as an indicator for determining whether the legal protection of injured parties - victims of personal data abuse - has been improved.

For this purpose, all judgments rendered by courts in cases referred to in Article 146 of the CC in the period between September 2020 and August 2021 were collected and analyzed. The information was obtained from the courts, using a mechanism established by the Law on Free Access to Information of Public Importance.

Overview of Case Law for Article 146 of the CC: September 2020 - August 2021

The sample we have formed contains three convictions for the criminal offense of unauthorized collection of personal data by an official person referred to in Article 146 paragraph 3 of the CC. In these cases, the public prosecutor's office is in charge of initiating criminal proceedings against the perpetrator. In addition to this, there were two convictions in cases initiated by private lawsuits for the criminal offense of unauthorized collection of personal data referred to in Article 146 paragraph 1 of the CC.

In order to make more detailed conclusions about the case law, we need to analyze judgments in the relevant cases on the basis of the imposed penalties and the method of commission of the criminal offense.

In cases within the jurisdiction of the public prosecutor's office, suspended sentences were imposed in two cases[12] and a fine in the third.[13] Interestingly, in all three cases, both parties - the public prosecutor and the defendant - waived their right to appeal[14] and the reasonings of the judgments, in accordance with the law, contained only a brief summary of facts.[15] This is a step forward because of the efficiency of the procedure: it only took seventy-seven (77) days between the date when the motion to indict was submitted to the court by the competent public prosecutor to the date of the trial and publication of the judgment.

More specifically, in the first case[16] the criminal offense was committed by an administrative employee in the municipality, who, without the consent of the injured party, entered her UMCN (unique master citizen's number) in a certificate issued by the municipality and handed it over to her ex-husband.

In the other case,[17] the convicted person was a police officer who used his ID card to access the official computer in order to check the date of

[12] Basic Court in Aleksinac K.No. 359/20 and Basic Court in Užice K 547/20.

[13] Basic Court in Užice K.No. 122/21.

[14] Art. 510 ZKP.

[15] Art. 429, paragraph 1, item 1 ZKP.

[16] Basic Court in Aleksinac K.No. 359/20.

[17] Basic Court in Užice K 547/20.

expiry of a car registration, and while checking another car, he looked up the place of residence of the owner as the place of registration of the vehicle. He later disclosed the data to a friend, in accordance with their previous arrangement.

The third case[18] also involved a police officer. He had access to the Serbian MoI electronic database, which he used to obtain identification data for a number of individuals, registration numbers, notions and designations.

In the cases initiated by private lawsuits – the first case ended with a suspended sentence,[19] while the court issued a judicial admonition in the other[20].

In the first of the two cases,[21] the defendants used their Facebook page to post a decision containing a private prosecutor's personal data, which they had obtained illegally, thus enabling an unlimited number of people to get access to it.

In the other case[22] the defendant posted a number of photos on her Facebook account showing the judgment of the Basic Court in Požarevac with unredacted personal data (name, family name, address, UMCN, current account number and bank) of the private prosecutor as well as his cell phone number.

According to the available documentation used in the research, court proceedings were suspended in five cases due to the following reasons: expiry of the absolute statute of limitations for criminal prosecution[23] (4 years for paragraph 1 in a case initiated by a private lawsuit, and 6 years for paragraph 3 in a case initiated by a criminal report against an official person[24]), failure of the heirs to state whether they wanted the court proceedings to continue after the death of a family member who had filed

[18] Basic Court in Užice K.No. 122/21.
[19] Basic Court in Novi Sad K.No.1249/20.
[20] Basic Court in Požarevac 89 K.No.9/21.
[21] Basic Court in Novi Sad K.No.1249/20
[22] Basic Court in Požarevac 89 K.No.9/21
[23] First Basic Court in Belgrade 8 K.254/17 and 19 K.239/21.
[24] Art. 103 and 104 KZ.

the private lawsuit,[25] absence of the private prosecutor or his proxy at the trial to which they were duly summoned, i.e. received the summons, but failed to justify their absence,[26] due to the withdrawal of a private criminal lawsuit and because of the withdrawal of a criminal lawsuit.[27]

Since the court always reviews whether a private lawsuit was filed by an authorized prosecutor, it is important to pay attention to whether the defendant has been charged under paragraphs 1, 2 or 3, in view of the fact that only a public prosecutor can prosecute official persons who have committed the criminal offense of unauthorized collection of personal data referred to in paragraph 3. What makes things complicated for citizens is that they can waste valuable time on a wrong charge (either through a private lawsuit or through a criminal report) and thus run the risk of expiry of the absolute statute of limitations for this criminal offense, which, in fact, does not last long, just 4 years from the date of commission of the criminal offense. To be fair, we have to say that the court is entitled to take into account the timeliness of the private lawsuit, even if it had first been filed in the format of a criminal report or motion for criminal prosecution to the police/competent prosecutor's office. This will be the case if it is has been filed within the time frame envisioned for a private lawsuit, and it turns out that the prosecution believes that there are elements of a criminal offense that can be prosecuted by a private lawsuit.[28]

In the cases in which the court decided to reject the private lawsuit, the reasons were the failure of the injured party's attorney to describe why the defendant is guilty, to state the general subjective elements of the criminal offense – i.e., sanity, intent, awareness of the criminal act itself, i.e., the fact that it is prohibited, and as a result the court believed that there was no room for the charge, because the requirements were not met for the implementation of a security measure and because the subject matter of the charge was not a criminal offense.[29] In another case, a decision to reject was made and the reason was that the private prosecutor had desisted from the criminal prosecution of the defendants. [30] In our opinion, in this specific

[25] Art. 57 ZKP/First Basic Court in Belgrade 5 K.2218/19.

[26] Basic Court in Stara Pazova, court unit in Inđija Kbr.11/17.

[27] Basic Court in Sombor 1K.No.302/20.

[28] Art. 65 ZKP; Basic Court in Novi Sad K.No. 1249/20.

[29] Third Basic Court in Belgrade (redacted number) od 22.07.2021.

[30] Basic Court in Novi Sad K.No. 441/2020.

case, there was room for dismissal of a part of the private lawsuit, in view of the fact that the second defendant was charged with the commission of a criminal offense referred to in paragraph 3, which means that there was no authorized prosecutor, because the public prosecution is competent for initiating criminal proceedings under that paragraph.

These elements are important because if they are absent, or if they have not been supplemented or put in order at the order of the court, the court will believe that the shortcomings of the private lawsuit have not been removed and will reject it. Most frequently, private lawsuits are rejected because of the very order of the court to the private prosecutor to put the private lawsuit in order by supplementing it with the aforementioned elements within a certain period of time.

***

In view of the previous research, there is a number of court decisions with reasonings that shed light on the direction which the current modest case law will take with regard to the criminal offense of unauthorized collection of personal data referred to in Article 146 of the CC. Specifically, according to the reasonings of the judgments, we may conclude that the court in these cases reviews the following criteria to decide on the existence of the criminal offense referred to in Article 146 of the CC, and that the failure to fulfill them results in acquittal**:**

- Can the data be regarded as personal data?
- Was the person authorized to obtain this piece of information and what have they used it for? In this context, the important documents are those containing the job description if the criminal offense has allegedly been committed by an official person.
- Do the data refer to a specific person or any individual, has that person given his/her consent for the publication of his/her personal data, and therefore does the criminal offense exist?
- Did the defendant actively participate in the acts he/she is accused of (e.g., the act of disclosure, sharing on social networks, etc.)?
- Is it clear how the data which enjoy criminal law protection have been transferred (made available, how the access to them was provided, etc.)?
- Were personal data publicly accessible (e.g., on the website of the APR or the municipality) and had to be anonymized? It is important to

determine whether the anonymization has been done correctly, the date of publication of the document that contained the relevant personal data and whether it was subsequently changed/published again.[31]

- - Has the defendant done everything in his/her power to keep the confidentiality of the personal data (marking, redacting, etc.) or has the document been published/disclosed in its integral form?
- - Provisions of relevant laws that may lead to exceptions in the publication of personal data, as well as whether the public has the interest to know in the relevant case (Law on Public Information and Media, Law on the Prevention of Corruption...).
- - Until when did the defendant engage in personal data processing? This is important in order to determine the intent and statute of limitations (because of possible tardiness of the consequences of the criminal act.)

On the basis of everything presented above and the available case law, we can conclude that in order for it to be evident that a criminal offense has been committed, the defendant would have to take actions that are, in essence, active, and it is up to the prosecutor (public or private) to prove, i.e., put into context, the actions of the defendant as the very actions which constitute the elements of the criminal offense.[32] Let us take the act of acquiring as an example. The prosecutor would have to provide the court with evidence clearly linking a series of defendant's actions- from whom, how, when and with what intention he/she has obtained personal data. All this should also be interpreted in the context of unauthorized actions, because when an authorized person does it, within his/her job description or competence and the specific tasks of which he is in charge,[33] then this is not a criminal offense referred to in Article 146 para. 1, 2 and 3.

Conclusion

Observed against the two convictions from the period between 2015 and August 2020, we can note an increase in the number of such decisions in the period covered by the new research. It is evident that in a significantly shorter period of one year, there were more convictions than in the previous 5.5 years.

[31] First Basic Court in Belgrade 27 K.No.2087/20.

[32] First Basic Court in Belgrade 15 K.1720/18.

[33] Basic Court in Novi Sad K.No.751/20.

On the basis of the presented description of facts in cases that resulted in convictions, we can note that the defendants were public officials who had abused their official powers with regard to access to other people's personal data, while the cases initiated by private lawsuits, we can stress the unauthorized publication of other people's data on social media, as the method of commission the criminal offense.

Although it is, without doubt, important that the perpetrators in these cases were sanctioned, i.e., that the victims in the relevant cases got satisfaction through convictions, we would like to point out that in our case law there are still no judgments in "major" cases of violation of citizens' rights to the protection of personal data referred to in Article 146 of the CC.

In last year's analysis, we pointed out that the cases initiated on the basis of the Commissioner's criminal reports for this criminal offense were "at a standstill" in the public prosecutor's office, i.e.,, that they have not had an epilogue. Since the number of cases that are resolved at court is still small, that is, since there have been only seven convictions since 2015, the quality of the case law cannot be determined this year, nor can we say whether the sentencing policy is lenient or strict. The key recommendation to that end is similar to the one presented last year: the number of motions to indict submitted to the court by public prosecutors' offices has to increase, especially in cases in which there have been large-scale violations of citizens' rights, either because of the number of injured parties, or because of the consequences experienced by them.

GENERAL COMMENT NO. 25 OF THE COMMITTEE ON THE RIGHTS OF THE CHILD on children's rights in relation to the digital environment and protection of the right of the child to privacy in the digital environment in Serbia

Author: Vlada Šahović

1. Introduction

At its 86th session, the Committee on the Rights of the Child adopted the General Comment No. 25 on the children's rights in relation to the digital environment. At the very beginning of this document, the Committee recalls that "the digital environment is becoming increasingly important across most aspects of children's lives, including during times of crisis, as societal functions, including education, government services and commerce, progressively come to rely upon digital technologies. This affords new opportunities for the realization of children's rights, but also poses the risks of their violation or abuse. "[34]

The necessity to protect children and their privacy in the digital environment was recognized as an issue of major importance in the past by different players, such as international and intergovernmental organizations[35]

[34] Child Rights Committee (CRC), 'General Comment No. 25 (2021) on children's rights in relation to the digital environment', 2 March 2021, CRC/C/GC/25, para 3.

[35] For example, on the following link you can find the research of the UNICEF Office

or regional human rights protection bodies/mechanisms.[36] In view of the prevalence of digital technologies and their frequent use by children of an increasingly young age, the Committee as early as in 2019 started a consultation process for the purpose of drafting the General Comment with different players, including state parties to the Convention on the Rights of the Child, experts on children's rights, intergovernmental organizations, civil society organizations, national human rights protection institutions, and most importantly the children themselves - 709 children from 28 countries, who live in diverse conditions. At the end of the consultations, one of the more extensive general comments of this body was produced and published in March this year, touching upon different individual rights of the child contained in the Convention, and pertains to the protection and realization of children's rights in the digital environment.

Namely, this document will primarily focus on the specific Authoritative guidelines of the Committee presented in the General Comment, which refer to children's rights to privacy in relation to the digital environment and to the harmonization of the national regulatory frameworks with it. As pointed out by Krivokapić, PhD, and Antonijević, the regulatory framework is not the only factor in the improvement of child protection.[37] Of course, the Convention on the Rights of the Child clearly states that the state parties will undertake "all appropriate legislative, administrative, and other measures" for the implementation of the rights recognized in the Convention,[38] which is what the Committee recalls in General Comment No. 25, making it clear that it is necessary to have a comprehensive approach to children's rights in the digital environment[39]. In view of this, the central focus of this text will be on the aforementioned regulatory framework and due to the focus of this analysis it will not refer much to other existing measures, programs, etc.

of Research – Innocenti: https://www.unicef-irc.org/research/child-rights-in-the-digital-age/; accessed on 14.8.2021.

[36] Council of Europe, Guidelines to respect, protect and fulfil the rights of the child in the digital environment, Strasbourg, June 2019, CM/Rec(2018)7.

[37] Krivokapić, Đ., PhD, and Antonijević, M., 'Ostvarivanje prava dece na zaštitu od štetnih sadržaja i zaštitu privatnosti' (Realizing Children's Right to the Protection from Detrimental Contents and Protection of Privacy), available at: https://bit.ly/3CZ2NkG, page accessed on 12.8.2021.

[38] UN General Assembly, 'Convention on the Rights of the Child, November 20, 1989, UN Doc A/RES/44/25, Art. 4.

[39] CRC, *supra* footnote 1, paragraph 7.

First of all, we will review the measures for the protection of children's right to privacy in the digital environment which the Committee regards as necessary for ensuring the fulfilment of obligations of the States Parties to the Convention on the Rights of the Child. The next segment is dedicated to the analysis of Serbia's existing regulatory framework on the protection of children's right to privacy in the digital environment. The last part of the text will analyze the extent to which the domestic legislation is harmonized with the Committee's Authoritative Guidelines contained in the General comment No. 25 (2021) on children's rights in relation to the digital environment, i.e. the extent to which it complies with the obligations arising from the Convention on the Rights of the Child.

2. General Comment No. 25 and the Issue of Children's Privacy in the Digital Environment

Although the General Comment refers to a large number of rights contained in the Convention on the Rights of the Child, it is clear that the Committee believes that the issue of protection of children's privacy in relation to the digital environment is of great importance, in view of the size of the section dedicated to this issue in the document.[40] Article 16 of the Convention on the Rights of the Child envisions the obligation of States Parties to ensure that "[n]o child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honor and reputation," and that every "[c]hild has the right to the protection of the law against such interference or attacks."[41]

Before we review the part of the General Comment which is specifically dedicated to the issue of children's right to privacy, we need to review the basic principles of the Convention on the Rights of the Child. In the Comment, the Committee emphasizes their importance in establishing the measures necessary for realizing all rights of the child in relation to the digital environment, including the right to privacy. Namely, all measures that are established must be non-discriminatory, in the best interest of the

[40] Ibid, paragraphs 67-78.

[41] UN General Assembly UN, *supra* footnote 5, translated by UNICEF, available at: https://www.unicef.org/serbia/media/3186/file/Konvencija%20o%20pravima%20deteta.pdf, page accessed on: 12.8.2021.

child, respect the child's right to life, survival and development, and enable children to express their opinion in relation to all measures established by the state that concern them. When adopting measures, States Parties must also consider the development capacity of children and be aware of all opportunities and dangers which might affect children of different ages in the creation of these measures.[42]

Therefore, all measures concerning the rights of the child must be informed by these principles. Speaking about what States Parties should consider when developing regulations on the children's right to privacy in the digital environment, in addition to these basic principles, the Committee emphasizes that encroaching on a child's privacy is permissible only in a situation where this is neither arbitrary nor illegal. This means that any interference with the child's privacy should be provided by law, have a legitimate purpose, support the principle of data minimization, be proportionate and in accordance with the best interests of the child and must not be contrary to the provisions and objectives of the Convention.[43]

Legislative measures imposed by the state for protecting the child's privacy from all those who process his/her data must include strong safeguards, transparency, independent oversight and access to remedy. They should also require the integration of 'privacy-by-design' into digital products and services that affect children. Whenever consent is needed for processing a child's data, the state must ensure that the consent is informed, meaningful and given freely, either by the child, or by his/her parents or caregiver, depending on the age of the child. Finally, it is necessary to regularly revise all laws concerning the protection of children's privacy and data.[44]

States Parties should ensure that children and their parents or caregivers can easily access stored data, rectify data that is inaccurate or outdated and dele data unlawfully or unnecessarily stored by public authorities, natural persons or other bodies. They should also ensure the right of children to withdraw their consent and object to personal data processing where the data controller does not demonstrate legitimate, overriding grounds for the processing. The law should also prescribe which authorities, organizations and individuals are allowed to process the child's personal data, in compliance

[42] CRC, *supra* footnote 1, paragraphs 8-21.

[43] Ibid, paragraph 69.

[44] Ibid, para. 70 and 71.

with such due process guarantees regular audits and accountability measures. Children's data gathered for defined purposes should be protected and exclusive to those purpose. The data should not be retained unlawfully or unnecessarily or used for other purposes. It should also be possible to use the child's collected data in another setting if this is useful for the child, but the use of such data should be transparent, accountable and subject to the consent of the child/parent/caregiver.[45]

Privacy and data protection legislation should not arbitrarily limit other rights of the child, and the States Parties should ensure that this legislation respects the children's privacy and personal data in relation to the digital environment. Any digital surveillance of children, together with any associated automated personal data processing, should respect the child's right to privacy and should not be conducted routinely, without the knowledge of the child/parent/caregiver, nor should it take place without the right to object to such surveillance. Priority should also be given to the least intrusive methods that can fulfill the desired purpose.[46]

Therefore, laws on the protection of children's privacy in the digital environment, or those that regulate the method of collection of children's data, either for the purpose of regulating work in the public or in the private sector, should contain the following elements:

- clear safeguards
- transparency of all measures
- independent mechanisms for monitoring the implementation of the measures
- defined legal remedy and access to it
- provisions on the necessity of getting an informed agreement/consent for data processing from the child, parent or caregiver
- possibility to withdraw one's agreement/consent
- instructions on regular audits
- provisions on the accessibility of personal data to data subjects
- provisions on the possibility of requesting the rectification/deletion of collected data
- provisions specifying those who are allowed to process personal data

[45] Ibid, para. 72 and 73.

[46] Ibid, para. 74 and 75.

- accountability measures for persons, authorities or organizations that process personal data
- a provision on the digital surveillance of children, preventing any routine and non-selective implementation of such monitoring without the knowledge of the child, and enabling objections to such a treatment.

In addition to this, the laws themselves, i.e., provisions of the law on privacy should not arbitrarily deprive the children of other rights.

The next segment of the text will focus on the analysis of the existing legal framework for the protection of the child's right to privacy in the digital environment from the aspect of the elements defined above, in order to determine whether the existing regulatory framework complies with the obligations arising from the Convention.

3. Protection of the Children's Right to Privacy in the Digital Environment – International, Regional and National Legal Framework

International

It has already been mentioned that Article 16 of the Convention on the Rights of the Child and Article 40(2)(b)(VII) establish the obligation of the States Parties, including the Republic of Serbia, to ensure the enjoyment of this right for all children in their territory. The provisions of this Convention should be directly applicable and the Convention obliges the States Parties to undertake measures, including legislative ones, in order to fulfill the obligations established by this treaty.[47] The Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, which Serbia has ratified, requires the States Parties to protect the privacy and identity of child victims and to take measures compliant with the national legislation to avoid inappropriate dissemination of information that could lead to the identification of the child. Other treaties adopted under the auspices of the United Nations, and

[47] UN General Assembly, *supra* footnote 5.

ultimately the Universal Declaration of Human Rights,[48] which can be said to have the status of international common law, also clearly emphasize the right to privacy of individuals. Out of the key international human rights protection treaties adopted under the UN auspices, the Convention on the Rights of the Child,[49] the International Covenant on Civil and Political Rights, the Convention on the Rights of Persons with Disabilities[50] and the International Convention for the Protection of All Persons from Enforced Disappearance[51] contain provisions that refer to the right to privacy. Although these treaties do not specifically mention children, children certainly either do or can belong to all groups protected under these treaties. Since the wider framework of international standards pertaining to this issue exceeds the limits of this text, they will not be quoted here.[52]

Regional

There are also regional agreements regulating the issue of privacy protection, both generally, of persons in the territories of the States Parties, and specifically, of children. Namely, under Art. 8 of the European Convention on Human Rights, "everyone has the right to respect for his private and family life, his home and his correspondence" and "[t]here shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being 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,"

[48] UN General Assembly, Universal Declaration of Human Rights, December 10, 1948, UN Doc A/RES/217(III), Art. 12: „ No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."

[49] UN General Assembly, International Covenant on Civil and Political Rights, (open to signing on December 16, 1966, entered into force on March 23, 1976) 999 UNTS 171 (ICCPR), Art. 17.

[50] UN General Assembly, Convention on the Rights of Persons with Disabilities, December 13, 2006, UN Doc A/RES/61/106, Art. 21.

[51] UN General Assembly, International Convention for the Protection of All Persons from Enforced Disappearance, December 20, 2006, UN Doc A/RES/61/177, Art. 19 and 20.

[52] For a more detailed overview, see Dr. Krivokapić, Đ. and Antonijević, M., footnote 4.

while Art. 6, *inter alia*, touches upon the right to privacy of children charged with a criminal offense.[53] Moreover, Serbia is a party to the Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), under which it has the obligation to respect or protect the privacy of individuals during any kind of automatic processing of personal data (including: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination)[54] in the public or private sector.

None of the above-mentioned documents, however, refer specifically to children's rights to privacy in the context of digital environment. The document that stands out in this regard and applies to the Council of Europe member-states is called Guidelines to respect, protect and fulfil the rights of the child in the digital environment - Recommendation CM/Rec(2018)7 of the Committee of Ministers (2018).[55] It refers to similar issues as the General Comment, which is the subject-matter of this text, and, like the General Comment, it is not binding. Although it is not binding, the recommendations contained therein are based on international and European conventions and standards, as well as the case law of the European Court of Human Rights, and although not binding *per se*, it serves as guidance to countries on how to comply with their obligations towards children in the context of digital environment that derive from other documents.[56]

However, we have to mention the EU instrument which has actually had a decisive influence on the amendments to the Serbian legislation – specifically the Law on Personal Data Protection –which has crucial importance from the aspect of protection of children's rights and the subject matter of this

[53] Council of Europe (CE), European Convention on Human Rights and Fundamental Freedoms as amended by Protocols Nos. 11, 14 and 15, (opened for signing on 4 November 1950, entered into force on 3 September 1953; latest amendments under Protocol 15 adopted on 1 August 2021(CETS No. 213)), ETS 5.

[54] Law on the Ratification of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *Official Gazette of the FRY – International Treaties, No. 1/92, Official Gazette of the SCG - International Treaties, No. 11/2005 – other law and Official Gazette of the RS - International Treaties, No. 98/2008 -other law and 12/2010*, Art. 2, para. 1(c).

[55] Council of Europe (CE), CM/REC(2018)7, *Adopted by the Committee of Ministers on 4 July 2018 at the 1321st meeting of the Ministers' Deputies*, 4 July 2018.

[56] Ibid, para. 1.

text. Namely, the EU General Data Protection Regulation (GDPR)[57] entered into force on May 25, 2018, establishing or raising to the level of obligation and making binding standards for personal data protection for EU Member States. Unlike previous EU regulations, i.e., EU Directive 95/46/EC,[58] which was replaced by the GDPR, it actually recognizes children as a special and vulnerable category, and an entire segment of the regulation is dedicated to the very issues that concern them. Although there is different critique that specifically refers to provisions regulating the rights of the child in the context of protection of the right to data privacy – from the fact that there is no definition of a child as such, to the arbitrary manner in which the age limit for a child's consent to personal data processing[59] is established – some believe the GDPR is at least just a step in the right direction,[60] while others believe that it is the most important document in the regulatory development of information policy in a single generation.[61]

[57] *EU General Data Protection Regulation (GDPR)*: 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), Official Journal 2016 L 119/1.

[58] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal L 281, 23 November 1995, pp.* 0031-0050, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046, page accessed on 28 August 2021.

[59] For a discussion on this topic, see Đorđe Krivokapić and Jelena Adamović, 'Impact of General Data Protection Regulation on Children's Rights in Digital Environment', *Anali Pravnog fakulteta u Beogradu 64(3)*, pp. 205-220, January 2016, available at: https://www.researchgate.net/publication/312355507_Impact_of_general_data_protection_regulation_on_children%27s_rights_in_digital_environment, page accessed on 28 August 2021.

[60] Martin Schmalzried, 'GDPR: A 'flexible' step in the right direction', *Better Internet for Kids*, available at: https://www.betterinternetforkids.eu/en-GB/practice/articles/article?id=687553, page accessed on 28 August 2021.

[61] Chris Jay Hoofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius, 'The European Union General Data Protection Regulation: what it is and what it means', *Information & Communications Technology Law 28(1), pp.* 65-98, (2019) Routledge, Taylor & Francis Group, pp. 66, available at: https://www.tandfonline.com/doi/full/10.1080/13600834.2019.1573501?scroll=top&needAccess=true, page accessed on 28 August 2021.

National

The Constitution of the Republic of Serbia clearly stipulates that human and minority rights are guaranteed and directly applied. It specifies that this also refers to human and minority rights guaranteed under generally accepted rules of international law, ratified by international treaties and laws. Laws that refer to guaranteed human and minority rights must not affect their essence, and "provisions on human and minority rights shall be interpreted to the benefit of promoting values of a democratic society, pursuant to valid international standards in human and minority rights, as well as the practice of international institutions which supervise their implementation."[62] In view of this, the above-mentioned provisions of international treaties to which Serbia is a party are of key importance for the protection and enjoyment of human rights in Serbia. Article 42 of the Constitution of the Republic of Serbia guarantees the protection of personal data as well as the right to court protection in case of their abuse.

In 2018, in view of its EU accession policy and process, the Republic of Serbiaadopted the Law on Personal Data Protection (LPDP),[63]).[64] The law was drafted based on the model of the GDPR, although the LPDP also includes provisions contained in the Law Enforcement Directive.[65] Similarly to the EU regulations, the LPDP is divided into sections and contains provisions beginning from the main principles of processing,[66] provisions on

[62] *Official Gazette of the RS*, No. 98/2006, Art. 18.

[63] LPDP, *Official Gazette of the RS*, No. 87/2018

[64] LPDP, *Official Gazette of the RS*, No. 87/2018

[65] EU Directive 2016/680 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, available in the Croatian language on: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A32016L0680.

[66] LPDP, *supra* footnote 30, Art. 5: Personal data shall be:

1) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'). Lawful processing shall be processing in accordance with this Law, or another law governing processing; 2) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; ('purpose limitations'"); 3) adequate,

the rights of data subjects, obligations of data controllers and processors, transfer of personal data to other countries and international organizations, the Commissioner for Information of Public Importance and Personal Data Protection, legal remedies, liability and penalties and special cases of processing and penal provisions. Through provisions on the protection of children and the legality of personal data processing in the case of minors,[67] issues concerning approvals for the processing of a juvenile's data[68] and adequate transparency and clarity of data,[69] provisions on the personal data protection obligation of persons[70] and obligation of the independent body for the supervision of the implementation of the Law, i.e., the Commissioner, with regard to juveniles' rights.[71]

When it comes to the protection of children's right to privacy with regard to the digital environment, the shortcomings of our law are largely the same as those of the GDPR, but from the aspect of the General Comment No. 25 of the Committee on the Rights of the Child, the LPDP seems to be largely in line with the elements highlighted in the first part of this document. Namely, it defines protection measures, as is the way in which the transparency of operation must be ensured and how the independent mechanism for monitoring the implementation of the measures is engaged (in this case the Commissioner for Information of Public Importance and Personal Data

relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization'); 4) accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'); 5) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation'); 6) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability'). The text is identical to Art. 5 of the GDPR - supra footnote 25, Art. 5.

[67] GDPR, Art. 6(f), LPDP Art. 12 para. 6

[68] GDPR Art. 8, LPDP Art. 16.

[69] GDPR Art. 12(1), LPDP Art. 21 para. 1.

[70] GDPR Art. 40(g), LPDP Art. 59 para. 1 item 7.

[71] GDPR Art. 57(1)(b), LPDP Art. 78 para. 1 item 2.

Protection). It defines the legal remedy and clearly regulates the necessity of giving informed and free consent for data processing and envisions the possibility to withdraw consent. The LPDP has provisions enabling access to personal data by data subjects and the child or the child's parent/guardian to request the modification or deletion of collected data. Additionally, it clearly defines those who are allowed to process data and under which circumstances and says that personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (so-called data minimization). The area where evident problems exist, although the Law addresses them, is monitoring, but this will be discussed later.

It is important, however, to mention that the General Comment is much less detailed than the GDRP or LPDP because it does not clearly define what must be fulfilled for the purpose of establishing the legitimate and lawful processing of a child's data nor does it define consent to the same extent. Namely, in the General Comment, the Committee says that States Parties should ensure that consent is informed and freely given by the child or by the parent or caregiver, while on the other hand, LPDP defines consent as "any voluntary, determined and informed and unambiguous expression of will of the person, by which that person, giving a statement or a clear affirmative act, gives his or her consent to the processing of personal data relating to him or her."[72] It is important to emphasize that the purpose of general comments is not to give precise instructions on how certain laws should look like, but to define which elements in relation to which area must be fulfilled in order for the States parties to be able to fulfill their obligations under (in this case) the Convention on the Rights of the Child. On the other hand, something that is of key importance in terms of obligations stemming from the Convention on the Rights of the Child is that, clearly, its basic principles have not been adequately reviewed during the development of the regulations, e.g., making it possible for children to express their opinion on the measures imposed by the state, which affect them. In this context, the Committee on the Rights of the Child clearly emphasizes the *obligation* of States Parties to take into account children's views in 'all matters affecting them', including in the adoption of such measures.[73] During the drafting

[72] LLPD, *supra* footnote 20, Art. 4 para. 2 item 12.

[73] Committee on the Rights of the Child, General comment No. 12 (2009): The right of the child to be heard, UN Doc CRC/C/GC/12, 20 July 2009, paragraphs 20, 27 and 28; also emphasized in the General Comment No. 25, *supra* footnote 1, para. 17: " When developing legislation, policies, programs, services and training on children's rights in

of this law, there was no meaningful discussion that would take into account children's views nor has there been any indication that an independent assessment was made of the lowest age for consent for data processing before it was set. The second key principle of the Convention, to consider children's evolving capacities during the development of the measure, was clearly not taken into account either. In addition to this, the Committee clearly emphasizes that the opinions of certain vulnerable groups of children must also be taken into account within the obligation to make it possible for the children to be heard in all matters affecting them.[74] However, since no process including children has been initiated during the adoption of this law, the positions of especially vulnerable groups have not been taken into account, which means that the issues of discrimination or of the potential discriminatory effect of the Law have not been taken into account either.

Although the LPDP is the central regulation governing the protection of individuals' right to privacy in the digital sphere, different sectoral laws also regulate ways in which children's personal data are processed and collected in the digital sphere.

Digital Surveillance – Collecting Children's Biometric Data Through Video Surveillance

In General Comment No. 25, the Committee for the Rights of the Child states specifically that any digital surveillance of children, together with any associated automated processing of personal data, should respect the child's right to privacy and should not be conducted routinely, indiscriminately or without the child's knowledge or, in the case of very young children, that of their parent or caregiver, nor should it take place without the right to object to such surveillance.[75] The LPDP clearly says that personal data must be processed lawfully and transparently,[76] as well as that the lawfulness of personal data processing is based on the fulfillment of certain criteria, one of which may be the consent of the data subject.[77]

relation to the digital environment, States parties should involve all children, listen to their needs and give due weight to their views."

[74] Ibid, para. 21, para. 1 item 3.

[75] General Comment No. 25, *supra* footnote 1, para. 75.

[76] LPDP, *supra* footnote 31, Art. 5 para. 1 item 1.

[77] Ibid, Art. 12 para. 1 item 1.

On the other hand, there are other criteria of lawfulness of personal data processing,[78] but the provision of great importance for this issue is the one on the processing of special types of data, including biometric data, collected for the purpose of the unique identification of a person.[79] Namely, the processing of this type of data is prohibited, but the Law envisions some exemptions allowing the processing of special types of data. This is, *inter alia*, the "realization of a significant public interest defined by law, if such processing is proportionate to the achievement of the goal and respects the substance of the right to personal data protection, and if appropriate and special measures of protection of fundamental rights and interests of data subjects have been applied."[80] Moreover, the processing of special types of personal data by competent authorities for special purposes is allowed only in certain cases prescribed by the Law, including where "the competent authority [is] authorized by law to process special types of personal data," or where "the processing of special types of personal data is carried out for the purpose of protection of the vital interests of the data subject or another individual." Although the Ministry of Interior has implemented an impact assessment of processing through video surveillance systems[81] on the protection of personal data in accordance with Article 54 of the LPDP and submitted it to the Commissioner for the Protection of Information of Public Importance and Personal Data, the Commissioner issued the opinion that this document, in fact, was not in accordance with the LPDP.[82]

[78] And these are: processing necessary for the realization and conclusion of a contract, processing with the aim of observing the legal obligations of the data controller, with the aim of protecting vitally important interests of the data subject or another individual, processing necessary for performing duties in the public interest or enforcing legally prescribed competences of the data controller and with the aim of achieving the legitimate interest of the data controller or a third party, LPDP, Art. 12 para. 1.

[79] Ibid, Art. 17 para. 1.

[80] Ibid, para. 2 item 7.

[81] Ministry of Interior of the Republic of Serbia, 'Procena uticaja obrade na zaštitu podataka o ličnosti korišćenjem sistema video nadzora' (Impact Assessment of Processing With the Use of Video Surveillance Systems to Personal Data Protection), 02/4 No. 072/2-28/19-20, of 29 March 2019.

[82] Namely, the assessment does not include data on the following „to which specific video surveillance system/systems it refers, the legal basis for this, planned processing activities, risks for the rights and freedoms of data subjects, and consequently, one cannot determine whether the data controller has appropriately assessed the risks to

Even if the possibility to include biometric surveillance in the above-mentioned exemptions existed, the law would have to treat the issue of children's right to privacy in this context separately, in view of children's special vulnerability. The Committee clearly emphasizes, along with the Council of Europe[83], that mass surveillance practices can result in arbitrary and unlawful interference in the children's rights to privacy[84]. UNICEF also focuses on the potential consequences of this type of surveillance of children, including misidentification as a result of the absence of adaptation of these systems to the child's physiognomy, inability of children and their parents or caregiver to recognize the risks and consequences of these systems for the child's well-being, as well as the inability to determine how lifelong collection of data on children will affect their right to privacy and general well-being throughout their lives.[85] In view of this and the fact that any interference with children's rights must be prescribed by law, collected personal data should be adequate and essential, the collection is limited to what is necessary for the purpose of data processing and the best interest of the child is of central importance in the development of any measure affecting the enjoyment of children's rights the compatibility between biometric surveillance as it is currently enforced and international obligations concerning children's rights is brought into question.

Protection of Children's Right to Privacy and Education

The Law on the Fundamentals of the Education System[86] envisions the establishment of a single education information system (SEIS), which is "a set of databases and computer programs needed for the collection

persons' rights and freedoms and whether it has envisioned appropriate measures for their reduction." Commissioner's opinion, available at: . For more information on this topic, see: https://praksa.poverenik.rs/predmet/detalji/FB967E2A-AE57-4B2C-8F11-D2739FD85A9B. For more information on this topic, see: https://hiljade.kamera.rs/sr/zakon-drustvo/.

[83] Council of Europe, *supra* footnote 22, para. 25.

[84] Committee on the Rights of the Child, *supra* footnote 1, para. 67.

[85] UNICEF, Faces, 'Fingerprints and Feet: Guidance on assessing the value of including biometric technologies in UNICEF-supported programs', July 2019, pp. 19.

[86] *Official Gazette of the RS*, No. 88/2017, 27/2018 -other law, 10/2019, 27/2018 -other law and 6/2020

and processing of data in records and registers, while ensuring personal data protection."[87] In addition to this, the Rulebook on the Single Education Information System regulates in greater detail the type of processed data and data management.[88] The Law and the Rulebook have been harmonized to the greatest possible extent with the LPDP and the General Comment No. 25. SEIS is accessible only to the legally defined data processors and the purpose of processing is clearly defined, while the access to a child's stored data using the unique education number (JOB) is granted only to the child or his/her parents/legal guardians, at request. However, it is not clear whether they can request the modification of data whenever they deem the modification or correction of incorrect data necessary. Additionally, it has not been specified on what grounds other bodies and organizations can gain insight into that data.

Moreover, it has not been clearly explained why certain data concerning pupils and students are kept permanently, while those concerning the social and functional status of the child are kept for five years.[89] In view of this, the time frames for the storage of pupils' and students' data need to be explained in greater detail and there is a need to prescribe when periodic assessments of the need for further keeping of data will be made. Although Article 181 paragraph 2 regulates the purpose of processing of the collected data on pupils and students, it is questionable whether all data referred to in the law needs to be kept indefinitely, or if particular data need to be kept for 5 years. At the very least, this calls for an expediency assessment of the keeping of behavior grades from the 6th grade for, e.g.,30 years.

Another questionable issue is the lawfulness of all processed personal data and the fact that, for example, parents must use their UMCN to be able to log in to the eDnevnik portal,[90] but this issue exceeds the scope of this analysis.

In addition to the issue of the normative framework for the protection of children's privacy in the digital sphere, it is also necessary to ensure the protection of this right during implementation. In this context, a striking

[87] Ibid, Art. 175. paragraph 1.

[88] *Official Gazette of the RS*, No. 81 of 15 November 2019.

[89] Law on the Fundamentals of the Education System, footnote 52, Art. 183 para. 5

[90] Commissioner for the Protection of Information of Public Importance and Personal Data, No. 072-03-0526/2019-05, of 6 March 2019.

case occurred in mid-2021, when users of the Reddit portal noticed that a script could be used for launching a brute-force attack using numbers from 10000000 to 99999999 on the mojasrednjaskola.gov.rs portal, and that students' personal data could be accessed, including names and family names, grades from all subjects from the sixth to the eighth grade of elementary school, etc.[91] The absence of an authentication system after the entry of eight-digit passwords for access to the database largely contributed to the exposure of a large number of children to the risk of privacy violation. Since the data controller has the obligation to implement the measures for the protection of collected data,[92] and since this had clearly not been done, and since, under the LPDP, the data controller also has the obligation to notify all persons affected about the violation of data,[93] it turns out that despite the existence of protection mechanisms, the prescribed measures must be implemented to ensure the enjoyment of rights. Otherwise, the observation of rights will remain only dead letter.

4. Conclusion

Although this analysis does not represent an exhaustive presentation of regulations and practice in the field of protection of children's privacy, its aim is to at least point to a wide range of issues concerning the protection of privacy of children in the digital sphere. Namely, this analysis does not touch upon the issue of protection of children's privacy in relation to non-state actors, nor does it focus on sectors such as health or employment, although according to the Labor Act, children above the age of 15 may get jobs.

There are good indications of progress in the field of protection of children's privacy in the digital sphere, especially after the adoption of the

[91] *Na državnom sajtu za upis u srednje škole nezaštićeni podaci učenika, Poverenik pokreće nadzor nad Ministarstvom prosvete (Students' data unprotected at the state-run website for enrolment in secondary schools, the Commissioner initiates supervision of Education Ministry)*, by Nikola Momčilović, startit.rs, 30. Jun 2021, available at https://startit.rs/na-drzavnom-sajtu-za-upis-u-srednje-skole-nezasticeni-podaci-ucenika-poverenik-pokrece-nadzor-nad-ministarstvom-prosvete/.

[92] LPDP, Art. 50. paragraph 2 item 1,

[93] LPDP, Art. 53 paragraphs 1 and 2, particularly in view of the fact that measures referred to in Art. 53 paragraph 3 item 1 have not been taken.

LPDP, and on the basis of everything stated above we can conclude that the domestic legislation has partly been harmonized with the provisions of General Comment No. 25 of the Committee for the Rights of the Child - children's rights to privacy in the digital environment in relation to protection of the right to privacy. However, it would be useful to reiterate that from the aspect of any digital surveillance of the child, including biometric surveillance, additional protection measures of the children's right to privacy should be introduced, which is clearly stressed in the General Comment. It is a fact that the General Comment represents an authoritative expert interpretation of the obligations of the States Parties to the Convention on the Rights of the Child, which means that the establishment of additional protection actually represents Serbia's international obligation.

On the other hand, normative protection is one thing, while the implementation of the normative framework in practice is something else, something that needs to be monitored constantly, as we can see from the example of the mojasrednjaškola.gov.rs. portal. Since the issue of children's privacy in the digital sphere is still more or less new, it is necessary to monitor developments in that sphere, constantly point to the space for the improvement of protection, and demand protection in accordance with the highest developed standards.

PERSONAL DATA PROTECTION IN THE JOB APPLICATION PROCESS

Author: Milica Marinković

Economic fulfillment represents the basis of social security and social inclusion of every individual, and in most cases, it is reflected in secure employment. Only those who earn enough to be above the poverty line and who have good chances on the labor market can be fulfilled in other social areas. Citizens' economic security represents the basis for the realization of many other rights, in the same way as the lack of opportunities represents the basis for social vulnerability. It is, therefore, important to ensure equal access to the labor market for all. Although equality is proclaimed, it is clear that employers value certain social groups less and see them as less desirable workers. The coronavirus crisis has only made the inequalities on the labor market more prominent. Members of social groups that are more exposed to discrimination on the labor market certainly have additional legal protection for that reason, but they can achieve equality on the labor market only if efforts are made for complying with the legal norms. However, one cannot simply adopt certain norms and expect legal entities whose primary goal is to make profit to comply with them. The prevention of such social phenomena requires work, both with employers who are to be explained why the principle of equality is important, and with candidates who are discriminated against and who can pave the way to the realization of their rights by seeking protection. In a system where citizens do not demand the protection of their rights, those rights are violated and undermined again and again.

This legal analysis was made with the aim of identifying the rights of job applicants and the obligations of a potential employer, from the aspect of the right to privacy.

Legal Organization

Article 42 of the Constitution of the Republic of Serbia explicitly prohibits and envisions sanctions for the unauthorized use of personal data that is not in accordance with the purpose of their collection, except in cases where this is designated as possible under a special law. It is said that everyone has the right to court protection in case of abuse of their personal data. Under the Constitution, the collection, holding, processing and use of personal data is regulated in more detail by special laws. In international documents, primarily the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, the protection of the right to privacy at the international and national levels refers to the private sphere of life, family life, inviolability of home and correspondence, honor and reputation of the individual. Since we are discussing the violation of the right to privacy in the job application process, in addition to this, it is important to emphasize that the Labor Act and the Law on Employment and Unemployment Insurance prescribe what must not be advertised in terms of job requirements, as well as what candidates must not be asked during job interviews. The laws require from the employer to ensure the equal treatment of those who apply for employment.[94] Provisions prescribing this prohibition and the obligation of equality in employment are also contained in the Law on the Prohibition of Discrimination and the Law on Gender Equality. They protect the rights of job applicants and workers by saying that their private characteristics must not affect employment and retaining jobs.

For the purpose of this analysis, job application process refers to the period in which one is looking for a job in a wider context, i.e., from the moment when they start looking at vacancies, until the moment when they are is hired. Therefore, it is important to stress that this includes all those situations in which a person is looking for a job and sees an ad and the requirements contained therein, even if he/she does not apply, that is, if he/she does not formally become an applicant. Also, the employer is a person or a legal entity that advertised the job, from the moment when the advertisement was published.

[94] Law on Employment and Unemployment Insurance, Art. 35. paragraph 1.

Prohibited Requirements for Employment

It is certainly important to emphasize that the requirements in job advertisements must refer only to professional qualifications, while all other requirements must be justified by the job description. Despite this, we can see every day that employers tend to add some requirements that are unrelated with the work to be performed. In this way, they are trying to bypass the legal provisions and eliminate the applicants whom they regard as unsuitable. Although aware that the employer should not request certain information, applicants provide them, nevertheless, knowing that they would otherwise be in a worse starting position because they are those who need employment. **The setting of such requirements results in the violation of the right to privacy because data which are requested are neither necessary nor important for the business and the application procedure. This results in excessive processing and the violation of the principles of proportionality and minimization, and, consequently, to the violation of the right to equality and equal treatment because, using the obtained data, the employer can eliminate a candidate only and exclusively because of a personal characteristic which is unrelated to professional qualifications**. This is frequently obvious in advertisements in which candidates of a certain age, appearance, marital status, etc. are looked for.

A job applicant said that at the interview at a law firm, she had been asked a question about her marital status, which she refused to answer. After that, she was informed by phone that she did not get the job.[95]

In the job application form on a bank's website, job applicants are required to disclose the following information: a) father's name b) marital status and c) children.[96]

A candidate who had been selected for a job and who, during the introduction into her duties, tried to postpone a meeting because of her child's illness, was informed that the company did not need somebody who had such obligations.[97]

[95] Opinion of the Commissioner for the Protection of Equality No. 07-00-116/15-02

[96] Opinion of the Commissioner for the Protection of Equality No. 07-00-624/13-02

[97] The Blic daily, https://bit.ly/3P5Zn4I

What is important is that, not only that unprofessional requirements lead to discrimination against applicants, but they also violate their right to privacy, and the danger from mobbing is certainly also present. These rights are doubtless closely interconnected, because the employer violates the right to privacy for the purpose of obtaining data that can violate the right to the equal treatment of applicants. Thus, for example, by asking about the marital and family status, the employer can get information about whether somebody has children, and they might not want to employ people with children in a belief that they often use sick leaves, which is one of the most frequent cases in practice; so, by revealing this information, an applicant puts himself/herself in a position in which the employer can discriminate against him/her. Employers can also get the desired information indirectly, through social media or if the candidate reveals some other private information, i.e., information unrelated to their qualifications.

In the first elimination round, employment agencies frequently organize interviews with the employer's HR staff. Since most of the HR staff are psychologists, this frequently represents a type of psychological assessment of the applicant. The applicant should approach such interviews with caution and focus on the requested information and the information that can be obtained based on his/her answers. The psychological testing of the Serbian Government's Human Resource Directorate is an interesting example. Namely, anyone applying for any vacancy in the state administration had to be subjected to psychological testing. The test contained some rather disputable questions and tasks. For example, one of the questions was: *How would you assess your sexuality*, and *do you think you can seduce any man/woman*, while during some tasks one just had to click on the keyboard as quickly as possible, and this would rule out applicants with disabilities, etc. The fact that this type of testing is no longer applied[98] does not erase the fact that for years, many applicants had to take this test regardless of whether they actually got a job or not, and that the test results had been kept so that they do not have to take it again the next time they applied.

[98] Under an opinion of the Commissioner for the Protection of Personal Data and Information of Public Importance No.: 011-00-01679/2015-02, according to which the psychological assessment of applicants in the way regulated under the Law on Civil Servants is in contravention to the Constitution and the LPDP, the provisions were put out of effect. Law on Civil Servants Art. 54-60.

It is noticeable that, in addition to professional documentation, the employer can also request a health certificate showing that the candidate is in good health, which can be justifiable depending on the circumstances. For example, if the workplace is high above the ground or outside and considered to represent a high risk, this requirement would be justified. But in the case of an office job, such a requirement could disclose the employer's intention to find out whether an applicant is pregnant or suffering from a serious disease.

After being hospitalized for pneumonia, an employee of a health center was referred to the Infectious Diseases Clinic to be treated for an HIV infection. During the treatment, he found out that the head of his department had informed his colleagues about his HIV status at the morning meeting and he then sent a letter to the director, informing him about his condition. After that, he was requested to undertake an assessment of his working capacity.[99]

Data That May be Collected

On the other hand, employers frequently need some data that are regarded as personal in order to decide whether to hire somebody. The key requirement in the processing of personal data is the observation of proportionality, which means that the data that have been taken are adequate and justify the purpose. Anything other than that would not be regarded as permissible, under the principles of processing referred to in Article 5 of the Law on Personal Data Protection (LPDP). Such data may be processed only if one of the legal grounds for data processing exists, under Article 12 of the LPDP. Thus, if data processing is not regulated by law, the most frequently used legal ground is the valid consent of the employee, i.e., the applicant, under Art. 15 of the LPDP, or the realization of a legitimate interest of the employer. When the validity of consent provided by applicants and employees is assessed, it has to be observed whether the consent represents a condition for the conclusion of the employment contract or if it belongs to other employment requirements.[100] In addition to this, if the applicant has

[99] Special Report on Discrimination in Labor and Employment, Commissioner for the Protection of Equality, pp. 225.

[100] For more information on proportionality when violating the privacy of an employee and conditions under which this may be regarded as justified, see Bărbulescu v. Romania, application No. 61496/08, Surikov v. Ukraine, application No. 42788/06

been offered a job, the employer might need some for the preparation of the employment contract, and in this case, this will constitute the legal ground for the processing.

Under certain conditions, the employer may process the so-called special types of personal data. **Article 17 of the LPDP explicitly defines the special types of personal data as follows: nationality or ethnic origin, political opinion, religious or philosophical belief or trade union membership, as well as processing of genetic data, health condition, sexual life or sexual orientation**. Although the employer may process this type of data only if this is permitted by law or if the employee provides his/her consent, if we take into account the imbalance of power of the two sides in these situations, where one is significantly more subordinated to the other, there is a dilemma whether this consent really represents the will of the employee or if the employee is forced to provide it because of his/her position. When this is assessed, one should take into account the Opinion No. 8/2001 of the European Council[101] on the processing of personal data in the employment context, according to which the consent of an employee or a job applicant can be regarded as freely given only when these persons can refuse to give their consent to data processing without any detrimental consequences to their labor-law status or possibility of employment, as well as when they can revoke a previously given consent for data processing without any consequences.

Legal Subordination of Participants in the Process of Candidate Selection

Practice has been observed lately, especially among larger companies, to look for applicants through employment agencies. In addition to this, there are some job types for which workers are usually sought though youth cooperatives (seasonal employment in the hospitality industry, short-term engagements in the event industry, building maintenance jobs, etc.). In both of these situations, the employer has no contact with the applicants in the first round of the selection process, which means that if a right is violated, it is often unclear who did it. The employer sets employment requirements and lists the characteristics which the applicant must have, but it is only to

[101] Article 29 – Data protection Working Party - WP 48 - Opinion 8/2001 on the processing of personal data in the employment context, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1365969

be expected that agencies and youth cooperatives, whose job is to deal with employment, will introduce some additional criteria during the selection process. Thus, the applicant himself/herself may not know who has really violated his/her right.

Since, as it has already been said, multiple entities may participate in the selection process, it is important to point out differences in their relations in view of their position towards data. In the majority of cases, the employer will advertise the vacancy on employment websites. In this case, the employer is the data controller and the advertiser is the data processor, which means that the relationship between the data controller and the data processor has to be regulated by contract. Although this is the most frequent situation, employers are hiring recruitment and employment agencies at an increasing pace. In the latter case, the employer is the data controller, while the agency, when it assesses the applicants, is the data processor, but when it independently evaluates applicants, it is a data controller. We can also come across situations in which an employee is seconded to a company, as a so-called leased employee, in which case the employer, the cooperative and/or the agency are all data controllers together.

When we discuss who and under which circumstances may process personal data, it is important to emphasize that the data controllers, or in this case employers or job advertisers, must do their best to provide data subjects with all information in relation to the exercise of their rights. The data controller has the duty to provide assistance to the data subject and must not refuse to comply with his/her request. When collecting information, the data controller must provide the data subject with a whole set of data regarding processing,[102] primarily regarding the: identity and contact information of the data controller; contact information of persons in charge of personal data protection; purpose of the intended processing and legal grounds for processing; existence of a legitimate interest of the data controller or a third party; recipient or a group of recipients of personal data; how long the data are stored, his/her rights; possibility of revoking his/her consent and of correcting or deleting data. If this information is not provided, the applicant has the right to request it. Since there are numerous situations in which multiple entities might be involved, it is important to stress that data may be transferred to another person upon consent.[103]

[102] Art. 21 and 23 of the LPDP

[103] Art. 36 of the LPDP

As job advertisers, the National Employment Service and other job advertising websites have the legal obligation to implement equality policies and must warn an employer who wants to advertise a vacancy quoting unlawful requirements that such an ad may not be published. Art. 7 paragraph 1 of the Law on Advertising, which regulates the conditions and method of advertising as well as the obligations of persons who participate in the advertising process, prescribes the principle of prohibition of discrimination and prohibits advertising which directly or indirectly incites discrimination on any basis, especially on the basis of race, skin color, gender, nationality, social origin, birth, religion, political or another belief, financial status, culture, language, age, mental or physical disability. Under Article 11 of the Law, the advertiser has the duty to provide the transmitter with a declaration containing all the details regarding the ad together with the advertisement. In practice, this would mean that the advertiser would violate the law if he/she published the relevant ad.

As for the mutual responsibility of entities participating in the selection process, there is a very interesting example from the practice of the Commissioner for the Protection of Equality, in which a complaint was filed against a Belgrade-based company.[104]

The applicant responded to a vacancy ad of a company, posted on the website of the National Employment Service, and applied for the position of "administrative employee (M/F)". On the same day, he received a response saying that "the company is looking for female applicants only," and that his application will not be reviewed for that reason. During the procedure, it was determined that the ad for the position of "administrative worker (M/F)" in this company had been posted on the National Employment Service website, that the applicant had applied, but that he had received two emails saying that they were looking for "for a female applicant only", a "female secretary", apologizing for their inability to give a positive reply to his application.

In this case, it is important to stress that the Commissioner for the Protection of Equality has established during the procedure that the advertiser had not violated the legal provisions and that the ad had been posted in accordance with the law, but that the applicant had been discriminated against through the employer's actions, which means that on this occasion, the NES had complied with the law, and the candidate's right had been violated by the employer.

[104] Opinion of the Commissioner for the Protection of Equality No. 07-00-396/16-02

Difficulties in Proving

In connection with the above-mentioned situation, where as a result of the participation of multiple players in the selection process, an applicant could not know who had set the requirement that violated his/her right to privacy, there is a dilemma regarding the person against whom the protection procedure needs to be initiated. On top of this, such situations are often difficult to prove, because they usually happen between two persons and the application documents are in the hands of the employer, which means that there is no written trace of the requested information. Of course, disputable requirements which violate the applicant's rights and which are contained in the advertisement are much easier to prove. In this case, it is important to stress that even the rights of a candidate who did not apply at all can be violated, if the potential candidate, having seen the requirements, had given up in advance, believing that the employer would eliminate him/her after the violation of his/her right to privacy and after getting certain information. In practice, though, a candidate who has not been formally eliminated would not have stand a good chance to prove anything. Just because of these aggravating circumstances, it depends on the person believing that his/her right has been violated whether he/she will look for evidence on his/her own, which can be done by text messaging or emailing the employer, as well as by talking to other applicants who would be willing to testify about the disputable requirements they had to fulfil.

A better recognition of this issue in the legal provisions would certainly facilitate the path to the protection of rights. A simplified approach to proving can be found in some procedures for the protection of rights, such as the procedure for protection against discrimination, but this is not the case with all procedures.

Punitive Policy

Many regulations that protect the right to equality and equal opportunities, which is closely related to the right to privacy in this context, contain provisions on misdemeanors committed through the violation of provisions on the application period and violation of rights. Under the Law on Gender Equality[105] a fine from RSD 50,000 to RSD 2,000,000 shall be imposed on

[105] Law on Gender Equality, Art. 67.

an employer who has the status of a legal entity if: it does not provide the employee, regardless of his/her gender, or gender and family status, with equal opportunities in the field of labor and employment; as well as when it violates the prohibition to discriminate.

The Law on Prohibition of Discrimination[106] envisions a fine of between RSD 50,000 and RSD 500,000 for a legal entity or an entrepreneur who violates the principle of equal opportunities in employment or prevents the exercise of all employment rights under equal conditions on the grounds of personal characteristics by a person doing temporary and occasional work, a person doing additional work, a student or a pupil undergoing vocational practice, a person undergoing professional training and development without concluding a contract of employment, or a volunteer.

The highest penalties are provided by the Employment Act[107], which envisions a fine of between RSD 600,000 and RSD 1,500,000 for a misdemeanor committed by an employer who has the status of a legal entity in case of violation of the prohibition of discrimination under this Act.

In addition to this, the LPDP also envisions hefty fines amounting to between RSD 50,000 and RSD 2,000,000 for the violation of the provisions of this law for an offense committed by a data controller or a data processor who has the status of a legal entity.

Concluding remarks

In order to improve the situation in this field, certain steps need to be taken with the aim of ensuring a better implementation of the law, on the one hand, and raising citizens' awareness, on the other.

Our analysis of punitive provisions shows that the statutory fines cannot be regarded as negligible, and that their amounts serve the purpose of intimidating employers and deterring them from breaking the law. Despite this, we can notice that, on the other hand, penal provisions are not applied widely. This primarily refers to the Labor Inspectorate, which, on the one hand, receives a small number of reports for the violation of rights, and, on

[106] Law on Prohibition of Discrimination, Art. 51.

[107] Employment Act, Art. 274.

the other, it finds violations of rights in a very small number of reports it is acting upon.[108] Such behavior of the authority whose sole purpose is to protect the applicants and employees causes distrust, which, in turn, leads to a small number of reports.

The Inspectorate has to apply its competences and act on reports to a greater extent. The purpose of the fines is to deter employers from violating the law, and if several hefty fines were imposed, the business community would very quickly start to observe the law much more.

As for persons who participate in the entire process and the determination of their obligations, one might say that the law recognizes them, like it recognizes their obligation to refrain from violations of the applicants' rights. However, since there is no facilitated procedure of proving, since employment intermediaries participate in the process and since the enforcement of the inspectorate's competences and penal policies are weak, employers easily break the barrier between the private and the professional, finding out applicants' data that are completely unrelated to their professional development. Prevention efforts would include the raising of employers' and applicants' awareness regarding this concept and its consequences. A multidisciplinary approach to prevention would be of key importance, ensuring that consequences are not observed just from one aspect of the violation of the law. In addition to this, raising the awareness of citizens would improve their knowledge of the concept and methods of protection, resulting in a greater number of requests for the protection of rights and enabling citizens to gain greater control over their own data.

[108] Research of the A 11 - Initiative for Economic and Social Rights, available at https://www.a11initiative.org/wp-content/uploads/2021/04/Polozaj-radnica-u-trgovinskim-radnjama_SRP.pdf